MCSA/MCSE

Training Kit

Exam 70-227

Microsoft®

Internet Security and Acceleration Server 2000

Microsoft® Press

Учебный
курс
MCSA/MCSE

Сертификационный экзамен 70-227

Microsoft®

Internet Security and Acceleration Server 2000

Официальное пособие Microsoft®
для самостоятельной подготовки

Издание 2-е, исправленное

Москва 2003

РУССКАЯ РЕДАКЦИЯ

УДК 004.738.5
ББК 32.973.202
М59

Microsoft Corporation

М59 Microsoft Internet Security and Acceleration Server 2000. Учебный курс MCSE/Пер. с англ. — 2-е изд., испр. — М.: Издательско-торговый дом «Русская Редакция», 2003. — 400 *стр.:* ил.

ISBN 5–7502–0144–9

Этот учебный курс посвящен серверу Microsoft Internet Security and Acceleration Server 2000. Вы узнаете о его основных функциях и достоинствах, в том числе о планировании установки, развертывании, конфигурировании и сопровождении версии Enterprise Edition ISA-сервера. Подробно описаны настройка и конфигурирование ISA-сервера для работы в качестве брандмауэра и сервера кэширования, рассказано о том, как безопасно публиковать в Интернете серверы корпоративной сети, применять многоуровневую систему политик, использовать привратник H.323 Gatekeeper и создавать иерархии серверов. Отдельная глава посвящена мониторингу и устранению неполадок, кроме того, подробно описано большинство сообщений о событиях ISA-сервера.

Учебный курс предназначен специалистам поддержки, системным администраторам, квалифицированным пользователям и всем, кто хочет получить исчерпывающие знания в области планирования, развертывания, конфигурирования, мониторинга и устранения неполадок ISA-сервера. Помимо теоретического материала курс содержит упражнения и контрольные вопросы для самопроверки. Он поможет вам подготовиться к экзамену № 70-227: Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server, Enterprise Edition по программам сертификации MCSA (Microsoft Certified Systems Administrator) и MCSE (Microsoft Certified Systems Engeneer).

УДК 004.738.5
ББК 32.973.202

Подготовлено к изданию по лицензионному договору с Microsoft Corporation, Редмонд, Вашингтон. США. ActiveX, JScript, Microsoft, Microsoft Press. MSDN, MS-DOS, PowerPoint, Visual Basic, Visual C++, Visual InterDev, Visual SourceSafe, Visual Studio, Win32, Windows и Windows NT являются товарными знаками или охраняемыми товарными знаками корпорации Micro-soft в США и/или других странах. Все другие товарные знаки являются собственностью соответствующих фирм.

Все названия компаний, организаций и продуктов, а также имена лиц, используемые в примерах, вымышлены и не имеют никакого отношения к реальным компаниям, организациям, продуктам и лицам.

ISBN 0–7356–1347–8 (англ.)
ISBN 5-7502-0144-9

© Оригинальное издание на английском языке, Microsoft Corporation, 2001-2003
© Перевод на русский язык, Microsoft Corporation, 2001–2003
© Оформление и подготовка к изданию, издательско-торговый дом «Русская Редакция», 2003

Содержание

Об этой книге . . . . . **XIII**

Глава 1. Основные сведения о сервере Microsoft Internet Security and Acceleration Server 2000 . . . . . **1**

Занятие 1. Краткий обзор ISA-сервера 2
Две версии ISA-сервера 2
Роли ISA-сервера 3
Интеграция с Windows 2000 4
Масштабируемость 6
Расширяемость 7
Архитектура ISA-сервера 7
Практикум. Презентация, посвященная ISA-серверу 12
Резюме 12
Занятие 2. Брандмауэр на базе ISA-сервера 13
Методы фильтрации 13
Правила пропускной способности 17
Интегрированная поддержка VPN 17
Встроенные механизмы обнаружения вторжений 18
Безопасная публикация 19
Резюме 20
Занятие 3. Кэширование на ISA-сервере 21
Высокопроизводительный Web-кэш 21
Сервер прямого Web-кэширования 21
Сервер обратного Web-кэширования 22
Загрузка информации по расписанию 23
Активное кэширование 23
Протокол CARP и масштабируемость сервера кэширования 24
Иерархическое кэширование 25
Маршрутизация Web-прокси 25
Резюме 26
Занятие 4. Особенности управления ISA-сервером 27
Интуитивно понятный пользовательский интерфейс 27
Встроенные механизмы администрирования 27
Управление доступом на основе политик 28
Многоуровневая политика 29
Резюме 31
Закрепление материала 32

Глава 2. Установка сервера Microsoft Internet Security and Acceleration Server 2000 . . . . . **33**

Занятие 1. Планирование установки ISA-сервера 34
Планирование конфигурации оборудования и подключения 34
ISA-сервер в составе массива 37

Режимы работы ISA-сервера . . . 38
Подключение к Интернету . . . 39
ISA-сервер в сети . . . 39
ISA-сервер в сетях различной топологии . . . 40
Проекты, предполагающие публикацию в Web . . . 42
Проекты, предполагающие использование сервера Exchange . . . 43
Проекты, предполагающие использование сети периметра . . . 44
Резюме . . . 46
Занятие 2. Установка ISA-сервера . . . 47
Подготовка к установке ISA-сервера . . . 47
Таблица маршрутизации в Windows 2000 . . . 48
Установка ISA-сервера . . . 48
Процедура установки . . . 50
Создание таблицы локальных адресов . . . 52
Стандартные параметры ISA-сервера . . . 53
Устранение неполадок при установке ISA-сервера . . . 53
Практикум. Установка ISA Server Enterprise Edition . . . 54
Резюме . . . 57
Занятие 3. Переход от Proxy Server 2.0 . . . 58
Переход от Microsoft Proxy Server 2.0 . . . 58
Операционная система . . . 58
Массивы серверов Proxy Server 2.0 . . . 60
Переход к массиву . . . 60
Перенос конфигурации Proxy Server 2.0 . . . 61
Резюме . . . 63
Закрепление материала . . . 64

Глава 3. Настройка безопасного доступа в Интернет . . . 65
Занятие 1. Настройка доступа локальных клиентов в Интернет . . . 66
Клиенты ISA-сервера . . . 66
Изучение потребностей клиентов . . . 67
Настройка клиентов SecureNAT . . . 68
Разрешение имен для клиентов SecureNAT . . . 69
Клиенты брандмауэра . . . 70
Параметры приложений клиента брандмауэра . . . 71
Служба Web-прокси . . . 74
Практикум 1. Организация безопасного доступа в Интернет клиентов Web-прокси . . . 75
Практикум 2. Установка клиента брандмауэра . . . 77
Резюме . . . 77
Занятие 2. Настройка подключений ISA-сервера по телефонной линии . . . 78
Настройка подключений по телефонной линии . . . 78
Вызов по требованию . . . 79
Конфигурирование вызова по требованию . . . 80
Закрытие подключений . . . 82
Практикум. Настройка записи подключения по телефонной линии . . . 82
Резюме . . . 84

Занятие 3. Конфигурирование механизма автоматического обнаружения ISA-серверов . . . 85
Автоматическое обнаружение . . . 85
Практикум. Настройка автоматического обнаружения . . . 89
Резюме . . . 91
Занятие 4. Устранение неполадок, возникающих при подключении клиентов к ISA-серверу . . . 92
Устранение неполадок при подключении клиентов . . . 92
Устранение неполадок при подключении по телефонной линии . . . 94
Перезапуск служб после изменений в конфигурации . . . 95
Резюме . . . 96
Закрепление материала . . . 97

Глава 4. Конфигурирование безопасного доступа в Интернет с использованием политик доступа . . . 99
Занятие 1. Создание политик доступа на ISA-сервере . . . 101
Управление исходящими запросами . . . 101
Правила и аутентификация . . . 103
Системная безопасность ISA-сервера (блокировка изменений системной конфигурации) . . . 105
Мастер Getting Started . . . 105
Резюме . . . 106
Занятие 2. Создание элементов политики . . . 107
Элементы политики . . . 107
Настройка расписаний . . . 107
Настройка подмножеств адресатов . . . 109
Подмножества адресов клиентов . . . ПО
Пользователи и группы в качестве клиентов . . . 111
Настройка определений протоколов . . . 112
Настройка групп содержимого . . . 113
Практикум. Создание элементов политики . . . 115
Резюме . . . 116
Занятие 3. Настройка правил протоколов . . . 117
Правила протоколов . . . 117
Пример настройки правила протоколов . . . 118
Доступные протоколы . . . 119
Порядок выполнения правил . . . 120
Правила протоколов уровня массива и уровня предприятия . . . 120
Web-протоколы . . . 120
Определения протоколов, поставляемые в составе ISA-сервера . . . 121
Практикум. Применение правил протоколов к учетным записям пользователей . . . 123
Резюме . . . 126
Занятие 4. Настройка правил узлов и содержимого . . . 127
Правила узлов и содержимого . . . 127
Подмножества адресатов и обработка путей . . . 128
Правила узлов и содержимого уровня массива и уровня предприятия . . . 129
Группы содержимого . . . 130
Практикум. Создание правила узлов и содержимого . . . 134
Резюме . . . 136

Занятие 5. Настройка фильтров IP-пакетов . . . 137
Условия, когда необходимо применять фильтры IP-пакетов . . . 137
Создание фильтров IP-пакетов . . . 137
Настройка параметров фильтров пакетов . . . 140
Фильтрация IP-фрагментов . . . 141
Фильтрация параметров протокола IP . . . 141
Ведение журналов пакетов . . . 141
Практикум. Запуск служб Интернета на ISA-сервере . . . 142
Резюме . . . 146
Занятие 6. Настройка ISA-сервера на обнаружение внешних атак и вторжений . . . 147
Типы вторжений и оповещения . . . 147
Сканирование портов . . . 148
IP-атака без создания подключения (IP halfscan) . . . 148
Атака с обратной адресацией (Land attack) . . . 148
Атака «ping смерти» (Ping of Death) . . . 149
Атака «UDP-бомба» (UDPbomb) . . . 149
Атака передачи срочных данных в Windows (Windows out-of-band attack или WinNuke) . . . 149
Настройка обнаружения вторжений . . . 149
Практикум. Настройка обнаружения вторжений на ISA-сервере . . . 151
Резюме . . . 151
Закрепление материала . . . 152

Глава 5. Ускорение доступа в Интернет средствами кэширования ISA-сервера . . . 153
Занятие 1. Создание базовой политики кэширования . . . 154
Как работает механизм кэширования . . . 154
Обработка правил кэширования . . . 154
Процесс кэширования . . . 159
Фильтрация кэша . . . 160
Дополнительная политика кэширования . . . 161
Практикум. Кэширование динамического содержимого . . . 161
Резюме . . . 162
Занятие 2. Настройка конфигурации кэша ISA-сервера . . . 163
Конфигурирование дисков кэша . . . 163
Выбор порядка кэширования объектов . . . 165
Настройка политик, определяющих устаревшие объекты кэша . . . 166
Настройка активного кэширования . . . 170
Настройка кэширования отрицательных ответов . . . 171
Практикум 1. Включение активного кэширования . . . 171
Практикум 2. Настройка объема оперативной памяти для кэширования . . . 172
Резюме . . . 172
Занятие 3. Загрузка содержимого кэша по расписанию . . . 173
Загрузка содержимого кэша по расписанию . . . 173
Практикум. Создание задания загрузки содержимого по расписанию . . . 176
Резюме . . . 177
Закрепление материала . . . 178

Глава 6. Безопасная публикация серверов . . . 179
Занятие 1. Особенности безопасной публикации серверов . . . 180
Правила политики публикации . . . 180
Правила публикации серверов . . . 180
Механизм публикации серверов . . . 181
Действия для правил публикации серверов . . . 182
Подмножества адресов клиентов . . . 183
Правила публикации серверов и фильтры IP-пакетов . . . 183
Практикум. Публикация внутреннего сервера . . . 184
Резюме . . . 186
Занятие 2. Безопасная публикация Web-серверов . . . 187
Правила Web-публикации . . . 187
Подмножества адресатов и клиентов . . . 187
Действия для правил Web-публикации . . . 188
SSL- и HTTP-сопряжение . . . 189
Порядок выполнения правил . . . 190
Пример создания правила Web-публикации . . . 191
Публикация Web-сервера, расположенного в локальной сети . . . 191
Публикация Web-сервера, расположенного на ISA-сервере . . . 192
Использование фильтров IP-пакетов для публикации Web-сервера, совмещенного с ISA-сервером . . . 192
Практикум. Публикация Web-сервера, расположенного на компьютере ISA-сервера . . . 193
Резюме . . . 195
Занятие 3. Публикация почтового сервера . . . 196
Мастер Mail Server Security . . . 196
Практикум. Публикация службы SMTP . . . 198
Резюме . . . 201
Закрепление материала . . . 202

Глава 7. Обеспечение безопасности сети предприятия средствами ISA-сервера . . . 203
Занятие 1. Применение политики предприятия . . . 204
Политики предприятия и массивы . . . 204
Настройка параметров политики предприятия . . . 205
Архивирование и восстановление конфигурации предприятия . . . 208
Практикум. Создание и применение политики предприятия . . . 209
Резюме . . . 212
Занятие 2. Настройка массивов ISA-серверов . . . 213
Создание массивов ISA-серверов . . . 213
Выдвижение изолированных серверов в члены массива . . . 214
Параметры членов массива . . . 215
Хранение конфигурации массива . . . 216
Управление членством в массиве . . . 216
Архивирование и восстановление конфигурации массива . . . 217
Восстановление конфигурации . . . 218
Обеспечение отказоустойчивости в массивах . . . 219
Протокол CARP . . . 220
Настройка протокола CARP . . . 221
Резюме . . . 223

Занятие *3.* Обеспечение безопасности виртуальных частных сетей средствами ISA-сервера . . . 224
Интеграция виртуальных частных сетей с ISA-серверами . . . 224
Настройка сети для использования VPN . . . 225
Использование мастеров конфигурации VPN . . . 225
Изменение конфигурации VPN . . . 226
ISA-сервер и IPSec . . . 227
Пример крупной сети с VPN и маршрутизацией . . . 227
Выполнение требований к сети . . . 228
Резюме . . . 231
Закрепление материала . . . 232

Глава 8. Безопасные видеоконференции с применением привратника **H.323** Gatekeeper . . . 233
Занятие 1. Настройка клиентов для использования привратника H.323 Gatekeeper . . . 234
Протокол H.323 . . . 234
Привратник H.323 Gatekeeper . . . 234
Примеры использования H.323 Gatekeeper . . . 235
Регистрация клиентов на H.323 Gatekeeper . . . 237
Атрибуты конечных точек . . . 238
Псевдонимы . . . 238
Преобразование адресов клиентов . . . 239
Установка привратника H.323 Gatekeeper . . . 240
Практикум. Настройка клиента для использования H.323 Gatekeeper . . . 24!
Резюме . . . 243
Занятие 2. Маршрутизация вызовов конференций средствами H.323 Gatekeeper . . . 244
Правила маршрутизации вызовов . . . 244
Правила IP-адресов . . . 247
Правила адресов электронной почты . . . 247
Обработка правил и адресаты . . . 249
Применение правил к запросам . . . 252
Резюме . . . 254
Закрепление материала . . . 255

Глава 9. Контроль и оптимизация производительности ISA-сервера . . . 257
Занятие 1. Настройка оповещений . . . 258
Предустановленные оповещения . . . 258
Условия возникновения оповещения . . . 259
Местоположение события . . . 260
Порог инициирования оповещения . . . 260
Действия, выполняемые в ответ на оповещение . . . 261
События ISA-сервера . . . 263
Практикум. Настройка оповещения для отправки сообщения по электронной почте . . . 265
Резюме . . . 265
Занятие 2. Ведение журнала работы ISA сервера . . . 267
Управление журналами ISA-сервера . . . 267
Запись в файл . . . 269

Формат W3C . . . 269
Формат ISA . . . 270
Имена файлов журналов . . . 270
Параметры ведения файлов журнала . . . 271
Запись журналов в базу данных . . . 271
Запись в журнал информации о пакетах . . . 273
Поля записей в журналах брандмауэра и Web-прокси . . . 274
Поля записей в журналах фильтров пакетов . . . 280
Практикум. Изучение журналов Web-прокси . . . 281
Резюме . . . 282
Занятие 3. Создание отчетов ISA-сервера . . . 283
Конфигурирование отчетов . . . 283
Просмотр отчетов . . . 283
Конфигурирование заданий по созданию отчетов . . . 285
Учетные записи для создания отчетов . . . 287
Конфигурирование сводок журналов . . . 287
База данных для хранения отчетов . . . 288
Практикум. Создание и просмотр отчетов . . . 289
Резюме . . . 291
Занятие 4. Управление пропускной способностью . . . 292
Понятие фактической пропускной способности . . . 292
Конфигурирование приоритетов пропускной способности . . . 294
Конфигурирование правил пропускной способности . . . 2%
Порядок применения правил пропускной способности . . . 297
Правило пропускной способности, применяемое по умолчанию . . . 298
Практикум. Создание правила пропускной способности . . . 298
Резюме . . . 299
Занятие 5. Дополнительные средства настройки и наблюдения . . . 300
Повышение производительности ISA-сервера . . . 300
Повышение производительности кэша . . . 301
Объекты и счетчики производительности ISA-сервера . . . 302
Оснастка ISA Server Performance Monitor . . . 303
Резюме . . . 316
Закрепление материала . . . 317

Глава 10. Устранение неполадок в работе ISA-сервера . . . 319
Занятие 1. Средства выявления неполадок в работе ISA-сервера . . . 320
Средства устранения неполадок . . . 320
Таблицы маршрутизации . . . 324
Практикум. Определение состояния портов . . . 326
Резюме . . . 328
Занятие 2. Методики выявления неполадок в работе ISA-сервера . . . 329
Устранение неполадок пользовательского доступа . . . 329
Устранение неполадок пакетного уровня . . . 330
Перечень типичных неполадок и способы их устранения . . . 332
Резюме . . . 336
Закрепление материала . . . 337

Приложение А Вопросы и ответы 338

Приложение Б Развертывание и администрирование ISA-сервера в сложных сетях 354

Предметный указатель 361

Об этой книге

Мы рады представить вам учебный курс MCSA/MCSE «Microsoft Internet Security and Acceleration Server 2000». В нем изложены принципы установки и конфигурирования Microsoft Internet Security and Acceleration Server 2000, или *ISA-сервера,* используемого в качестве брандмауэра и сервера Web-кэширования уровня предприятия. В первых занятиях книги описаны основные функции и достоинства ISA-сервера, а также порядок планирования его установки и развертывания. Далее рассказано о том, как настраивать разные функции ISA-сервера, в том числе брандмауэр, кэширование, публикацию, многоуровневые политики и параметры привратника H.323 Gatekeeper. В последней главе рассматриваются методики наблюдения и устранения неполадок ISA-сервера.

Главы состоят из занятий. Большинство занятий содержат упражнения, предназначенные для демонстрации излагаемых методов и приобретения практических навыков. Каждая глава заканчивается контрольными вопросами по материалам главы. В некоторых вопросах смоделированы ситуации, которые вам предлагается разрешить. Отвечая на вопросы, вы сможете оценить уровень полученных знаний и степень усвоения материала главы.

В разделе «С чего начать» (см. далее) даны важные инструкции по установке и настройке ISA-сервера для выполнения заданий данного курса, а также представлена информация о сетевой конфигурации, в которой выполняются практические задания курса. Внимательно ознакомьтесь с содержанием этого раздела прежде, чем приступать к их выполнению.

Кому адресована эта книга

Данный курс предназначен специалистам в области информационных технологий:

- специалистам поддержки (системным администраторам, специалистам по технической поддержке среднего звена, консультантам);
- квалифицированным пользователям и всем, кто хочет получить исчерпывающие знания в области планирования, развертывания, конфигурирования, мониторинга и устранения неполадок ISA-сервера;
- тем, кто планирует сдать сертификационный экзамен 70-227: *Installing, Configuring and Administering Microsoft Internet Security and Acceleration (ISA) Server, Enterprise Edition.*

Требования к читателям

Для успешного изучения материала и понимания концепций и задач, изложенных в учебном курсе, требуется предварительная подготовка. Как минимум, необходимы:

- по крайней мере годичный опыт администрирования сетевых операционных систем, в том числе не менее полугодового опыта работы с сетями Windows 2000;
- хорошее знание таких элементов инфраструктуры TCP/IP, как DNS, шлюзы, подсети и таблицы маршрутизации;

- хорошее знание таких элементов инфраструктуры Windows 2000, как Active Directory, служба Routing and Remote Access (Маршрутизация и удаленный доступ), Performance Monitor (Производительность), служба Quality of Service (QoS) и консоль Microsoft Management Console (MMC).

Справочные материалы

- Материалы по ISA-серверу, доступные на официальном Web-узле ISA-сервера по адресу *http://www.microsoft.com/isaserver.*
- Материалы Microsoft TechNet, доступные ежемесячно на компакт-диске или в интерактивном режиме на Web-узле Microsoft по адресу *http://www.microsoft.com/technet.*
- Материалы MCP Magazine Online, доступные на Web-узле по адресу *http://www.mcpmag.com.*
- Книга Томаса Ли (Thomas Lee) и Джозефа Дейвиса (Joseph Davies) «Windows 2000 TCP/IP Protocols and Services Technical Reference», Microsoft Press, 2000.

Компакт-диск с дополнительными материалами к курсу

На компакт-диске, прилагаемом к книге, хранятся:

- вспомогательные материалы по курсу, а также 120-дневная пробная версия ISA-сервера. Подробнее о содержании компакт-диска — в разделе «С чего начать» далее;
- электронный вариант этой книги на английском языке с возможностью полнотекстового поиска. Подробнее об электронной версии книги — в разделе «Электронный вариант книги» далее;
- файлы, необходимые для выполнения практикумов. Они содержат мультимедийную демонстрацию возможностей ISA-сервера, а также информацию, используемую в процессе выполнения заданий. Их можно загружать либо непосредственно с компакт-диска, либо предварительно скопировав на жесткий диск;
- приложение к книге, содержащее описание сообщений о событиях, которые происходят при работе ISA-сервера;
- словарь терминов, содержащий определения терминов, применяемых в этом курсе.

Структура книги

- Каждая глава начинается с раздела «В этой главе», содержащего краткий обзор обсуждаемых тем.
- Главы состоят из занятий и практикума. Упражнения из занятий обозначаются значком на полях.
- Каждую главу завершает раздел «Закрепление материала», вопросы которого помогут вам проверить, насколько твердо вы усвоили материал.

В приложении А «Вопросы и ответы» собраны вопросы ко всем главам книги и ответы для самопроверки.

Примечания

Практически во всех главах встречаются примечания разных видов.

- **Совет** — поясняет возможный результат или описывает альтернативный метод решения задачи.

- **Внимание!** — предупреждает вас о возможной потере данных или содержит сведения, необходимые для выполнения поставленной задачи.
- **Примечание** — содержит дополнительную информацию.

Обозначения

В этом разделе описаны обозначения, используемые в книге.

Графические обозначения

- *Курсивом* выделяются важные термины, положения и другие существенные сведения, после которых, как правило, указан их английский эквивалент.
- Имена файлов, папок и каталогов начинаются с прописных букв (за исключением имен, которые вы задаете сами).
- Расширения имен файлов набраны строчными буквами.
- Аббревиатуры обозначаются ЗАГЛАВНЫМИ БУКВАМИ.
- Примеры кода, текста, выводимого на экран и вводимого в командной строке, набраны моноширинным шрифтом.
- Необязательные элементы операторов заключены в скобки []. Например, [*имя_файла*] в синтаксисе команды означает, что после команды можно указать имя файла. Сами скобки вводить НЕ надо.
- Обязательные элементы операторов заключены в фигурные скобки {}. Сами скобки вводить НЕ надо.
- Значками на полях помечены конкретные разделы.

Значок	Описание
	Файл, хранящийся на компакт-диске, прилагаемом к книге. Часть файлов необходима для выполнения практических заданий, другие содержат дополнительную информацию по обсуждаемой теме. В тексте рассказывается о назначении и местоположении соответствующего файла
	Упражнение или практикум, выполняя который вы приобретете необходимые навыки
	Вопросы, отвечая на которые вы проверите, насколько твердо и безошибочно усвоили изложенный материал. Вопросы обычно содержатся в разделе «Закрепление материала» в конце главы, ответы для самопроверки — в приложении А «Вопросы и ответы»

Клавиатура

- Знак «+» между названиями клавиш означает, что их следует нажать одновременно. Например, выражение «Нажмите Alt+Tab» обозначает, что нужно нажать клавишу Tab, удерживая нажатой клавишу Alt.
- Запятая между названиями клавиш означает их последовательное нажатие. Например, выражение «Нажмите Alt, F, X» означает, что надо последовательно нажать и отпустить указанные клавиши. Если же указано «Нажмите Alt+W, L», то вам придется сначала нажать клавиши Alt и W вместе, потом отпустить их и нажать клавишу L.
- Команды меню можно выбирать с клавиатуры. Для этого нажмите клавишу Alt (чтобы активизировать меню), а затем последовательно — выделенные или подчеркнутые буквы в названиях нужных вам разделов меню или команд. Кроме того, некоторым командам сопоставлены клавиатурные сокращения (они указаны в меню).

- Флажки и переключатели также можно устанавливать и сбрасывать посредством клавиатуры. Для этого достаточно нажать Alt, а затем клавишу, соответствующую подчеркнутой букве в названии флажка или переключателя. Кроме того, нажимая клавишу Tab, вы можете сделать зону нужного параметра активной, а затем установить или снять выбранный флажок или переключатель, нажав клавишу «пробел».
- Работу с диалоговым окном всегда можно прервать, нажав клавишу **ESC.**

Обзор глав и приложений

Материал этого учебного курса поможет вам научиться устанавливать, конфигурировать и внедрять ISA-сервер. Конечно, учебный курс предназначен для последовательного изучения, однако вы можете работать с ним так, как вам удобно, скажем, проштудировать лишь отдельные главы. Советуем в этом случае обращать внимание на раздел «Прежде всего» в начале каждой главы, где указаны предварительные требования для выполнения практических заданий.

Во вводной главе собраны сведения о содержании книги и данные о структурных единицах и условных обозначениях, принятых в ней. Внимательно прочитайте эту главу — это поможет вам эффективнее работать с материалами курса, а также выбрать интересующие вас темы.

Далее кратко описаны главы и приложения учебного курса.

В главе 1 «Основные сведения о сервере Microsoft Internet Security and Acceleration Server 2000» рассказано об основных особенностях и возможностях ISA-сервера.

В главе 2 «Установка сервера Microsoft Internet Security and Acceleration Server 2000» описано, как устанавливать ISA-сервер, в том числе как планировать установку и переход от Proxy Server 2.0.

В главе 3 «Настройка безопасного доступа в Интернет» вы узнаете, как обеспечивать безопасный доступ в Интернет клиентов ISA-сервера. Кроме того, здесь рассказано об установке и конфигурировании клиентов брандмауэра и клиентов SecureNAT, о конфигурировании автоматического обнаружения серверов, о конфигурировании доступа в Интернет по телефонной лини, а также об устранении неполадок подключения к Интернету.

Глава 4 «Конфигурирование безопасного доступа в Интернет с использованием политик доступа» посвящена созданию пользовательских безопасных политик доступа в Интернет, в том числе таких элементов политики, как расписания и подмножества адресатов, которые в дальнейшем применяются в правилах узлов и содержимого или правилах протоколов. Здесь рассказывается, как создавать правила, обеспечивающие полный контроль над входящим и исходящим сетевым трафиком. Отдельное занятие посвящено механизму фильтрации пакетов ISA-сервера и его применению в соответствии с требованиями к сети. В последнем занятии рассказывается о настройке механизма обнаружения вторжений.

Глава 5 «Ускорение доступа в Интернет средствами кэширования ISA-сервера» посвящена использованию ISA-сервера в качестве средства ускорения доступа клиентов в Интернет. Подробно рассказано о конфигурировании свойств кэша, об активном кэшировании и загрузке информационного наполнения по расписанию.

В главе 6 «Безопасная публикация серверов» рассказано о безопасной публикации в Интернете серверов, расположенных в сети, защищенной ISA-сервером. В частности, описана публикация Web-серверов, почтовых серверов и FTP-серверов.

В главе 7 «Обеспечение безопасности сети предприятия средствами ISA-сервера» объясняется, как развертывать ISA-сервер в более сложных корпоративных сетях, в том числе в сетях с виртуальными частными сетями и централизованной многоуровневой политикой.

Глава 8 «Безопасные видеоконференции с применением привратника H.323 Gatekeeper» посвящена развертыванию ПО для поддержки видеоконференций в сетях с ISA-сервером. Здесь рассказывается об использовании привратника H.323 Gatekeeper в качестве центрального коммутатора вызовов видеоконференций и о создании правил для маршрутизации вызовов по псевдонимам абонентов.

В главе 9 «Контроль и оптимизация производительности ISA-сервера» описано, как пользоваться различными инструментальными средствами ISA-сервера для наблюдения за ним и оптимизации его работы. Здесь также рассказывается о конфигурировании оповещений, использовании журналов и отчетов ISA-сервера, о настройке правил пропускной способности, а также о работе со счетчиками производительности ISA-сервера.

Из главы 10 «Устранение неполадок в работе ISA-сервера» вы узнаете об инструментальных средствах и стратегиях, применяемых для устранения неполадок в работе ISA-сервера.

В приложении А «Вопросы и ответы» приведены ответы для самопроверки на вопросы из упражнений и разделов «Закрепление материала» всех глав учебного курса.

В приложении Б «Развертывание и администрирование ISA-сервера в сложных сетях» показано несколько примеров установки версии Enterprise Edition ISA-сервера в сложных сетях. Используйте их, чтобы проверить, как вы усвоили материал курса и научились устранять неполадки. Мы настоятельно рекомендуем изучить это приложение тем, кто собирается сдавать экзамен 70-227, так как, чтобы его успешно выдержать, необходимо не только знать программный продукт, но и уметь устранять неполадки.

Приложение В «Сообщения о событиях» в русском издании помещено на компакт-диск, прилагаемый к книге. В нем содержится перечень всех сообщений о событиях ISA-сервера, а также их описание. Кроме того, здесь рассказано, какие ответные действия следует предпринимать в том или ином случае.

Четвертое приложение из оригинального издания — «Словарь терминов» — в русском издании также помещено на компакт-диск, прилагаемый к книге. В словаре вы найдете определения терминов, которые помогут вам работать с данной книгой.

С чего начать

Данный курс предназначен для самостоятельного изучения, поэтому вы можете пропускать занятия, материал которых вам знаком. И все же помните, что для выполнения упражнений в большинстве случаев требуются результаты упражнений предыдущих глав. Чтобы помочь вам определить, с чего начать изучение курса, мы предлагаем следующую таблицу.

Если вы	Что делать
Готовитесь к сдаче сертификационного экзамена 70-227: *Installing, Configuring, and Administering Microsoft Internet Security and Acceieration (ISA) Server, Enterprise Edition*	См. раздел «Начало работы», а также описание процедур установки далее в этой главе. Затем изучите материал всех глав этой книги
Хотите изучить определенные темы для сдачи экзамена	См. раздел «Материалы для подготовки к экзаменам»

Материалы для подготовки к экзаменам

Далее перечислены темы сертификационного экзамена 70-227: *Installing, Configuring, and Administering Microsoft Internet Security and Acceleration (ISA) Server, Enterprise Edition* и главы настоящего учебного курса, где обсуждаются соответствующие вопросы.

Примечание Конкретная программа любого экзамена определяется Microsoft и может быть изменена без предварительного уведомления.

Установка ISA-сервера

Тема	Где обсуждается
Предварительное конфигурирование сетевых интерфейсов	Глава 2, занятие 2
Проверка подключения к Интернету перед установкой ISA-сервера	Глава 2, занятие 2
Проверка разрешения имен системой DNS	Глава 2, занятие 2
Установка ISA-сервера в режиме брандмауэра, сервера кэширования или в смешанном режиме	Глава 2, занятие 1 Глава 2, занятие 2
Создание и изменение таблицы локальных сервера кэширования	Глава 2, занятие 2
Определение и настройка необходимого объема кэша	Глава 2, занятие 1 Глава 2, занятие 2 Глава 5, занятие 2
Установка ISA-сервера в качестве члена массива	Глава 2, занятие 2 Глава 7, занятие 2
Обновление Microsoft Proxy Server 2.0 до ISA-сервера	Глава 2, занятие 3
Архивирование конфигурации Proxy Server 2.0	Глава 2, занятие 3
Устранение неполадок при установке ISA-сервера	Глава 2, занятие 2

Конфигурирование и устранение неполадок в работе служб ISA-сервера

Тема	Где обсуждается
Конфигурирование и устранение неполадок исходящего доступа в Интернет	Глава 3 ,занятие 4
Конфигурирование ролей ISA-сервера	Глава 6, занятие 1 Глава 6, занятие 2 Глава 6, занятие 3
Конфигурирование ISA-сервера для Web-публикации	Глава 6, занятие 2
Конфигурирование ISA-сервера в качестве прокси-сервера	Глава 3, занятие 1 Глава 5, занятие] Глава 5, занятие 2
Конфигурирование ISA-сервера для публикации серверов	Глава 6, занятие I Глава 6, занятие 3
Конфигурирование привратника H.323 Gatekeeper для поддержки аудио- и видеоконференций	Глава 8, занятие 1 Глава 8, занятие 2
Настройка правил привратника, в том числе телефонов, электронной почты и протокола IP	Глава 8, занятие 2
Настройка адресатов привратника средствами мастера Add Destination Wizard	Глава 8, занятие 2
Настройка и устранение неполадок подключений по телефонной линии и вызовов по требованию службы Routing and Remote Access (Маршрутизация и удаленный доступ)	Глава 3, занятие 4 Глава 10, занятие 2

Тема	Где обсуждается
Настройка и устранение неполадок правил маршрутизации для статических IP-маршрутов в службе Routing and Remote Access (Маршрутизация и удаленный доступ)	Глава 5, занятие I Глава 10, занятие 1
Настройка и устранение неполадок доступа по виртуальным частным сетям (VPN)	Глава 7, занятие 3 Глава 10, занятие 2
Конфигурирование ISA-сервера в качестве конечной точки VPN-туннеля без помощи мастера **VPN** Wizard	Глава 7, занятие 3 Глава 10, занятие 2
Конфигурирование сквозного VPN-туннеля через ISA-сервер	Глава 7, занятие 3 Глава 10, занятие *2*
Конфигурирование масштабирования множества ISA-серверов средствами службы балансировки сетевой нагрузки (Network Load Balancing, NLB) и протокола Cache Array Routing Protocol (CARP)	Глава 7, занятие 2

Конфигурирование, управление и устранение неполадок в работе политик и правил

Тема	Где обсуждается
Конфигурирование и обеспечение безопасности брандмауэров в соответствии с корпоративными требованиями	Глава 4, занятие 1
Конфигурирование фильтров пакетов для различных уровней безопасности системы, в том числе блокировка изменений системной конфигурации	Глава 4, занятие 1 Глава 4, занятие 5
Создание и конфигурирование политик доступа и пропускной способности	Глава 9, занятие 4
Создание и конфигурирование правил узлов и содержимого для ограничения доступа в Интернет	Глава 4, занятие 4
Создание и конфигурирование правил протоколов для управления доступом в Интернет	Глава 4, занятие 3
Создание и конфигурирование правил маршрутизации для ограничения доступа в Интернет	Глава 5, занятие I
Создание и конфигурирование правил пропускной способности для ограничения доступа в Интернет	Глава 9, занятие 4
Устранение неполадок доступа	Глава 10, занятие 1
Устранение неполадок доступа на уровне пользователей	Глава 10, занятие 2
Устранение неполадок доступа на уровне пакетов	Глава 10, занятие 2
Создание новых элементов политики, в том числе расписаний, приоритетов пропускной способности, подмножеств адресатов, подмножеств адресов клиентов, определений протоколов и групп содержимого	Глава 4, занятие 2
Управление массивами ISA-серверов на предприятии	Глава 7, занятие I Глава 7, занятие 2
Создание массивов прокси-серверов	Глава 7, занятие 2
Определение политики уровня предприятия в массиве	Глава 7, занятие 1

Развертывание, конфигурирование и устранение неполадок в работе клиентов

Тема	Где обсуждается
Планирование развертывания клиентских компьютеров для использования служб ISA-сервера с учетом аутентификации клиентов, клиентских операционных систем, сетевой топологии, затрат, сложности и функций клиентов	Глава 2, занятие 1
Конфигурирование и устранение неполадок клиентов SecureNAT	Глава 3, занятие 1 Глава 3, занятие 4
Установка программного обеспечения клиента брандмауэра с учетом затрат и сложности развертывания	Глава 3, занятие 1
Устранение неполадок автоматического брандмауэра	Глава 3, занятие 2
Конфигурирование Web-браузера на клиентских компьютерах для использования ISA-сервера в качестве HTTP-прокси	Глава 3, занятие 1

Наблюдение, управление и анализ использования ISA-сервера

Тема	Где обсуждается
Наблюдение за безопасностью и использование сети средствами механизма ведения журналов и оповещений	Глава 9, занятие 1 Глава 9, занятие 2
Конфигурирование обнаружения вторжений	Глава 4, занятие 6
Конфигурирование оповещения с отправкой администратору сообщения по электронной почте	Глава 9, занятие 1
Автоматизация конфигурирования оповещений	Глава 9, занятие 1
Наблюдений за состоянием оповещений	Глава 9, занятие 1 Глава 10, занятие 1
Устранение неполадок с безопасностью и использованием сети	Глава 10, занятие 1
Определение подключений средствами утилиты Netstat	Глава 10, занятие 1
Проверка состояния внешних портов средствами утилит Telnet и Network Monitor	Глава 10, занятие 1
Анализ производительности ISA-сервера с помощью отчетов, в том числе сводных отчетов и отчетов об использовании Web, использовании приложений, трафика, а также сети и безопасности	Глава 9, занятие 3
Оптимизация производительности ISA-сервера с учетом планирования мощностей, определения приоритетов и анализа тенденций	Глава 2, занятие 1 Глава 9, занятие 5
Анализ производительности ISA-сервера средствами оснастки Performance Monitor	Глава 9, занятие 5
Анализ производительности ISA-сервера на основании отчетов и журналов	*Глава 9,* занятие 2 Глава 9, занятие 3
Управление использованием оперативной памяти ISA-сервера для кэширования	Глава 9, занятие 5

Начало работы

Данный курс предназначен для самостоятельного изучения и содержит упражнения и практические рекомендации, которые помогут вам получить навыки работы с ISA-сервером. Для выполнения большинства заданий нужны два компьютера под управлением Windows 2000 Server с пакетом исправлений Service Pack 1, объединенные сетью.

Аппаратное обеспечение

Компьютеры должны соответствовать приведенной далее минимальной конфигурации, а установленное на них оборудование необходимо выбрать из списка совместимого оборудования Microsoft Windows 2000 Professional Hardware Compatibility List:

- компьютер с процессором PentiumII с частотой не менее 300 МГц под управлением Microsoft Windows 2000 Server или Windows 2000 Advanced Server с пакетом исправлений Service Pack 1 или более поздним;
- не менее 256 Мбайт оперативной памяти;
- жесткий диск с разделом NTFS размером не менее 2 Гбайт;
- 200 Мбайт свободного пространства на диске после установки операционной системы;
- сетевой адаптер для подключения к внутренней сети;
- модем для доступа в Интернет;
- привод CD-ROM;
- звуковая карта и устройство воспроизведения звука;
- мышь Microsoft или другое совместимое указательное устройство.

Программное обеспечение

Для выполнения упражнений и практикумов данного курса необходимо следующее программное обеспечение:

- Windows 2000 Server (пакет исправлений Service Pack 1 или более поздний);
- 120-дневная пробная версия ISA-сервера (Microsoft Internet Security and Acceleration Server 2000, Enterprise Edition) — ее вы найдете на прилагаемом к книге компакт-диске.

Внимание! Прилагаемая к данному курсу 120-дневная пробная версия не предназначена для продажи и предлагается исключительно для ознакомления. Поддержка этой версии не предоставляется. Подробнее о данной книге и прилагаемом компакт-диске (в том числе ответы на часто задаваемых вопросы) — на Web-узле технической поддержки Microsoft Press Technical Support *http://mspress.microsoft.com/support*. Если вы все же захотите задать вопросы или поделиться своими предложениями или комментариями, обращайтесь в издательство Microsoft Press по одному из указанных далее адресов:

электронная почта: TKINPUT@MICROSOFT.COM,

почтовый адрес: Microsoft Press, Attn:MCSE Training Kit — Microsoft Windows 2000 Professional Editor, One Microsoft Way, Redmond, WA 98052-6399.

Подготовка компьютера к выполнению практических заданий

Многие практические задания данного курса выполняются на двух компьютерах в сети Ethernet. Для выполнения упражнений необходимо настроить сеть в соответствии с приведенными далее указаниями.

На первом компьютере установите сетевой адаптер и внешний модем, подключений к работающей телефонной линии. Компьютеру назначьте имя Server1 и сконфигурируйте

его как контроллер домена domain01.local. Сетевому адаптеру сервера Server1 присвойте IP-адрес 192.168.0.1/24. Не определяйте основной шлюз для внешнего интерфейса, в качестве основного DNS-сервера назначьте работающий внешний сервер в Интернете, а в качестве альтернативного DNS-сервера — 192.168.0.1. Кроме стандартных компонентов, на Server1 следует установить Management and Monitoring Tools (Средства управления и наблюдения) и Windows Media Services (Службы Windows Media). Прежде чем устанавливать ISA-сервер, как описано в главе *2,* подключитесь с сервера к провайдеру и проверьте работоспособность доступа в Интернет.

После установки на Server1 операционной системы Windows 2000 установите и сконфигурируйте службу каталогов Active Directory в соответствии с приведенными далее инструкциями.

Установите сервер в качестве первого контроллера домена в новом лесе:

- имя нового домена и леса — domain01.local;
- NetBIOS-имя нового домена — DOMAIN01;
- местоположение базы данных Active Directory — C:\WINNT\NTDS;
- местоположение журналов Active Directory — C:\WINNT\NTDS;
- местоположение папки Sysvol — C:\WINNT\SYSVOL;
- DNS устанавливается и конфигурируется автоматически;
- в домене следует использовать разрешения, совместимые с серверами, предшествующими Windows 2000 [то есть следует установить флаг **Pre-Windows 2000 compatible permissions** (Разрешения, совместимые с серверами пред-Windows 2000)]. В этом случае возможен анонимный доступ к доменной информации;
- Active Directory устанавливается для домена domain01.local;
- контроллер домена размещается в сайте Default-First-Site-Name. Управление сайтами осуществляется средствами оснастки Active Directory Sites and Services (Active Directory — сайты и службы)

Завершив конфигурирование сервера Server1, установите Windows 2000 на втором компьютере. На нем достаточно установить сетевой адаптер, подключенный к локальной сети. Компьютеру следует назначить имя Server2 и сконфигурировать в качестве рядового сервера в домене Domain01. Серверу Server2 присвойте IP-адрес 192.168.0.2/24, а в качестве основного шлюза укажите адрес 192.168.0.1. В качестве основного (предпочитаемого) DNS-сервера назначьте работающий внешний сервер в Интернете, а в качестве альтернативного DNS-сервера — 192.168.0.1. Кроме стандартных компонентов на Server2 следует установить Management and Monitoring Tools (Средства управления и наблюдения), Networking Services (Сетевые службы) и Windows Media Services (Службы Windows Media).

Примечание Если настраиваемые компьютеры являются частью большей сети, вы *должны* проконсультироваться с системным администратором, чтобы избежать конфликтов некоторых параметров — имен компьютеров, доменов и других свойств ISA-сервера, описанных в главах 2 и 3. Если предлагаемые в курсе параметры нельзя применять в сети, договоритесь *с* администратором о предоставлении альтернативных имен и других параметров и используйте при выполнении заданий курса именно их.

Электронный вариант книги

На компакт-диске, прилагаемом к книге, находится электронный вариант оригинального издания этого учебного курса, который доступен для просмотра при наличии Microsoft Internet Explorer 5.0 или более поздней версии.

Установка электронной версии книги

1. Вставьте компакт-диск, прилагаемый к книге, в привод CD-ROM.
2. Выберите к меню **Start** (Пуск) команду Run (Выполнить) и введите команду **D:\Ebook\Autorun.exe**, где D: — это имя вашего привода CD-ROM.

   Ярлык электронного варианта книги будет размещен на рабочем столе.
3. Щелкните кнопку **OK**, чтобы завершить работу мастера Installation Wizard.

Примечание Электронная **версия книги доступна только с компакт-диска.**

Программа сертификации специалистов Microsoft

Программа сертификации специалистов Microsoft (Microsoft Certified Professional, MCP) — отличная возможность подтвердить ваши знания современных технологий и программных продуктов этой фирмы. Лидер отрасли в области сертификации — Microsoft разработала современные методы тестирования. Экзамены и программы сертификации подтвердят вашу квалификацию разработчика или специалиста по реализации решений на основе технологий и программных продуктов Microsoft. Сертифицированные Microsoft профессионалы квалифицируются как эксперты и высоко ценятся на рынке труда.
Подробнее о программах сертификации Microsoft — на странице *http://www.tnicrosqft.com/nK/mcp.*

Преимущества программы сертификации Microsoft

Программа сертификации Microsoft — один из самых строгих и полных тестов оценки знаний и навыков в области проектирования, разработки и сопровождения программного обеспечения. Звание сертифицированного специалиста Microsoft присваивается лишь тому, кто демонстрирует умение решать конкретные задачи, применяя продукты компании. Программа тестирования позволяет не только оценить квалификацию специалиста, но и служит ориентиром для всех, кто стремится достичь современного уровня знаний в этой области. Как и любой другой тест или экзамен, сертификация Microsoft служит критерием определенного уровня знаний специалиста, что важно как при трудоустройстве, так и для карьерного роста в организации.

Для специалистов. Звание Microsoft Certified Professional дает следующие преимущества:

- **официальное признание знаний и опыта работы** с продуктами и технологиями Microsoft;
- **подписка на MSDN.** MCP получает скидку на годовую подписку на Microsoft Developer Network *(msdn.microsoft.com/subscriptions)* в первый год после сертификации. (Конкретные условия зависят от региона. Подробнее — в Welcome Kit.) Размер скидки при приобретении библиотеки MSDN Library составляет 50 долларов США;
- **доступ к технической информации о продуктах Microsoft в защищенной области Web-узла MCP.** Для этого следует открыть страницу по адресу *http://www.microsoft.com/trainingand-services*, развернуть узел **Certification** и щелкнуть ссылку For MCPs Only;
- **эксклюзивные скидки на продукты и услуги различных компаний.** Подробнее об этом — на Web-странице по адресу *http://www.microsoft.com/trainingandservices*Разверните узел **Certification,** щелкните ссылку **For MCPs Only** и далее — ссылку **Other Benefits;**
- **эмблемы, сертификат, отчет об экзамене, карточка для бумажника и значок, свидетельствующие о присвоении звания Microsoft Certified Professional.** После того как вы успешно выдержите экзамен, вы получите право загрузить электронные копии эмблемы и отчета об экзамене с защищенной области Web-узла MCP. Для этого следует открыть страницу по адресу *http://www.microsoft.com/trainingandservices*развернуть узел **Certification** и щелкнуть ссылку **For MCPs Only;**

- приглашения на конференции, семинары и мероприятия, предназначенные для специалистов Microsoft;
- **бесплатный доступ к онлайновому журналу «Microsoft Certified Professional Magazine Online».** На зашищенной части Web-узла этого журнала расположены: свежий выпуск журнала (доступен только для MC'P), дополнительные, доступные только в интерактивном режиме материалы и колонки, база данных только для MCP и регулярные онлайновые чаты со специалистами Microsoft и другими техническими экспертами.

Кроме того, специалисты Microsofi Certified System Engineer получают дополнительное преимущество:

- **50-процентную скидку на годовую подписку на компакт-диски TechNet или Tech Net Plus в течение года после сдачи экзамена.** (Конкретные условия зависят от региона. Подробнее — в Welcome Kit.) Кроме тогэ, бесплатный доступ к Web-узлу TechNet (*http://www.microsoft.com/technet*) на котором опубликовано 95 % материалов с указанных компакт дисков.

Для работодателей и организаций. Сертифицированные специалисты эффективно работают с новейшими технологиями Microsoft, а значит, организация не только быстро окупит затраты на приобретение этих технологий, но и сможет достаточно быстро получить прибыль. Исследования показывают, что сертификация сотрудников по программам Microsoft:

- быстро окупается за счет стандартизации требований к обучению специалистов и методов оценки их квалификации;
- позволяет повысить эффективность обслуживания клиентов и производительность труда, а также снизить расходы на сопровождение операционных систем;
- предоставляет надежные критерии найма специалистов и их продвижения по службе;
- позволяет разработать гибкие методы оценки профессионального уровня и премирования персонала;
- предоставляет возможность переподготовки сотрудников для обучения новым технологиям;
- позволяет оценить профессиональный уровень сторонних фирм — партнеров по бизнесу.

Подробнее о пользе сертификации для вашей компании — в материалах и документах на узле http://www.microsoft.com/trainingandservices (разверните узел **Certification** и щелкните ссылку **Case Studies**.). Здесь опубликованы:

- «белая книга» «MCSE Criterion Validity Study White Paper, Oct. 1998» об оценке звания Microsoft Certified Systems Engineer (SysEngrCert.doc, 339 Кбайт);
- пример использования сертификации в компании Compaq (Compaq Case Study, Compaq .doc, 85 кбайт);
- пример использования сертификации в компании CrossTier.com (CrossTier.com Case Study, CrossTier.doc, 246 кбайт);
- пример использования сертификации в компании Extreme Logic (Extreme Logic Case Study, Extreme Logic.doc, 74 кбайт):
- «белая книга» «Financial Benefits to Supportersof Microsoft ProfessionalCertification» («Финансовые выгоды от поддержки профессионально сертификации Microsoft ») (1998wpidc .doc, 948 кбайт);
- пример использования сертификации в компании Lyondel (Lyondel Case Study, lyondel .doc, 20 кбайт);
- пример использования сертификации в компании Prudential (Prudential Case Study, prudentl.exe, 74 кбайт, самораспаковывающийся файл);

- пример использования сертификации в компании Stellcom (Stellcom Case Study, stellcom .doc, 72 кбайт);
- пример использования сертификации в компании Unisys (Unisys Case Study, Unisys.doc, 48 кбайт).

Требования к соискателям

Требования к соискателям определяются специализацией, а также служебными функциями и задачами сотрудника.

Соискатель сертификата Microsoft должен сдать экзамен, подтверждающий его глубокие знания в области программных продуктов Microsoft. Экзаменационные вопросы, подготовленные с участием ведущих специалистов компьютерной отрасли, отражают реалии применения программных продуктов компании Microsoft.

- **Сертифицированный специалист Microsoft** — кандидаты на это звание сдают экзамен на знание одной из операционных систем. Кандидат может сдать дополнительные экзамены, которые подтвердят его право на работу с продуктами Microsoft BackOffice, инструментальными средствами или прикладными программами.
- **Сертифицированный системный инженер Microsoft** — кандидаты на это звание сдают экзамены на знание технологии ОС Microsoft Windows, сетевых технологий и технологий семейства серверных продуктов Microsoft BackOffice.
- **Сертифицированный администратор баз данных Microsoft** — кандидаты на это звание сдают три основных экзамена и один — по выбору.
- **Сертифицированный разработчик программных решений на основе продуктов Microsoft** — кандидаты сдают два экзамена по основам технологии ОС Microsoft Windows и два — по технологиям интегрированного семейства серверных продуктов Microsoft BackOffice.
- **Сертифицированный преподаватель Microsoft** — соискателю надо подтвердить свою теоретическую и практическую подготовку для ведения соответствующих курсов в авторизованных учебных центрах Microsoft. Более подробные сведения о сертификации по этой программе вам сообщат сотрудники компании Microsoft по телефону (800) 636-7544 (в США и Канаде) или на узле *http://www.microsoft.com/train_cert/mcs*. За пределами США и Канады обращайтесь в местные отделения компании Microsoft.

Подготовка к экзаменам

Рекомендуются три режима подготовки: самостоятельная работа, интерактивный режим, а также занятия с инструктором в авторизованных центрах подготовки.

Самостоятельная подготовка

Самостоятельная работа — наиболее эффективный метод подготовки для инициативных соискателей. Издательства «Microsoft Press» и «Microsoft Developer Division» предлагают широкий спектр учебных пособий для подготовки к экзаменам по программе сертификации специалистов Microsoft. Учебные курсы для самостоятельного изучения, адресованные специалистам компьютерной отрасли, содержат теоретические и практические материалы, мультимедийные презентации, упражнения и необходимое ПО. Все эти пособия позволяют изучить весь необходимый материал, чтобы успешно выдержать любой из сертификационных экзаменов.

Интерактивная подготовка

Интерактивная подготовка через Интернет — альтернатива занятиям в учебных центрах. вы можете выбрать наиболее удобный распорядок занятий в виртуальном классе, где научитесь работать с продуктами и технологиями компании Microsoft и подготовитесь к сдаче экзаменов. В интерактивном виде доступно множество курсов Microsoft — как обычные официальные тесты, так и специальные, предназначенные специально для интерактивного обучения. Интерактивные ресурсы доступны круглосуточно в сертифицированных центрах подготовки.

Сертифицированные центры технического обучения Microsoft

Сертифицированные центры технического обучения Microsoft (Certified Technical Education Center, CTEC) — самый простой способ изучить материалы курса под руководством опытного инструктора для сдачи экзамена на звание сертифицированного специалиста Microsoft. Всемирная сеть учебных центров Microsoft CTEC позволяет специалистам повысить технический потенциал под руководством сертифицированных преподавателей Microsoft.

Подробнее о центрах CTEC в США и Канаде — на Web-узле компании Microsoft по адресу *http://www.microsoft.com/CTEC/default.htt*(на русском языке — *http://wwwmicrosoft.com/rus/CTEC/default.htm*).

Техническая поддержка

Мы постарались сделать все от нас зависящее, чтобы и сам учебный курс, и прилагаемый к нему компакт-диск не содержали ошибок. Если все же у вас возникнут вопросы или вы захотите поделиться своими предложениями или комментариями, обращайтесь в издательство Microsoft Press по одному из указанных ниже адресов.

Электронная почта: TKINPUT@MICROSOFT.COM

Почтовый адрес: Microsoft Press

Attn:MCSE Training Kit-Microsoft Windows 2000 Professional Editor

One Microsoft Way

Redmond,WA 98052-6399

Издательство Microsoft Press постоянно обновляет список исправлений и дополнений к своим книгам, он опубликован на узле *http://mspress.microsoft.com/supporl.*

Поддержка 120-дневной оценочной версии ISA-сервера не предоставляется ни Microsoft, ни Microsoft Press. Ее нельзя устанавли вать на основных компьютерах сети. За информационной поддержкой полной версии ISA-сервера (которая также, возможно, применима к пробной версии) обращайтесь на Web-узел *http://support.microsoft.com.*

Учтите, что по указанным почтовым адресам техническая поддержка не предоставляется. Для получения подробной информации о технической поддержке программных продуктов Microsoft обращайтесь на Web-узел компании Microsoft по адресу *http://www.microsoft.com/support* или звоните в службу Microsoft Support Network Sales по телефону (800) 936-3500 – в США.

Подробнее о получении полных версий программных продуктов Microsoft вы можете узнать, позвонив в службу Microsoft Sales по телефону (800) 426-9400 или по адресу *www.microsoft.com.*

ГЛАВА 1

Основные сведения о сервере Microsoft Internet Security and Acceleration Server 2000

Занятие 1. Краткий обзор ISA-сервера 2

Занятие 2, Брандмауэр на базе ISA-сервера 13

Занятие 3. Кэширование на ISA-сервере 21

Занятие 4. Особенности управления ISA-сервером 27

Закрепление материала 32

В этой главе

В этой главе рассказано об основных особенностях и возможностях сервера Microsoft Internet Security and Acceleration Server (ISA-сервера). Вы узнаете об основных ролях ISA-сервера — брандмауэра и сервера Web-кэширования, которые позволяют обеспечивать повышенную безопасность, а также превосходную производительность, управляемость, масштабируемость и расширяемость, а также о настраиваемой защите ISA-сервера, когда он функционирует в режиме брандмауэра, его работе в качестве сервера кэширования и мощных возможностях управления.

Прежде всего

Для изучения материалов этой главы необходимо иметь общее представление о следующих компонентах Microsoft Windows 2000:

- службе каталогов Active Directory;
- групповой политике;
- консоли MMC (Microsoft Management Console).

Занятие 1. Краткий обзор ISA-сервера

На этом занятии мы расскажем о возможностях и преимуществах ISA-сервера.

Изучив материал этого занятия, вы сможете:

- ✓ рассказать о различиях двух версий ISA-сервера;
- ✓ описать функциональные возможности ISA-сервера;
- ✓ объяснить, как ISA-сервер использует возможности Windows 2000 для обеспечения повышенной безопасности, производительности и управляемости;
- ✓ рассказать о масштабируемости и расширяемости ISA-сервера.

Продолжительность занятия - около 45 минут.

ISA-сервер — это расширяемый брандмауэр масштаба предприятия и сервер Web-кэширования, который базируется на операционной системе Windows 2000. Многоуровневый брандмауэр на базе ISA-сервера обеспечивает защиту сетевых ресурсов от вирусов и несанкционированного доступа, а сервер Web-кэширования позволяет организациям обеспечить более быстрый доступ к Web-ресурсам, сохраняя локальные копии объектов Интернета и возвращая их пользователям без обращения к узлам, хранящим оригинал. Режим работы ISA-сервера определяется в процессе установки — режим брандмауэра (Firewall), сервера Web-кэширования (Cache) или смешанный режим (Integrated).

ISA-сервер позволяет минимизировать сложности, сопутствующие внедрению и управлению брандмауэром и сервером кэширования, предоставляя интуитивно понятные и мощные средства управления, в том числе оснастки консоли MMC (Microsoft Management Console), *панели заданий* (taskpads) и мастеры.

Две версии ISA-сервера

ISA-сервер поставляется в двух модификациях: ISA Server Enterprise Edition и ISA Server Standard Edition.

ISA Server Enterprise Edition

Эта версия удовлетворяет высоким требованиям по производительности, управляемости и масштабируемости в средах с интенсивным трафиком Интернета. Она поддерживает централизованное управление сервером, многоуровневые политики доступа, кластеризацию серверов путем создания массивов и обеспечение отказоустойчивости.

ISA Server Standard Edition

Эта версия обеспечивает возможности защиты сетей посредством брандмауэра и кэширование Web-содержания для небольших предприятий, рабочих групп и отдельных подразделений. Она отличается превосходным соотношением «цена/качество» среди систем, применяемых в критически важных бизнес-средах.

Основные различия

Функции безопасности, кэширования, управления, производительности и расширяемости одинаковы в обеих версиях ISA-сервера. Однако версия Standard работает только как изолированный ISA-сервер с локальной политикой и поддерживает не более 4 процессоров. Версия Enterprise может работать в многосерверных массивах с централизованным управлением, политиками уровня предприятия и уровня массива и неограниченной масштабируемостью.

Хотя эта книга и посвящена конфигурированию и управлению версией Enterprise Edition ISA-сервера, понимание различий между двумя версиями позволяет правильно выбрать подходящую в той или иной ситуации. Эти различия перечислены в таблице 1-1.

Таблица 1-1. Различия двух версий ISA-сервера

	ISA Server Standard Edition	ISA Server Enterprise Edition
Развертывание сервера	Только изолированный	Многосерверная конфигурация с централизованным управлением
Поддержка различных уровней политики	Только локальная политика	Политики уровня предприятия и уровня массива
Масштабируемость оборудования	Не более 4 процессоров	Не ограничена

Роли ISA-сервера

ISA-сервер — отличное решение для организаций самых разных размеров, заинтересованных в обеспечении безопасности, производительности и управляемости сетей за разумные деньги. С ним могут работать ИТ-менеджеры, администраторы сети и специалисты информационной безопасности. ISA-сервер работает в одном из трех возможных режимов: как брандмауэр (Firewall), как кэширующий сервер (Cache) или в смешанном режиме (Integrated). В последнем случае он совмещает выполнение функций брандмауэра и сервера Web-кэширования. Существует множество вариантов развертывания ISA-сервера в конкретных организациях — в этой книге описаны лишь наиболее популярные.

Брандмауэр Интернета

ISA-сервер можно установить как выделенный брандмауэр, выполняющий функции защищенного шлюза Интернета для клиентов внутренней сети. ISA-сервер работает незаметно («прозрачно») для соединяемых клиентов, если только они не обмениваются информацией, запрещенной ограничениями доступа или правилами защиты.

Работая в качестве брандмауэра, ISA-сервер позволяет реализовать определяемую бизнесом политику безопасности при работе через Интернет, предоставляя богатые возможности по настройке обширного набора правил, которые определяют порядок пересылки через него трафика различных узлов, протоколов и Web-содержимого. Постоянно контролируя запросы и ответные сообщения между Интернетом и клиентскими компьютерами внутренней сети, ISA-сервер управляет доступом различных клиентов к тем или иным компьютерам корпоративной сети. Также он позволяет управлять доступом клиентов внутренней сети к компьютерам Интернета.

Безопасная публикация серверов

ISA-сервер позволяет публиковать службы в Интернете, не нарушая безопасность внутренней сети. Для этого он обрабатывает внешние клиентские запросы от имени опубликованного внутреннего сервера.

Сервер прямого Web-кэширования

Выполняя функции сервера прямого Web-кэширования, ISA-сервер поддерживает централизованный кэш наиболее часто запрашиваемых данных Интернета и использует содержимое кэша для обслуживания запросов от браузеров в частной сети. Таким образом удается добиться повышения производительности браузера, сократить время отклика и снизить потребление пропускной способности подключений к Интернету.

Сервер обратного Web-кэширования

ISA-сервер иногда действует как Web-сервер, используя данные из кэша для обслуживания входящих клиентских запросов и пересылая запросы на локальный Web-сервер только при отсутствии нужной информации в кэше.

Сервер, совмещающий функции брандмауэра и сервера кэширования Web-содержимого

ISA-сервер обычно используют в одном из режимов — брандмауэра или сервера кэширования, однако существует возможность совместить эти функции на одном компьютере для обеспечения безопасной и быстрой связи с Интернетом. Независимо от варианта развертывания, ISA-сервер обеспечивает все преимущества централизованного управления на основе политик.

Интеграция с Windows 2000

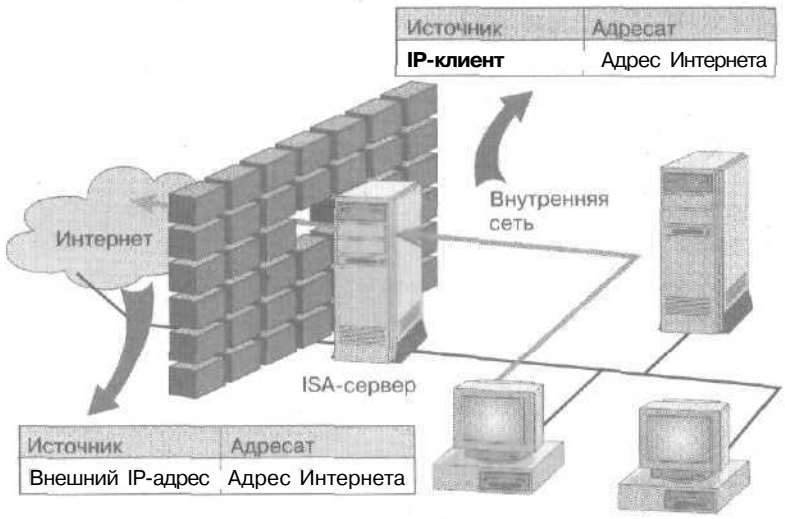
ISA-сервер базируется на технологиях Windows 2000, за счет чего обеспечивается повышенная безопасность и производительность, а также расширенные возможности управления. Далее перечислены возможности Windows 2000, применяемые на ISA-сервере для поддержки перечисленных функций.

- **Преобразование сетевых адресов (Network Address** Translation, NAT). ISA-сервер расширяет возможности NAT в Windows 2000, поддерживая специальную политику для клиентов SecureNAT (рис. 1-1),

---

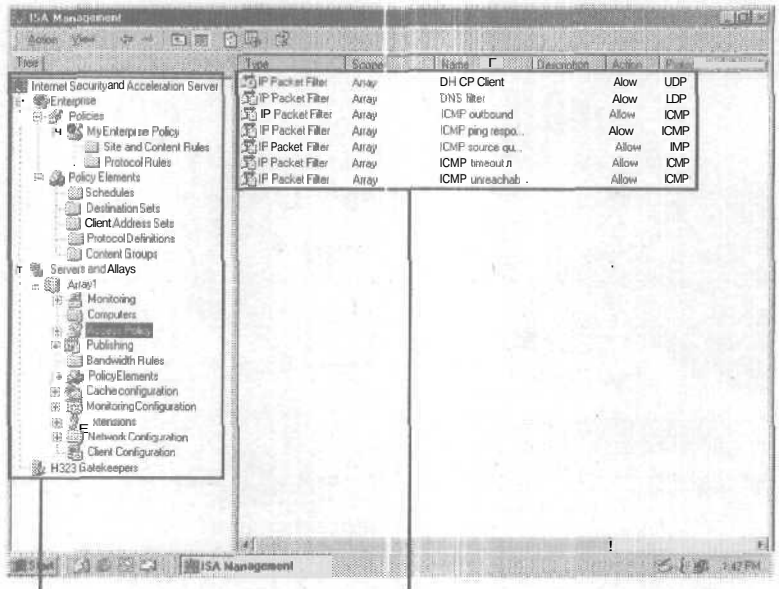
Примечание Стандарт NAT описан в документе RFC 1361 сообщества IETF (Internet Engineering Task Force). NAT является встроенным компонентом Windows 2000 и представляет собой шлюз, скрывающий IP-адреса клиентов внутренней ЛВС (LAN) от внешних клиентов, что достигается путем сопоставления внутренних адресов другим, доступным извне, адресам.

- **Интегрированные виртуальные частные сети (Virtual Private Network, VPN).** ISA-сервер можно сконфигурировать как VPN-сервер для поддержки безопасных удаленных подключений типа «шлюз — шлюз» или «клиент — шлюз» через Интернет. Основанная на общепринятых стандартах подсистема Windows 2000 для работы по VPN поддерживает протоколы PPTP (Point to Point Tunneling Protocol) и L2TP/IPSec (Layer 2 Tunneling Protocol/Secure Internet Protocol).
- **Аутентификация.** ISA-сервер поддерживает принятые в Windows 2000 методы проверки подлинности, в том числе базовую аутентификацию, проверку подлинности по протоколам NTLM (NT LAN Manager) и Kerberos, а также аутентификацию на основании
  * цифровых сертификатов.
- **Ограничение возможностей пользователей по настройке системы.** Для частичного или полного предотвращения модификации системы пользователями на ISA-сервере применяются шаблоны безопасности Windows 2000.



Рис, 1-1. Механизм SecureNAT

- **База данных** Active **Directory.** Когда ISA Server Enterprise Edition конфигурируется для работы в многосерверном массиве, конфигурация и политики хранятся централизованно в базе данных службы каталогов Active Directory. Кроме того, для управления доступом пользователей и групп на ISA-сервере часто применяют данные Active Directory.
- **Многоуровневая подсистема управления на основе политик.** Сервер ISA Server Enterprise Edition позволяет использовать распределенные службы каталогов Active Directory, для этого определяется одна или несколько политик, которые затем применяются к массивам всего предприятия. Указанный механизм поддерживает многоуровневую и масштабируемую модели администрирования.
- **Административные консоли MMC.** Интерфейс управления ISA-сервером называется ISA Management (рис. 1-2) и представляет собой оснастку MMC, отображаемую в *виде панели задании* (Taskpad) или в *расширенном виде* (Advanced). Консоль MMC расширяема и позволяет «гладко» интегрировать средства управления, созданные сторонними поставщиками, в панель управления ISA-сервером.
- **Качество обслуживания (Quality of Service, QoS).** ISA-сервер обеспечивает механизмы управления пропускной способностью, которые базируются на службе качества обслуживания (QoS) в Windows 2000 и применяются для распределения трафика в соответствии с приоритетами.
- **Поддержка многопроцессорных систем.** Для повышения производительности на ISA-сервере применяется присутствующая в Windows 2000 архитектура поддержки симметричных многопроцессорных вычислений (SMP).
- **Автоматическое обнаружение прокси-сервера клиентами.** Поддержка протокола автоматического обнаружения прокси-сервера WPAD (Web Proxy Autodiscovery Protocol) на клиентах брандмауэра, основанного на ISA-сервере, позволяет им автоматически подключаться к ISA-серверу, при этом нет необходимости индивидуально конфигурировать каждый клиент.
- **COM-объект администрирования ISA-сервера.** ISA-сервер представляет доступ из программ к механизму управления правилами брандмауэра и всеми административным параметрами.



Пространство имен ISA-сервера Политика доступа: Правила доступа

Рис. 1-2. Окно оснастки ISA Management

- **Web-фильтры.** Для контроля и управления проходящим через шлюз трафиком протоколов HTTP и FTP применяются Web-фильтры ISA-сервера, создаваемые на основе интерфейса ISAPI (Internet Server Application Programming Interface).
- **Оповещения.** ISA-сервер регистрирует оповещения Windows 2000 в журнале событий.

Масштабируемость

Компьютеры с ISA Server Enterprise Edition можно объединять в массивы для обеспечения повышенной отказоустойчивости, балансирования нагрузки и распределенного кэширования. Массив ISA-серверов рассматривается и управляется как единый логический объект. Установка массива также позволяет повысить производительность и снизить потребление пропускной способности. Объединение в массивы позволяет распределять клиентские запросы между многими ISA-серверами, что сокращает время отклика на клиентские запросы. За счет распределения нагрузки между серверами массива удается добиться повышения производительности даже на оборудовании средней мощности.

Существуют и другие возможности, способствующие высокой масштабируемости ISA-сервера.

- **Поддержка симметричных многопроцессорных вычислений (SMP).** ISA-сервер использует преимущества поддержки технологии SMP в Windows 2000 для поддержки многопроцессорных систем и масштабирования производительности вверх. Версия ISA Server Standard Edition поддерживает до 4 процессоров на компьютере, а версия ISA Server Enterprise Edition — неограниченное число процессоров, что достигается за счет использования массивов. В отличие от других программных продуктов на ISA-сервере дополнительные вычислительные мощности применяются для повышения производительности.

- **Балансировка сетевой нагрузки (Network Load Balancing).** Поставляемая в составе Microsoft Windows 2000 Advanced Server и Windows 2000 Datacenter Server служба балансировки сетевой нагрузки используется на ISA-серверах для объединения их в кластеры и обеспечения отказоустойчивости, высокой готовности и производительности. Служба NLB особенно эффективна в конфигурациях, где требуется обеспечить работу брандмауэра, обратное кэширование (Web-публикация) и публикацию серверов.

Расширяемость

Ряд сторонних поставщиков предоставляют расширения ISA-сервера, обеспечивающие дополнительные функции, такие как обнаружение вирусов, фильтрация информации, классификация Web-узлов, расширенные возможности отчетности и администрирования.

Клиенты и разработчики также вправе создавать собственные расширения ISA-сервера. Для этого в составе ISA-сервера поставляется полноценный *комплект ресурсов для разработчиков* (software development kit, SDK), позволяющий создавать дополнительные функции на основе существующих возможностей ISA-сервера — брандмауэра, кэширования и управления. Кроме того, в составе ISA-сервера поставляются типовые сценарии, освобождающие администраторов от необходимости создавать их «с нуля»: зачастую достаточно лишь изменить типовой сценарий, указав требуемые протоколы, правила или узлы, и успешно использовать его для решения своих задач.

Архитектура ISA-сервера

ISA-сервер обеспечивает защиту корпоративной сети на многих коммуникационных уровнях. ISA-сервер осуществляет фильтрацию на уровне пакетов. При включенной фильтрации пакетов ISA-сервер статически управляет пересылкой данных через внешний интерфейс, оценивая входящий и исходящий трафик до того, как тот достигает какого-либо ресурса. Данные, прошедшие через фильтры пакетов, передаются службам брандмауэра и Web-прокси, где вступают в игру правила ISA-сервера и определяется возможность обслуживания запроса.

ISA-сервер обеспечивает защиту клиентам трех типов (рис. 1-3): брандмауэра, SecureNAT и Web-прокси.

Клиенты брандмауэра — это компьютеры с установленным и работающим программным обеспечением *клиента брандмауэра* (Firewall Client). Запросы от клиентов брандмауэра поступают на брандмауэр ISA-сервера, где определяется возможность предоставления доступа. В дальнейшем трафик от клиента брандмауэра обычно проходит через фильтры приложений и других дополнительных модулей. Запрос HTTP-объекта клиентом брандмауэра перенаправляется редиректором HTTP на Web-прокси, который, возвращая запрошенный объект, может параллельно разместить его в своем кэше. При наличии HTTP-объекта в кэше ISA-сервер не обращается в Интернет, а возвращает копию объекта из кэша.

Клиенты SecureNAT — это компьютеры, на которых не установлен клиент брандмауэра. Запросы от клиентов SecureNAT сначала попадают на NAT-драйвер, который заменяет глобальный IP-адрес Интернета клиента SecureNAT на адрес клиента во внутренней сети. Далее запросы от клиентов брандмауэра поступают на брандмауэр ISA-сервера, где определяется возможность доступа. В дальнейшем трафик от клиента брандмауэра проходит через фильтры приложений и других дополнительных модулей. Как и в предыдущем случае, запрос HTTP-объекта клиентом брандмауэра перенаправляется редиректором HTTP на Web-прокси, и тот, возвращая ответ, может параллельно разместить полученный из Интернета запрошенный объект в своем кэше. Далее он не обращается в Интернет, а возвращает копию из кэша.

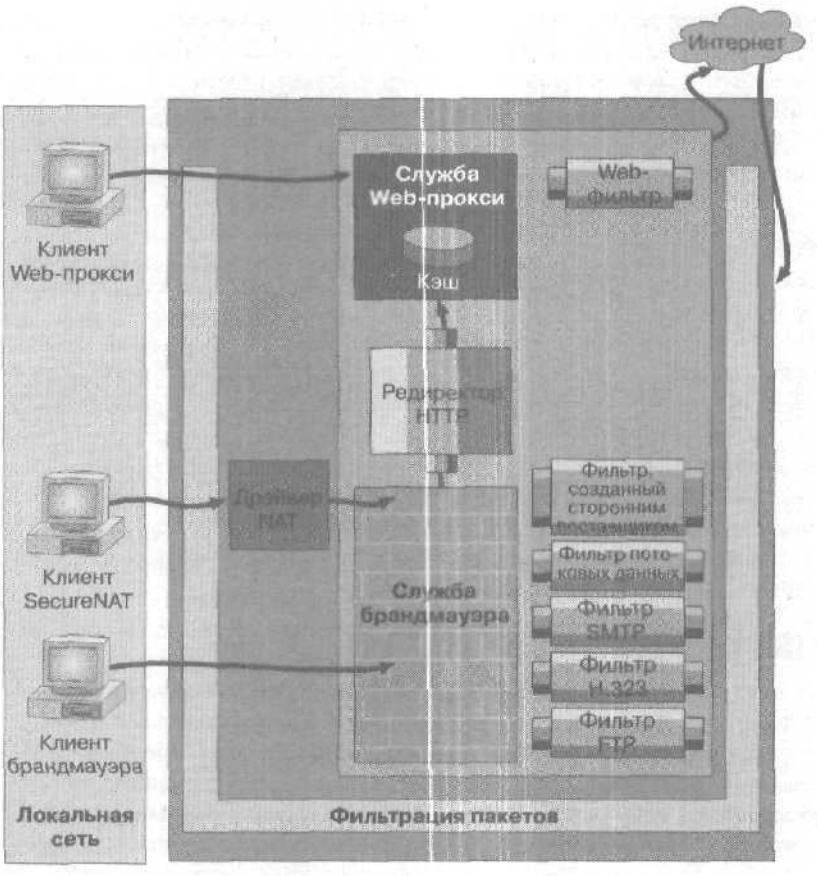


Рис. 1-3. Общая схема архитектуры ISA-сервера

Клиенты Web-прокси — это любые поддерживающие стандарты CERN Web-приложения, например Microsoft Internet Explorer. Запросы от клиентов Web-прокси направляются в службу Web-прокси ISA-сервера для определения возможности предоставления доступа. Служба Web-прокси возвращает запрошенный объект непосредственно из Интернета (одновременно размещая его копию в кэше) или из кэша ISA-сервера.

В таблице 1-2 описаны основные возможности ISA-сервера.

Таблица 1-2. Основные возможности Microsoft ISA Server

Возможность	Достоинства
Режим брандмауэра предприятия	
Контроль на основании всех состояний	ISA-сервер динамически и «интеллектуально» следит за трафиком, пересылаемым через брандмауэр, контролируя протоколы и состояние подключения для обеспечения непрерывной связи и предотвращения нарушений защиты

Таблица 1-2. *(продолжение)*

Возможность	Достоинства
«Интеллектуальная»	ISA-сервер обеспечивает не только базовые функции по фильтрация трафика приложений. Специальные фильтры, распознающие виды данных, позволяют управлять трафиком отдельных приложений. Поддерживается пересылка, блокирование, переадресация и модификация данных средствами интеллектуальной фильтрации протоколов HTTP, FTP, SMTP, электронной почты, конференций H.323 (мультимедиа), потоковых мультимедийных данных и RPC
Безопасная публикация серверов, в том числе Web-серверов	Зашита Web-серверов, почтовых серверов и приложений электронного бизнеса от атак извне обеспечивается механизмом безопасной публикации серверов. ISA-сервер выступает от имени опубликованного сервера, обеспечивая дополнительный уровень зашиты. Правила Web-публикации позволяют защитить Web-серверы путем разрешения доступа лишь определенным компьютерам. Правила публикации серверов защищают серверы от несанкционированного доступа внешних пользователей
Обнаружение вторжений	Встроенные механизмы обнаружения атак основаны на технологии компании Internet Security Systems Inc. (ISS). В случае обнаружения вторжения инициируется оповещение и выполняются ответные действия. Обнаруживаются сканирование портов (port scan), WinNuke и «Ping смерти» (Ping of Death)
Интегрированная технология виртуальных частных сетей (VPN)	Обеспечивается поддержка основанного на стандартах удаленного доступа с применением VPN-служб в Windows 2000. ISA-сервер поддерживает безопасные VPN-подключения, в том числе подключения филиалов и удаленных пользователей к корпоративной сети через Интернет
Запрещение изменений системной конфигурации	Мастер Security Configuration позволяет администраторам заблокировать компьютеры для любых изменений конфигурации путем определения соответствующего уровня безопасности в зависимости от функций, выполняемых ISA-сервером в корпоративной сети
Разбиение потоковых мультимедийных данных	Значительный объем пропускной способности удается сэкономить за счет разбиения потоковых данных средствами фильтров мультимедиа ISA-сервера, которые, получая данные из Интернета, располагают их на сервере Windows Media Technologies Server и предоставляют для доступа пользователям внутренней сети
«Прозрачность» брандмауэра	Протокол SecureNAT обеспечивает расширяемые и «прозрачные» механизмы зашиты брандмауэра для всех IP-клиентов путем динамической замены глобальных IP-адресов на локальные. При этом не требуется никакого дополнительного клиентского ПО и программ конфигурирования клиентов

(см. след. стр.)

Таблица **1-2.** *(продолжение)*

Возможность	Достоинства
Надежная аутентификация пользователей	Обеспечивается стандартными средствами аутентификации Windows (NTLM и Kerberos), выполняется на основании сертификатов клиентов и хешей. Кроме того, поддерживается базовая и анонимная аутентификация в Web
Двухэтапная аутентификация по протоколу SSL (сопряжение)	На Web-серверах, где следует обеспечить аутентификацию и шифрование при клиентском доступе, ISA-сервер обеспечивает сквозную безопасность и фильтрацию брандмауэра посредством двухэтапной процедуры с применением протокола SSL. На первом этапе ISA-сервер запрашивает у клиента сертификат пользователя и проверяет содержащиеся в нем данные, а на втором — представляет свой собственный сертификат сервера Web-серверу. В отличие от большинства брандмауэров ISA-сервер позволяет проверять зашифрованные данные до того, как они поступят на Web-сервер
Режим сервера **кэширования** Web-информации	
Высокопроизводительное Web-кэширование	При наличии ISA-сервера производительность доступа к корпоративному Web-серверу извне и доступ пользователей внутренней сети в Интернет существенно возрастает за счет быстрого кэширования Web-информации в оперативной памяти и на дисках
«Интеллектуальное» активное кэширование	Функция активного кэширования ISA-сервером популярной информации заметно облегчает клиентам получение самых свежих данных. ISA-сервер автоматически определяет, какие Web-узлы наиболее популярны и как часто информация на них обновляется (а значит, с какой периодичностью нужно обновлять ее копию в кэше) на основании информации о том, как долго объект хранится в кэше или как давно он был загружен. ISA-сервер активно загружает Web-данные в кэш в периоды низкой загрузки сети, при этом не требуется вмешательства диспетчера сети
Кэширование по расписанию	Существует возможность загружать в кэш содержимое целых Web-узлов по расписанию загодя, до того как к ним обратятся клиенты Загрузка по расписанию гарантирует актуальность предоставляемых пользователям данных и данных, хранящихся на серверах-зеркалах
Распределенное и иерархическое кэширование	В версии ISA Server Enterprise Edition можно сконфигурировать распределенное кэширование в массивах ISA-серверов. Кроме того, администраторы вправе создавать иерархии, или цепочки, кэшей, что позволяет клиентам получать доступ к информации из ближайшего к ним кэша

Таблица 1-2. *(продолжение)*

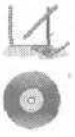
Унифицированное управление	
Управление доступом на основе политик	Управление входящим и исходящим доступом осуществляется на основании информации о пользователях, данных групп, приложений и адресатов, а также в зависимости от типа информации и по расписанию. Мастеры конфигурации политик позволяют определить узлы и содержимое, доступ к которым разрешен, а также ограничить перечень доступных протоколов раздельно для входящего и исходящего трафики. Кроме того, можно разрешить или запретить связь между конкретными IP-адресами по указанным протоколам и портам
Многоуровневое управление	Версия Enterprise Edition поддерживает многоуровневое управление на основе политик доступа уровня массив и предприятия. Таким образом обеспечивается преемственность политики предприятия в филиалах и подразделениях, причем местные администраторы вправе дополнительно определять локальные правила в соответствии с потребностями своих подразделений
Управление пропускной способностью	Обеспечивается возможность управлять пропускной способностью и использованием сети, назначая приоритеты при выделении пропускной способности для конкретных запросов информации в Интернете на уровне групп, приложений, узлов или типов информации. На ISA-сервере используются преимущества службы управления качеством QoS в Windows 2000
Интеграция со службой каталогов Active Directory	Интеграция со службой каталогов Active Directory при развертывании ISA-сервера необязательна, однако она позволяет централизованно управлять и хранить в Active Directory информацию обо всех пользователях, правилах и конфигурации. В версии Enterprise Edition служба Active Directory позволяет использовать единую схему, развертывать кэширующие массивы, автоматически распространять изменения параметров масштаба предприятия, получать доступ к политикам доступа и публикации, а также выполнять мониторинг конфигураций
Графические *панели заданий* (taskpad) и мастеры конфигурирования	Эти элементы облегчают перемещение по интерфейсу и выполнение стандартных задач по конфигурированию. В частности, мастеры применяются для публикации серверов Microsoft Exchange Server, конфигурирования ISA-сервера в качестве шлюза **VPN** или для создания правил узлов и содержимого
Удаленное управление	ISA-серверы управляются удаленно посредством оснасток MMC или службы терминалов в Windows 2000 (Microsoft Windows 2000 Terminal Services). Кроме того, для удаленного управления службами ISAсервера администраторам предоставляется возможность применять сценарии командной строки
Ведение журналов, отчетность и оповещения	Детализированные журналы безопасности и доступа создаются в стандартных форматах данных, в том числе в форматах W3C и ODBC. Существует возможность создавать встроенные отчеты о Web-трафике, об использовании приложений, схемах сетевого трафика и безопасности. Оповещения на основе событий можно настраивать для автоматической отправки электронной почты администраторам, остановки или запуска служб или других действий, определяемых критериями оповещения

(см. след. стр.)

Таблица 1-2. *(окончание)*

Возможность	Достоинства
Управление на уровне пользователей	Администраторы вправе управлять средствами службы брандмауэра ISA-сервера, предоставляя доступ на уровне отдельных пользователей, а не просто IP-адресов, что обеспечивает более точное управление доступом как для входящего, так и исходящего трафика для всех протоколов

Практикум. Презентация, посвященная ISA-серверу



Сейчас вы посмотрите 15-минутную мультимедийную презентацию, посвященную возможностям и преимуществам ISA-сервера. Для этого дважды щелкните файл ISA_Demo.exe, расположенный в папке \Exercises\Chapter1\ на прилагаемом к книге компакт-диске.

Резюме

ISA-сервер позволяет создавать решения подключения к Интернету масштаба целого предприятия, которые содержат устойчивый многофункциональный брандмауэр и масштабируемый Web-кэш для ускорения работы в Интернете. Брандмауэр и сервер кэширования Web-содержимого можно развертывать как по отдельности, так и совмещать — все определяется проектом сети и требованиями заказчика.

ISA-сервер поставляется в двух версиях, что позволяет удовлетворить любые бизнес-требования и требования к проектам сетей заказчика. ISA Server Standard Edition позволяет обеспечить функции брандмауэра и сервера кэширования для предприятия в небольших компаниях, рабочих группах и отдельных подразделениях. Версия ISA Server Enterprise Edition предназначена для более крупных организаций и является масштабируемым решением с поддержкой брандмауэра и сервера Web-кэширования благодаря поддержке многосерверных массивов и многоуровневых политик.

Развитые функции безопасности ISA-сервера базируются на мощных возможностях баз данных безопасности в Windows 2000 и позволяют конфигурировать правила безопасности, основанные на конкретных типах графика на уровне отдельных пользователей, компьютеров или групп Windows 2000.

Консоль управления ISA Management обеспечивает простоту управления брандмауэром и кэшем ISA-сервера. Она базируется на консоли MMC и объединяет все «рычаги управления» ISA-сервером, позволяя централизованно контролировать его работу с помощью мастеров и панелей заданий, которые существенно упрощают наиболее популярные процедуры управления. ISA-сервер также обеспечивает мощные средства управления безопасностью на основе политик. Администраторы получают возможность управлять доступом и пропускной способностью, определяя их для любых существующих элементов политики — пользователей, компьютеров, протоколов, типов информационного наполнения, расписаний и Web-узлов. Наконец, ISA-сервер — это чрезвычайно гибкая расширяемая платформа с собственным комплектом ресурсов для разработчиков (SDK) и набором типовых сценариев, которые позволяют настраивать архитектуру подключения к Интернету в соответствии с потребностям бизнеса.

Занятие 2, Брандмауэр на базе ISA-сервера

Интернет предоставляет организациям новые возможности связи с клиентами, партнерами и сотрудниками, однако его использование связано с определенным риском и трудностями, что вызывает необходимость принятия дополнительных мер для обеспечения безопасности, производительности и управляемости. Вместе с ростом популярности Интернета растут и требования к производительности и безопасности. Брандмауэр ISA-сервера позволяет решить многие связанные с зашитой проблемы, предоставляя возможности по управлению доступом как извне к корпоративным сетевым ресурсам, так и из сети к серверам в Интернете. Управление доступом осуществляется на основании правил, реализуемых согласно настраиваемым политикам, число которых практически ничем не ограничено.

Изучив материал этого занятия, вы сможете:

- рассказать о трехуровневой фильтрации на ISA-сервере;
- рассказать о встроенных фильтрах приложений на ISA-сервере;
- описать типы обнаруживаемых ISA-сервером атак на уровне пакетов и на уровне приложений.

Продолжительность занятия — около 35 минут.

Методы фильтрации

Брандмауэр обеспечивает защиту, применяя различные методы фильтрации, в том числе фильтрацию пакетов, низкоуровневую фильтрацию протоколов и фильтрацию трафика приложений. На развитых брандмауэрах предприятия, к числу которых относится ISA-сервер, эти методы объединяются для обеспечения защиты на многих уровнях сети.

Фильтрация IP-пакетов

Фильтры пакетов позволяют управлять входящим и исходящим потоками IP-пакетов через ISA-сервер (рис. 1-4). При включенной фильтрации пакетов (включение и отключение фильтрации выполняется в диалоговом окне **IP Packet Filters Properties)** на внешнем интерфейсе игнорируются (то есть не пропускаются) все пакеты, прохождение которых не разрешено явно. Система перехватывает и оценивает пакеты до того, как они попадут на более высокий уровень брандмауэра или на фильтр приложений.

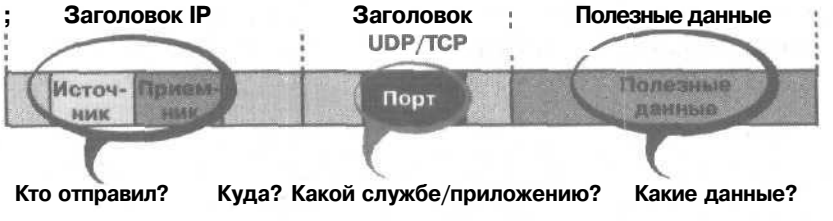


Рис. 1-4. Фильтрация IP-пакетов

Сконфигурировав фильтры IP-пакетов на разрешение пересылки лишь ограниченного числа вполне определенных типов пакетов, вы существенно повысите защищенность своей сети. Фильтрация IP-пакетов также позволяет блокировать трафик от конкретных серверов Интернета и не пропускать пакеты, которые явно относятся к наиболее популярным видам атак. Кроме того, вам предоставляется право заблокировать пакеты, адресо-

ванные определенным службам во внутренней сети, в том числе Web-прокси, Web-серверу или почтовому SMTP-серверу.

Фильтры IP-пакетов поддерживают анализ пакетов на основании таких критериев, как тип службы, номер порта, имя компьютера-источника или компьютера-приемника. Фильтры IP-пакетов статические, то есть они применяются к определенным портам и не изменяют своих свойств, постоянно пропуская или блокируя пакеты согласно заданным критериям. Разрешающие фильтры (Allow) беспрепятственно пропускают весь трафик через указанный порт, а запрещающие (Block) — полностью блокируют.

Примечание Даже если фильтрация пакетов отключена, связь между локальной сетью и Интернетом становится возможной только после того, как вы сконфигурируете правила протокола на явное разрешение доступа.

Фильтрация на уровне каналов (протоколов)

Предусмотрена возможность конфигурировать фильтрацию на уровне отдельных протоколов трафика, проходящего через ISA-сервер, настройкой правил политики доступа и правил публикации. Как показано на рис. 1-5, эта особенность позволяет контролировать сеансы, а не просто отдельные подключения или пакеты. Сеанс часто охватывает многие подключения — таким образом обеспечивается ряд важных преимуществ для клиентов брандмауэра, работающих под управлением операционных систем семейства Windows.

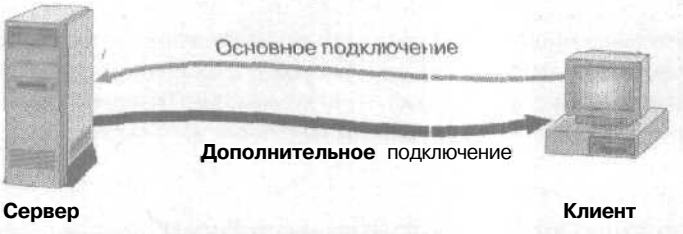


Рис. 1-5. Фильтрация сеансов на уровне каналов или сеансов может охватывать несколько подключений

Динамическая фильтрация

ISA-сервер поддерживает динамическую фильтрацию на основании правил политики доступа и правил публикации. Она позволяет автоматически открывать порты только на время связи и закрывать после разрыва подключения, Благодаря такому подходу минимизируется число открытых портов во всех направлениях и обеспечивается высокий уровень защиты сети.

Фильтрация на уровне каналов обеспечивает встроенную поддержку таких поддерживающих дополнительные подключения протоколов, как FTP и протоколы потоковой передачи мультимедиа. Основное и дополнительные подключения протокола указываются непосредственно в пользовательском интерфейсе без какого-либо дополнительного программирования или применения средств сторонних поставщиков. В процессе настройки вы можете определить номер порта или их диапазон, тип протокола, протокол TCP или UDP, а также направление — входящее или исходящее.

Фильтрация трафика приложений

Наиболее сложный вариант управления трафиком через брандмауэр — это защита на уровне приложений. Качественные фильтры приложений позволяют анализировать поток данных конкретных приложений и выполнять особые, характерные для данного приложения операции, например контроль, экранирование или блокирование, перенаправление или модификацию данных при их проходе через брандмауэр. Как показано на рис. 1-6, этот механизм применяется для защиты от таких угроз, как небезопасные команды SMTP или атаки на внутренние серверы DNS. Во всех средствах сторонних поставщиков, предназначенных для перекрытия доступа к определенному содержанию (экранирование), в том числе для обнаружения вирусов, лексического анализа и классификации Web-узлов, применяются Web-фильтры и фильтры приложения. Таким образом эти дополнительные программные средства расширяют функциональные возможности брандмауэра.

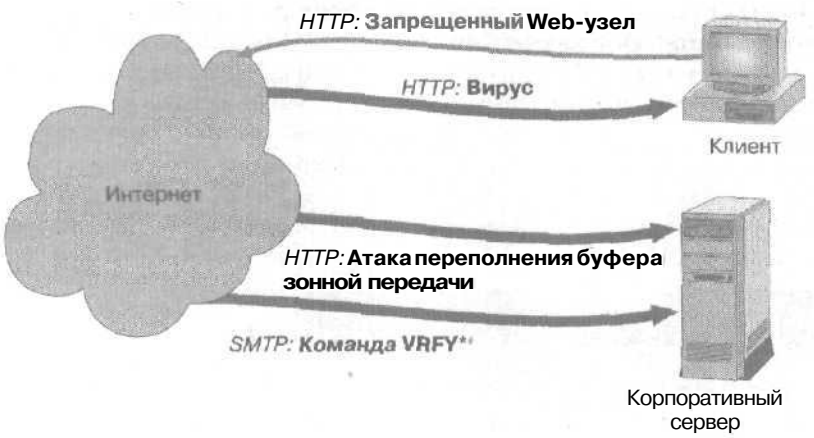


Рис. 1-6. Фильтрация на уровне приложений

В составе ISA-сервера поставляются различные встроенные фильтры трафика приложений.

- **Фильтры редиректора HTTP** управляют пересылкой прямых HTTP-запросов от брандмауэра и клиентов SecureNAT к Web-прокси. Таким образом обеспечивается «прозрачное» кэширование для клиентов, которые не в состоянии переконфигурировать свой браузер на перенаправление запросов на Web-прокси.
- **Фильтры доступа по протоколу FTP** перехватывают и проверяют данные протокола FTP. Работающая в режиме ядра подсистема передачи данных обеспечивает высокую скорость для разрешенного трафика.
- **Фильтры SMTP** перехватывают и проверяют трафик электронной почты, пересылаемой по протоколу SMTP, таким образом защищая почтовые серверы от атак. Фильтр распознают небезопасные команды и способны проверять сообщения электронной почты на предмет запрещенного содержания или превышения размера и отбрасывать такие сообщения до того, как они достигнут почтового сервера.
- **Фильтры SOCKS** пересылают в службу брандмауэра ISA-сервера запросы от поддерживающих SOCKS 4.3 приложений на клиентских компьютерах без установленного клиента брандмауэра. Доступ приложения клиента SOCKS к Интернету управляется правилами политики доступа. В отличие от Winsock, SOCKS поддерживает все клиентские платформы, в том числе Unix, Macintosh и нестандартные вычислительные устройства.
- **Фильтры RPC** обеспечивают сложную фильтрацию вызовов удаленных процедур для определенных интерфейсов, выбор которых определяется администратором.

- **Фильтры H.323** перенаправляют H.323-пакеты с данными мультимедиа и телеконференцсвязи и управляет вызовами, в том числе позволяют обслуживать входящие запросы и подключаться к определенному *привратнику* (gatekeeper) H.323.
- **Фильтры потоковых мультимедийных данных** поддерживают отраслевые стандарты, в том числе Microsoft Windows Media Technologies и оба потоковых протокола компании RealNetworks — PNA (Progressive Networks Audio) и Real-Time Streaming Protocol (RTSP). Они также предоставляют пользователям возможность разбивать (размножать) онлайновые потоки Windows Media и таким образом экономить полосу пропускания.
- **Фильтры протокола POP и обнаружения атак на DNS** распознают и блокируют многие типы атак на внутренние серверы, в том числе переполнение буфера имени узла в DNS, переполнение буфера зонной передачи и буфера почтового протокола POP (Post Office Protocol).

Привратник Gatekeeper H.323 используется совместно с фильтром протокола H.323 для поддержки всех возможностей связи зарегистрированных клиентов H.323 с приложениями, совместимыми с привратником H.323, например NetMeeting 3.x. Привратник предоставляет зарегистрированным клиентам услуги по маршрутизации вызовов и доступу к каталогу адресатов, а также позволяет по известному псевдониму связаться с ними другим клиентам. Клиенты, зарегистрировавшиеся на H.323 Gatekeeper, получают возможность использовать его для участия во встречах с применением видео, звука и данных в ЛВС и ГВС, через брандмауэры и Интернет. Настройка привратника Gatekeeper H.323 выполняется средствами консоли ISA Management в узле **H323** Gatekeepers (рис. 1-7).

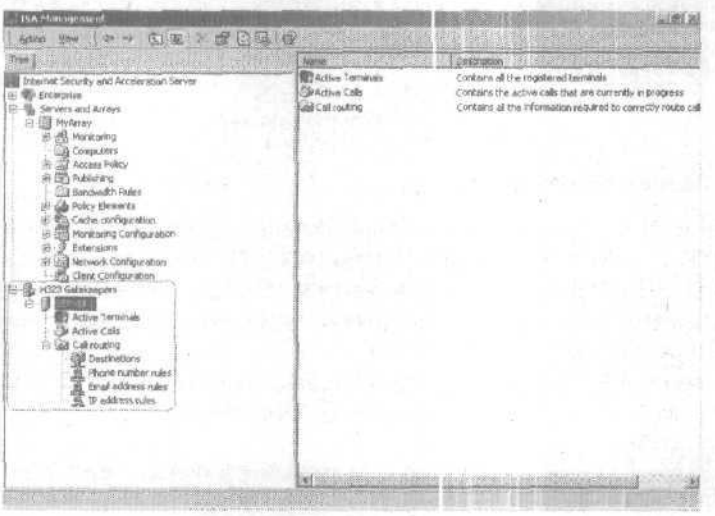


Рис. 1-7. Конфигурирование привратников H.323 Gatekeeper

На ISA-сервере определены около 100 протоколов приложений, кроме того, администраторам предоставлено право определять дополнительные протоколы, задавая номер и тип порта, протокол — TCP или UDP — и направление. Поддержка протоколов с добавочными (вторичными) подключениями обеспечивается средствами ПО клиента брандмауэра или фильтра приложений.

Правила пропускной способности

Правила пропускной способности определяют приоритеты подключений. Средства управления пропускной способностью ISA-сервера не ограничивают ее, а лишь информируют службу качества обслуживания (QoS) Windows 2000 о приоритетах тех или иных сетевых подключений. Подключениям, с которыми не связаны никакие правила пропускной способности, присваивается приоритет по умолчанию. Любое подключение с таким правилом пользуется преимуществом перед подключением с приоритетом по умолчанию.

Интегрированная поддержка VPN

ISA-сервер облегчает администраторам установку и обеспечение безопасности виртуальных частных сетей (VPN). Как показано на рис. 1-8, VPN — это расширение частной сети, простирающееся далеко за ее пределы через совместно используемые или общедоступные сети, такие как Интернет. VPN позволяет пересылать данные между двумя компьютерами через открытые сети так, как это происходит по связи типа «точка — точка* в частной сети. ISA-сервер можно сконфигурировать как сервер VPN для обеспечения безопасной связи между шлюзами или для поддержки удаленного доступа между клиентами и шлюзами через Интернет.

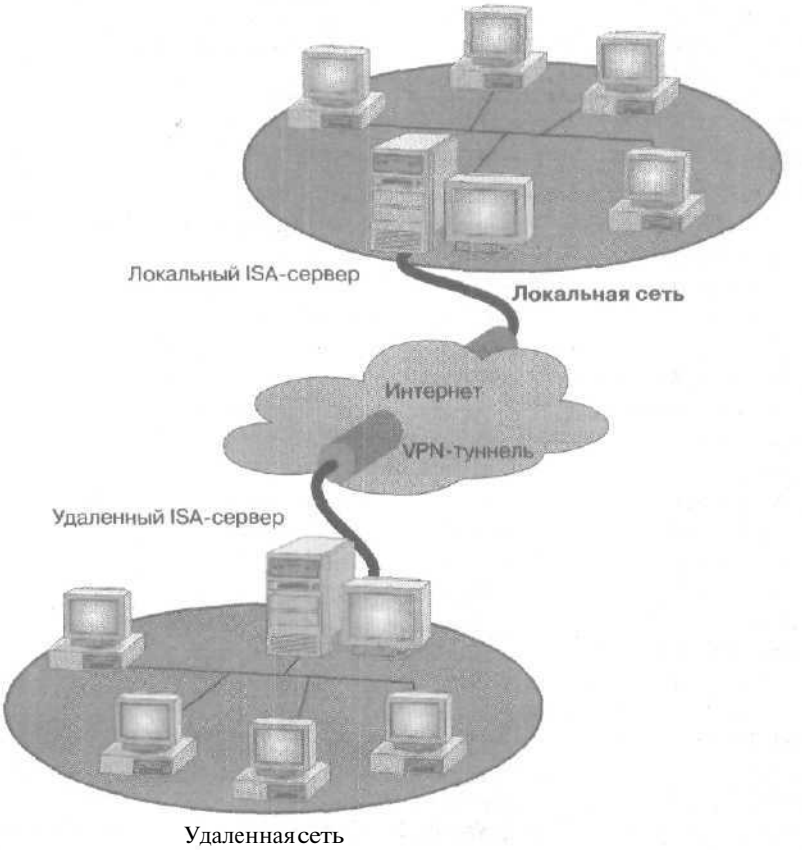


Рис. 1-8. Поддержка VPN средствами ISA-сервера

На ISA-сервере в локальной сети выполняется мастер создания локальной VPN, а на ISA-сервере в удаленной сети — мастер создания удаленной VPN. ISA-серверы подключаются к своим интернет-провайдерам (ISP). В процессе обмена информацией данные инкапсулируются и пересылаются через VPN-туннель. Основанные на отраслевых стандартах службы VPN в Windows 2000 поддерживают туннельные протоколы PPTP и L2TP/IPSec. Эти протоколы используются для управления туннелями и инкапсуляции частных данных. Для создания полноценного VPN-подключения данные, пересылаемые по туннелю, следует шифровать.

Встроенные механизмы обнаружения вторжений

В ISA-сервер встроены механизмы, которые позволяют обнаруживать атаки на сеть. Администраторы брандмауэра обычно определяют оповещения, инициируемые при обнаружении вторжения, а также ответные действия, предпринимаемые системой. В числе последних — отправка сообщения администратору по электронной почте или на пейджер, остановка службы брандмауэра, создание записи в журнале событий Windows 2000 или запуск заранее определенной программы или сценария. Обнаружение вторжений на ISA-сервере выполняется как на уровне фильтров пакетов, так и фильтров приложений.

Примечание Функции обнаружения вторжений ISA-сервер основываются на технологии, полученной по лицензии от компании Internet Security Systems Inc. (ISS), расположенной в Атланте, штат Джорджия (адрес в Интернете — *http://www.iss.net*).

Обнаружение вторжений с помощью фильтров пакетов

Перечисленные далее типы атак ISA-сервер обнаруживает на уровне фильтров пакетов.

- **Сканирование всех портов (port scan)** — попытка подключиться к большему числу портов, чем настроено на сервере.
- **Атака перечисления портов (enumerated port scan)** — попытка перечислить все работающие на компьютере службы путем направления запросов на все порты и получения ответов.
- **IP-атака без создания подключения (IP half scan)** — выполняется много попыток подключиться к атакуемому компьютеру, однако атакующий уклоняется от создания подключения. Таким образом нападающий пытается обнаружить открытые порты и при этом избежать регистрации подключения системой.
- **Атака с обратной адресацией (land** attack) — предусматривает создание TCP-подключения, в котором ложный IP-адрес и порт источника совпадает с IP-адресом и номером порта атакуемого компьютера. В некоторых реализациях протокола TCP такая атака вызывает зацикливание и аварийный отказ компьютера.
- **«Ping смерти» (Ping of Death)** — к пакету запроса или контроля связи (ping) по протоколу ICMP (Internet Control Message Protocol) добавляются избыточные данные. Успешно выполненное нападение приводит к переполнению буферов ядра при попытке ответить и аварийному отказу компьютера.
- **UDP-бомба (UDP-bomb)** — отправка атакуемому некорректного UDP-пакета. В некоторых ранних версиях операционных систем получение UDP-пакета с ошибочными значениями в определенных полях вызывает разрушение ОС.
- **Атака передачи срочных данных в Windows (Windows out-of-band attack)** — предпринимается в попытке вызвать отказ в обслуживании компьютера, защищенного ISA-сервером. Успешное нападение вызывает аварийный отказ компьютера или нарушение его подключения к сети.

На ISA-сервере также предусмотрены фильтры приложений с поддержкой POP и DNS, которые анализируют весь входящий трафик на предмет обнаружения атак. Фильтр обнаружения атак на DNS перехватывает и анализирует весь трафик DNS, направленный во внутреннюю сеть. Фильтр обнаружения атак по POP перехватывает и анализирует весь трафик протокола POP, поступающий во внутреннюю сеть. Фильтры конфигурируются на обнаружение типов атак, описанных далее.

- **Переполнение буфера имен узлов в DNS (DNS Hostname Overflow)** происходит, когда ответ DNS на запрос имени узла превышает установленную длину. Приложения, не проверяющие длину имен узлов, могут, возвращая слишком длинное имя, вызывать переполнение внутреннего буфера, что позволяет удаленному злоумышленнику выполнять свои команды на атакуемом компьютере.
- **Переполнение буфера номера узла в DNS (DNS Length Overflow)** обусловлено ограниченной 4 байтами длиной поля IP-адресов. Создавая ответ DNS большей длины, некоторые приложения поиска в DNS переполняют внутренние буферы, предоставляя удаленному злоумышленнику возможность выполнить его любые команды.
- **Зонная передача в DNS (DNS Zone Transfer) с привилегированных портов <с номерами 1–1024)** выполняется, когда приложение клиента DNS применяется для передачи данных зоны с внутреннего сервера DNS. Номер порта источника относится к диапазону привилегированных номеров порта, указывая на клиентский процесс.
- **Зонная передача в DNS с портов верхнего диапазона (с номерами более 1024)** выполняется, когда приложение клиента DNS применяется для передачи зоны с внутреннего сервера DNS. Номер порта источника относится к диапазону номеров портов верхнего диапазона, указывая на клиентский процесс.
- **Переполнение буфера POP (POP Buffer Overflow)** — нападающий пытается получить корневой доступ к серверу POP путем переполнения внутреннего буфера на сервере.

Безопасная публикация

Для обработки входящих запросов на внутренние серверы, например SMTP, FTP, серверы базы данных и другие, на ISA-сервере применяется механизм публикации серверов. Запросы перенаправляются внутреннему серверу, расположенному ниже по иерархии, чем ISA-сервер.

Публикация серверов позволяет опубликовать в Интернете практически любой компьютер внутренней сети. При этом защита не нарушается, так как все входящие запросы и исходящие ответы проходят через [SA-сервер. При публикации сервера компьютером ISA-сервера, его IP-адресом фактически становится адрес ISA-сервера. Посетители, запрашивающие объекты, полагают, что общаются с ISA-сервером — компьютером, IP-адрес которого они используют, а на самом деле взаимодействие осуществляется с опубликованным сервером.

Например, при наличии Microsoft Exchange Server и ISA-сервера вы вправе создавать правила публикации сервера, в которых оговорена публикация сервера электронной почты в Интернете. В описанной ситуации брандмауэр ISA-сервера перехватывает электронную почту, приходящую на Exchange Server, а значит, ISA-сервер выглядит для клиентов, как сервер электронной почты. ISA-сервер позволят фильтровать трафик, пересылаемый на Exchange Server, в соответствии с любыми, заранее определенными администратором правилам и политикам. Доступ к Exchange Server никогда не предоставляет внешним пользователям напрямую — сервер расположен в своей безопасной среде и продолжает взаимодействовать с другими внутренним сетевыми службами напрямую.

Рис. 1-9 иллюстрирует, как описанным способом ISA-сервер применяется для безопасной публикации Web-серверов. Когда клиент Интернета запрашивает объект Web-сервера, запрос направляется на IP-адрес ISA-сервера. Правила Web-публикации, сконфигурированные на ISA-сервере, распознают запрос и пересылают его иа внутренний Web-сервер.

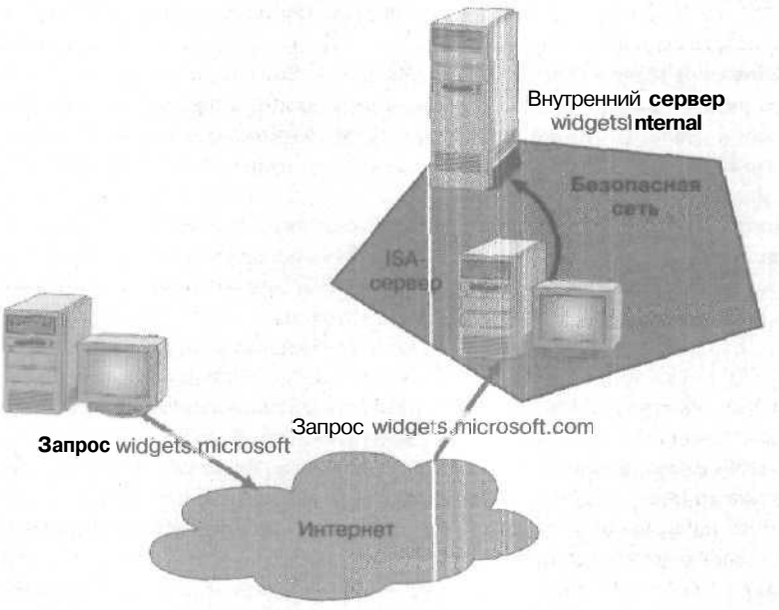


Рис. 1-9. ISA-сервер защищает опубликованные серверы внутренней сети

Резюме

Брандмауэр ISA-сервера обеспечивает фильтрацию на трех уровнях. Во-первых, контролируя прохождение IP-пакетов, ISA-сервер пропускает или блокирует подключение на основании информации о типе службы, Номере порта, имени компьютера-источника или компьютера-приемника. Фильтры пакетов IP статичны: они работают лишь на определенных портах и либо пропускают, либо блокируют прохождение пакетов. Во-вторых, ISA-сервер обеспечивает поддерживающие сеансы механизмы фильтрации на уровне каналов в форме правил политики доступа и правил публикации. Эта особенность позволяет выполнять динамическую фильтрацию пакетов и обеспечить поддержку протоколов с добавочными подключениями. И, наконец, фильтры трафика приложений на ISA-сервере применяются для анализа потоков данных отдельных приложений и выполняют особые преобразования в зависимости от типа приложения, в том числе контроль, экранирование или блокировку, перенаправление или изменение данных при проходе через брандмауэр.

Сложная многослойная структура брандмауэра ISA-сервер позволяет создавать мощные и гибкие политики управления доступом, обнаружения вторжений, безопасной публикации серверов, выделения пропускной способности в соответствии с приоритетами и интеграцией с VPN.

Занятие 3. Кэширование на ISA-сервере

Для повышения производительности сети на ISA-сервере реализован кэш, в котором хранятся часто запрашиваемые объекты. Чтобы в кэше размещались данные, наиболее часто используемые в компании и запрашиваемые пользователями Интернета, необходимо его сконфигурировать соответствующим образом.

Изучив материал этого занятия, вы сможете:

- объяснить различие между прямым и обратным Web-кэшированием;
- рассказать, как протокол Cache Array Routing Protocol используется для улучшения процедур конфигурирования кэша массива ISA-серверов;
- рассказать о преимуществах иерархических конфигураций кэширования на базе ISA-серверов.

Продолжительность занятия — около 30 минут.

Высокопроизводительный Web-кэш

Служба Web-прокси ISA-сервера поддерживает кэш Web-объектов, которые возвращаются в ответ на клиентские запросы. Если в кэше нет запрошенного объекта, инициируется новый запрос от имени клиента. Получив ответ от удаленного Web-сервера, ISA-сервер кэширует его и возвращает ответ клиенту.

В процессе быстрого кэширования в памяти ISA-сервера наиболее часто запрашиваемые данные размещаются в оперативной памяти компьютера. Это позволяет сократить время отклика, так как нужные данные извлекаются из памяти, а не с диска. ISA-сервер также поддерживает оптимизированный кэш дискового ввода-вывода, который сокращает время операций дискового чтения и записи. Перечисленные методики уменьшают время отклика и повышают общую производительность системы.

Сервер прямого Web-кэширования

ISA-сервер можно установить в качестве сервера прямого Web-кэширования, который поддерживает доступ в Интернет клиентов внутренней сети. ISA-сервер поддерживает централизованный кэш часто запрашиваемых объектов Интернета, доступ к которым осуществляется с любого браузера на компьютере, расположенном за брандмауэром во внутренней сети. На предоставление объектов из кэша уходит существенно меньше ресурсов и времени, чем на загрузку данных из Интернета. Таким образом, кэширование позволяет повысить производительность клиентского браузера, снизить время ответа на пользовательский запрос и сократить потребление пропускной способности на подключениях к Интернету.

Рис. 1-10 иллюстрирует преимущества кэширования на ISA-сервере для пользователей. Хотя на рисунке показан лишь механизм прямого Web-кэширования (когда клиенты из внутренней сети обращаются в Интернет), процесс обратного Web-кэширования (когда пользователи Интернета запрашивают ресурсы у опубликованных Web-серверов во внутренней сети) полностью аналогичен.

1. Первый пользователь (Клиент 1) запрашивает Web-объект.
2. ISA-сервер проверяет, нет ли запрошенного объекта в кэше. Так как объекта там нет, ISA-сервер запрашивает его у соответствующего сервера в Интернете.
3. Сервер в Интернете возвращает объект ISA-серверу.
4. ISA-сервер размещает копию объекта в своем кэше и возвращает объект Клиенту 1.

5. Клиент 2 запрашивает тот же самый объект.
6. Компьютер ISA-сервер возвращает объект из кэша, не обращаясь в Интернет.

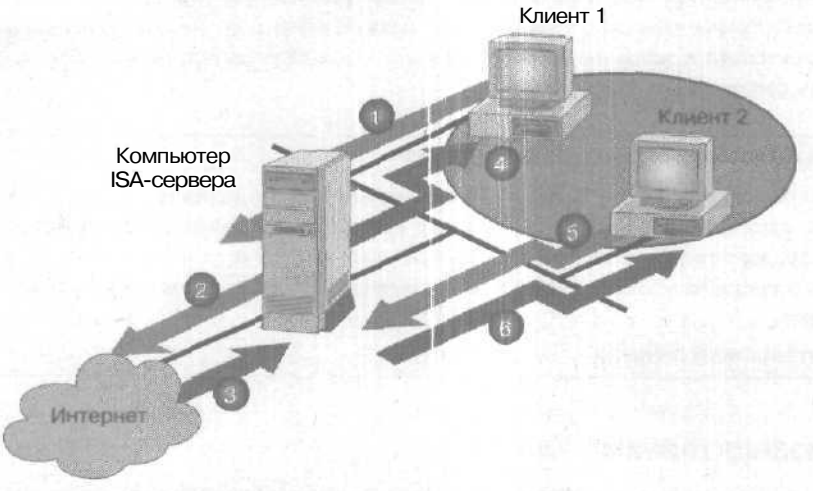


Рис. 1-10. Механизм прямого кэширования на ISA-сервере

Сервер обратного Web-кэширования

ISA-сервер можно разместить перед Web-сервером, на котором располагаются коммерческие связанные с бизнесом Web-ресурсы или который поддерживает связь с деловыми партнерами. С точки зрения внешних пользователей, ISA-сервер выполняет роль Web-сервера, обслуживая клиентские запросы Web-информации из своего кэша и переправляя запросы на Web-сервер только тогда, когда нужных данных в кэше нет.

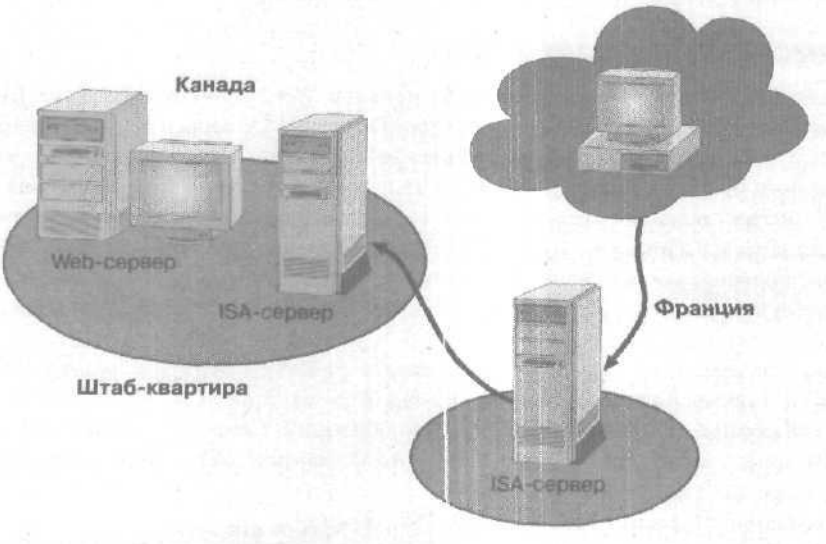


Рис. 1-11. Обратное кэширование на ISA-сервере

Как показано на рис. 1-11, когда клиент Интернета из Франции запрашивает информацию у Web-сервера, расположенного в локальной сети в Канаде, ISA-сервер во Фран-

ции анализирует запрос. Если требуемые данные имеются в кэше ISA-сервера, информация немедленно возвращается клиенту. Высокая производительность достигается за счет предоставления данных с компьютера ISA-сервера, который находится ближе к клиенту.

Если требуемого объекта на французском ISA-сервере нет, запрос переправляется на ISA-сервер в Канаде. Если объекта нет и в кэше массива в Канаде, канадский массив ISA-серверов обращается за объектом к Web-серверу,

Загрузка информации по расписанию

На ISA-сервере возможности повышения производительности кэширования расширены за счет загрузки кэша по расписанию. Служба *загрузки содержимого по расписанию* (Scheduled Content Download) позволяет получать данные по протоколу HTTP прямо в кэш ISA-сервера — как по запросу, так и по расписанию. В дальнейшем вы можете загружать в кэш ISA-сервера данные, которые, как ожидается, понадобятся клиентам в организации. Эта информация будет предоставляться пользователям непосредственно из кэша ISA-сервера, а не из Интернета.

Вы вправе загрузить как несколько страниц данных, так и содержание всего Web-узла. При создании задания на загрузку данных в кэш можно определить, какую информацию следует загружать, например лишь данные из одного домена или с заданной глубиной (числом переходов) от указанного адреса, а также ограничиться лишь загрузкой текста. Разрешается конфигурировать ISA-сервер на кэширование динамического содержания — даже если в заголовках управления кэшем протокола HTTP указано, что информация не кэшируется. Загрузка выполняется по расписанию в заданное время или периодически с определенным интервалом.

Запланированные задания загрузки настраиваются как для исходящих, так и входящих Web-запросов. Для исходящих запросов определяются наиболее часто запрашиваемые пользователями Интернета ресурсы. Далее настраиваются задания для загрузки в кэш данных из Интернета, которые в дальнейшем предоставляются пользователям внутренней сети. Для входящих Web-запросов данные локального Web-сервера загружаются в кэш ISA-сервера для предоставления информации пользователям Интернета с него, а не с Web-сервера.

Активное кэширование

ISA-сервер можно сконфигурировать на автоматическое обновление объектов кэша. При включенном активном кэшировании ISA-сервер анализирует объекты в кэше, определяя, какие из них запрашиваются особо часто. При «устаревании» популярных объектов ISA-сервер автоматически обновляет их копию в кэше,

Активное кэширование позволяет хранить в кэше и предоставлять клиентам самые свежие копии объектов, регулярно загружая их с исходного Web-сервера до истечения срока их годности. Основная цель этого — ускорение доступа для клиентов, при котором в обычных условиях потребовалось бы запросить и получить ответ от исходного сервера в процессе проверки «свежести» данных. Так как активное кэширование создает определенную нагрузку (как на прокси, так и на подключение к Интернету), обновлять рекомендуется только объекты, которые наверняка понадобятся клиентам.

Одной частоты обращения недостаточно для определения данных, нуждающихся в обновлении, ведь многие популярные страницы не успевают устареть, так как клиенты обновляют их вручную. Другие же объекты оказываются востребованными лишь короткое времени. При определении нужных объектов механизм активного кэширования следует правилу: кэшируются лишь устаревающие объекты, повторно запрашиваемые клиентами.

Протокол CARP и масштабируемость сервера кэширования

Версия Enterprise Edition ISA-сервера оснащена поддержкой протокола CARP (Cache Array Routing Protocol), который используется для обеспечения «гладкого» масштабирования и повышенной производительности при работе нескольких ISA-серверов с объединенным логическим кэшем. Для определения «пути разрешения запроса» в пределах массива в CARP используется маршрутизация, основанная на хеше. Путь разрешения запроса либо указывает точное местоположение нужной информации в массиве или в кэше подчиненного сервера, либо информирует о необходимости первичной загрузки и кэширования данных из Интернета.

CARP обладает рядом преимуществ.

- За счет четкого определения местоположения запрашиваемой информации в протоколе CARP отсутствует обмен сообщениями-запросами между прокси-серверами, который обычно выполняется в сетях с протоколом ICP (Internet Cache Protocol) и увеличивает нагрузку на сеть, особенно при большом числе серверов.
- CARP устраняет дублирование информации, которое при других условиях случается в массиве прокси-серверов. В сети *с* ICP в кэшах массива из пяти серверов может быстро накапливаться дублирующая информация, полученная с наиболее часто запрашиваемых URL-адресов. Основанная на хеше маршрутизация в CARP предотвращает дублирование, поддерживая единый логический кэш на всех пяти прокси-серверах. В результате время ответа на запрос существенно уменьшается, кроме того, гораздо эффективнее используются ресурсы сервера.
- CARP обеспечивает эффективную масштабируемость при росте числа серверов. Благодаря основанной на хеше маршрутизации, не нужен обмен сообщениями между равноправными узлами, а значит, CARP работает быстрее и эффективнее при добавлении дополнительных прокси-серверов. Этот механизм существенно отличается от механизма протокола ICP, в котором для определения местоположения нужной информации применяются сообщения — чрезвычайно неэффективный процесс, инициирующий значительный добавочный сетевой трафик. Массивы ICP характеризуются «отрицательной масштабируемостью», то есть, чем больше серверов в массиве, тем больше запросов в сети, что, естественно, перегружает сеть.
- CARP автоматическиреконфигурируется при добавлении или удалении серверов массива. Благодаря основанной на хеше маршрутизации, при добавлении или удалении серверов требуется лишь незначительное переназначение в кэше информации с различных URL-адресов.
- CARP обеспечивает управляемое распределение данных в кэше между серверами массива — равномерное или в соответствии коэффициентами, определенными для отдельных серверов.

За счет четкого определения местоположения запрашиваемой информации в CARP не нужно поддерживать объемные таблицы расположения информации кэша. Браузер выполняет с объектами стандартные операции.

ISA-серверы массива иногда имеют различное по мощности оборудование, что требует распределять нагрузку кэширования неравномерно. В протоколе CARP предусмотрена перенастройка конфигурации с определением коэффициентов нагрузки для отдельных серверов массива.

Кроме того, CARP поддерживает раздельную настройку для входящих и исходящих Web-запросов. Например, можно разрешить CARP для исходящих запросов и запретить для входящих.

Иерархическое кэширование

Версия Enterprise Edition ISA-сервера поддерживает так называемое *иерархическое кэширование,* или кэширование в цепочках. Под иерархией (или цепочкой) подразумевается структура, состоящая из ISA-серверов или их массивов. В процессе поиска требуемого объекта в кэше клиентские запросы пересылаются вверх по иерархии. После обнаружения искомого объекта результат запроса проходит через кэши всех серверов в цепочке, пока не возвращается клиенту. Иерархии — это эффективное средство распределения нагрузки между серверами и обеспечения отказоустойчивости. Администраторы вправе создавать иерархии ISA-серверов в филиалах и подразделениях.

На рис. 1-12 показан клиент в филиале, запрашивающий информацию в Интернете. Запрос поступает на ISA-сервер филиала, а затем (но до обращения в Интернет) — в региональное отделение или штаб-квартиру. После извлечения нужной информации из Интернета ISA-сервер в штаб-квартире кэширует ее и возвращает ISA-серверу филиала, который в свою очередь также кэширует данные и только после этого возвращает их клиенту. Преимущество иерархического кэширования в приведенной схеме заключается в том, что при первичном обращении данные пересылаются из Интернета через штаб-квартиру, а при повторных запросах — предоставляются непосредственно из массива ISA-серверов в филиале.

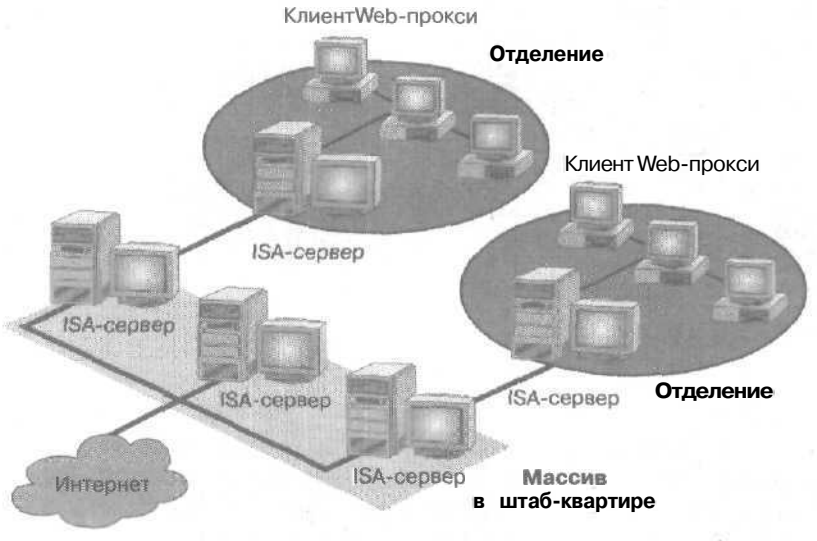


Рис. 1-12. Иерархическое кэширование

Иерархическое кэширование важно для бизнеса, так как обеспечивает максимальную близость информации в кэше к потребителю. Например, на предприятии механизм кэширования охватывает не только центральное местоположение на краю сети организации, а распространяется на уровень рабочих групп и филиалов. У сети интернет-провайдера структура кэширование может кроме центральной охватывать и региональные точки присутствия. Кроме того, кэширование по цепочке обеспечивает отказоустойчивость, создавая резервные маршруты, которые используются в случае выхода из строя основного маршрута.

Маршрутизация Web-прокси

Концепция создания иерархии (или цепочек) серверов получила развитие в правилах маршрутизации Web-прокси, которые подразумевают условную маршрутизацию, в зависимости от адресата. Представьте себе, что компания установила ISA-сервер в своем филиале

в Великобритании и подключила его к местному интернет-провайдеру. Далее администраторы настроили правило маршрутизации на ISA-сервере в филиале, предусматривающее перенаправление запросов к британским узлам Интернета локальному интернет-провайдеру, а всех остальных запросов — на массив ISA-серверов в штаб-квартире в США. Здесь подчиненный ISA-сервер в британском филиале пользуется преимуществами кэша на ISA-сервере в штаб-квартире. Дополнительным преимуществом также является добавочное кэширование локальных объектов, загруженных на ISA-сервер в филиале, через локального интернет-провайдера.

Рис. 1-13 иллюстрирует, как запросы Web-прокси перенаправляются на разные серверы в зависимости от адреса запрашиваемых узлов. ISA-сервер в филиале переправляет в Интернет все клиентские запросы Web-узлов внутри страны. Запросы других узлов направляются вверх по иерархии на ISA-сервер в США.

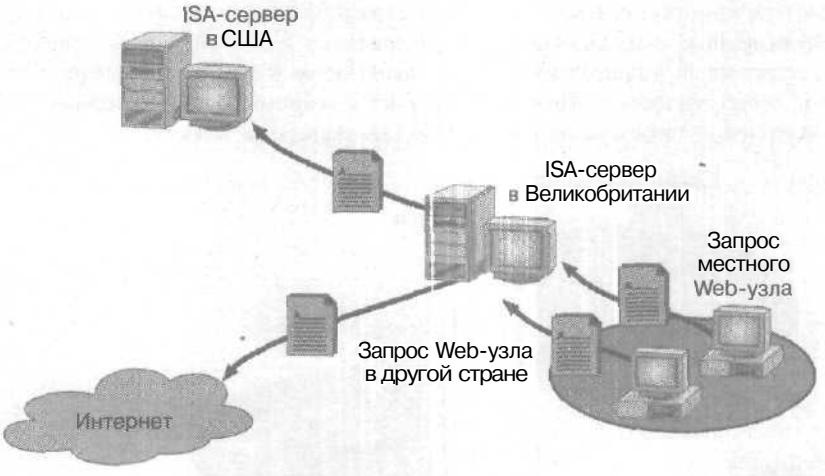


Рис. 1-13. Маршрутизация Web-прокси

Резюме

ISA-сервер применяется для совершенствования связи между локальной сетью и Интернетом. Выполняя прямое Web-кэширование, ISA-сервер сохраняет данные для клиентов внутренней сети при их обращении к данным в Интернете. Обратное Web-кэширование используется для обслуживания запросов внешних клиентов, обращающихся к опубликованным серверам во внутренней сети. В обеих описанных ситуациях ISA-сервер облегчает и ускоряет доступ пользователей к информации.

Механизм кэширования на ISA-сервере также предоставляет и другие возможности:

- **кэширование по расписанию** — поддерживается конфигурирование ISA-сервера для плановой загрузки в кэш часто запрашиваемой информации из Интернета;
- **активное кэширование** — автоматическая загрузка часто изменяемых данных в периоды снижения сетевого трафика;
- **распределенное кэширование** — версия Enterprise Edition ISA-сервера поддерживает протокол CARP, который позволяет объединять кэши многих ISA-серверов в единый логический кэш;
- **иерархическое кэширование** — ISA-серверы версии Enterprise Edition объединяются в иерархическую структуру с созданием цепочек кэшей. В этом случае клиенты, как правило, получают запрошенную информацию из кэша самого географически близкого к ним сервера.

Занятие 4. Особенности управления ISA-сервером

Отраслевые исследования показывают, что большинство изъянов зашиты обусловлено неудовлетворительной настройкой брандмауэров, а не плохой работой оборудования или программного обеспечения. ISA-сервер упрощает обеспечение безопасности, облегчая процедуры внедрения надежного брандмауэра путем предоставления интуитивно понятных, но тем не менее мощных средств управления.

Изучив материал этого занятия, вы сможете:

- рассказать, как средствами ISA-сервера обеспечить централизованное администрирование и как оно позволяет повысить безопасность сети;
- рассказать, как администраторы применяют политики предприятия и массивов для гибкого управления доступом в Интернет.

Продолжительность занятия — около 20 минут.

Интуитивно понятный пользовательский интерфейс

MMC-оснастка ISA Management представляет собой знакомый и удобный интерфейс для выполнения практически всех задач по администрированию ISA-сервера. Она обеспечивает простоту и управляемость процессов администрирования ISA-сервера. Графические *панели заданий* (taskpad) в ISA Management позволяют «одним щелчком мыши» решить стандартные задачи и запустить мастер, которые упрощают наиболее часто выполняемые процедуры управления, в том числе:

- начальные операции;
- конфигурированиеVPN-подключений — локальных, удаленных и типа «клиент — сервер»;
- определение правил протоколов;
- создание правил узлов и содержимого;
- создание правил пропускной способности;
- конфигурирование безопасной публикации;
- конфигурирование почтового сервера защищенного ISA-сервером, публикацию и обеспечение его безопасности, а также конфигурирование политики почтовых служб;
- обеспечение безопасности систем с ограниченными возможностями по конфигурированию пользователями.

Встроенные механизмы администрирования

ISA-сервер поддерживает функции и брандмауэра, и сервера кэширования как на отдельных серверах, так (в версии ISA Server Enterprise Edition) и в массивах. Предусмотрена также возможность устанавливать отдельные ISA-серверы для выполнения разных функций, то есть выделять отдельные компьютеры для разных компонентов, а администрирование выполнять централизованно, средствами одной оснастки. Единый механизм управления упрощает задачу одновременного управления и зашитой сети, и производительностью Web-доступа. Единый интерфейс конфигурирования политик доступа, применяемых как к брандмауэру, так и к серверу кэширования, обеспечивает непротиворечивость и последовательность процедур управления доступом в Интернет.

- Унифицированная политика и управление доступом — независимо от режима(брандмауэр, сервер Web-кэширования или смешанный) ISA-сервер предоставляет непротиворечивые процедуры управления доступом в Интернет на основании политик управле-

ния доступом. Ограничения доступа, заданные на брандмауэре, применяются и к серверу Web-кэширования.

- **Унифицированные механизмы управления** — единый интерфейс управления Web-кэшированием и брандмауэром предоставляет множество преимуществ. Брандмауэр и сервер Web-кэширования совместно используют одни службы регистрации событий, отчетности и оповещения.

Централизованное администрирование обычно обеспечивает большую безопасность. Все административные операции выполняются с одного компьютера, а заданная конфигурация применяется ко всем компьютерам, обеспечивая унификацию конфигурации политик доступа. Это особенно важно для крупных организаций, где массивы состоят из большого числа ISA-серверов.

Управление доступом на основе политик

ISA-сервер позволяет определять и проводить в жизнь единую для всей организации политику работы с Интернетом. Контроль всех входящих и исходящих запросов и применение правил доступа на ISA-сервере гарантирует выполнение требований этих политик пользователями внутренних и внешних сетей.

На ISA-сервере применяются предопределенные, настраиваемые, расширяемые и повторно используемые элементы политик, в том числе:

- **подмножества адресов клиентов** — IP-адреса или, при наличии службы каталогов Active Directory, прошедшие аутентификацию пользователи и группы;
- **подмножества адресатов во внешних сетях** — URL-адреса;
- **протоколы;**
- **типы информации** — различные виды данных в Интернете, например файлы со звуком, видео, текстом или изображениями. Поддерживается более подробная детализация, например файлы с расширениями .wav, .mp3, .mov или .gif;
- **задания (графики);**
- **приоритеты пропускной способности.**

Эти и другие элементы политики определяются в оснастке ISA Management (рис. 1-14).

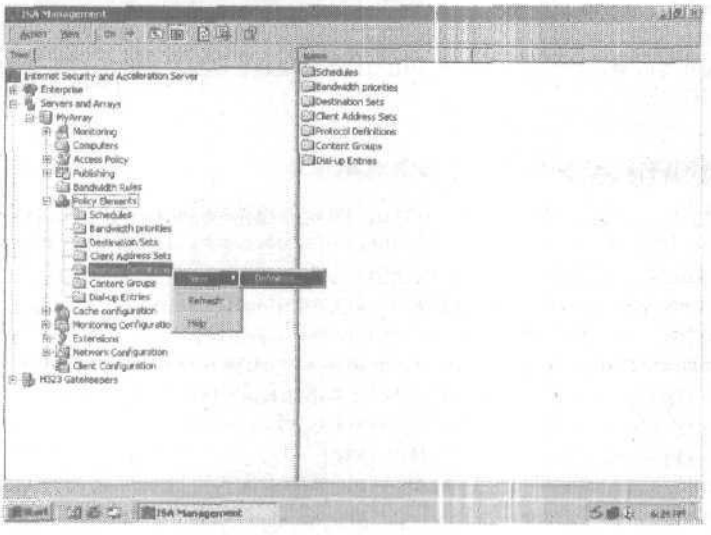


Рис. 1-14. Определение нового элемента политики

После определения элементы политики используются для создания политик доступа, которые состоят из названий протоколов и правил узлов и содержимого. Правила протоколов (рис. 1-15) определяют перечень протоколов разрешенных для взаимодействия между локальной сетью и Интернетом. Например, правило протокола, которое разрешает клиентам работать по протоколу HTTP. Правила узлов и содержимого определяют, какие данные узлов Интернета доступны клиентам внутренней сети, защищенной ISA-сервером. В том числе посредством правил, к примеру, можно предоставлять клиентам ничем не ограниченный доступ к любым узлам Интернета.

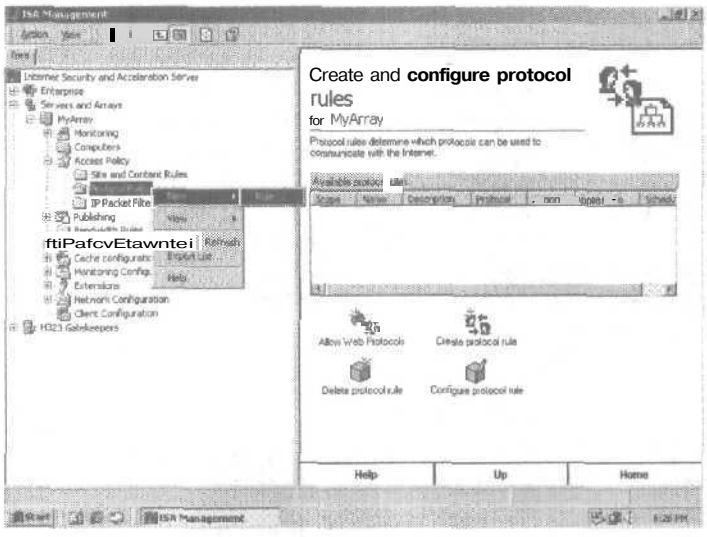


Рис. 1-15. Конфигурирование политики доступа путем настройки правил

Кроме конфигурирования политики доступа в Интернет администраторы вправе настраивать политику публикации серверов для доступа внешних клиентов. Эти политики состоят из правил публикации серверов или правил Web-публикации. Правила публикации серверов фильтруют все входящие запросы, при необходимости преобразуют их и направляют соответствующим серверам во внутренней сети. Правила Web-публикации преобразуют и пересылают входящие запросы на Web-серверы внутренней сети, защищенной ISA-сервером.

Многоуровневая политика

Версия Enterprise Edition ISA-сервера поддерживает два уровня политики — массива и предприятия.

Примечание Версия Standard Edition ISA-сервера поддерживает только политику автономного сервера.

Политика массива

ISA Server Enterprise Edition устанавливается либо как автономный сервер, либо в качестве узла массива, В массиве или на автономном сервере *политика массива* состоит из правил узлов и содержания, правил протоколов, фильтров IP-пакетов, правил Web-публикации и правил публикации серверов. Для всех членов массива задана единая конфигурация, что облегчает управление и администрирование. При изменении конфигурации массива изменяются параметры всех ISA-серверов массива, в том числе все политики доступа и кэширования.

Политика предприятия

Политика предприятия стоит на уровень выше. Ее можно применить к одному или нескольким массивам в корпоративной сети. Политика предприятия состоит из правил протоколов и правил узлов и содержания. Она применяется к любому массиву (рис. 1-16) и расширяется за счет собственной политики массива.

Рис. 1-16. Политику предприятия можно применять к нескольким массивам

Разрешение поддержки обеих политик — предприятия и массива — позволяет обеспечить реализацию единой корпоративной политики во всей организации. В то же время можно предоставить локальным администраторам право по мере необходимости изменять конфигурацию на уроне отделов или филиалов. Например, политика предприятия разрешает доступ по протоколу HTTP и запрещает любые другие протоколы. На уровне массива, где действует указанная политика предприятия, разрешается добавить правило, ограничивающее круг субъектов, которым доступен протокол HTTP. Переопределение политики предприятия политикой массива запрещено, то есть в массиве нельзя разрешить связь по другим протоколам.

Резюме

ISA-сервер упрощает обеспечение безопасности, облегчая процедуры установки защищенного брандмауэра и сервера кэширования, а также предоставляя интуитивно понятные, но тем не менее мощные средства управления. Графические *панели заданий* (taskpad) в ISA Management позволяют «одним щелчком мыши» решать стандартные задачи и запускать мастер, которые упрощают наиболее популярные процедуры управления: Централизованное администрирование обычно обеспечивает большую безопасность. Все административные операции выполняются с одного компьютера, а заданная конфигурация применяется ко всем компьютерам, обеспечивая унификацию конфигурации политик доступа.

ISA-сервер позволяет определять и проводить в жизнь единую для всей организации политику работы с Интернетом посредством назначения правил для предопределенных и пользовательских элементов политик. Разрешение поддержки и конфигурирование обеих политик — предприятия и массива — позволяет обеспечить реализацию единой корпоративной политики во всей организации. В то же время можно предоставить локальным администраторам право по мере необходимости изменять конфигурацию на уровне отделов или филиалов.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия, Ответы для самопроверки — в приложении А «Вопросы и ответы» в конце книги.

1. Какой протокол позволяет браузерам автоматически подключаться к ISA-серверу?

2. Какие функции выполняет фильтр редиректора HTTP?

3. Как и когда в конфигурации ISA-сервер применяется служба каталогов Active Directory?

4. Каковы преимущества протокола CARP по сравнению с протоколом ICP?

5. Зачем применяются многоуровневые политики в версии ISA Server Enterprise Edition?

6. Какая возможность в Windows 2000 Advanced Server или Windows 2000 Datacenter Server позволяет повысить производительность массива ISA-серверов версии Enterprise Edition?

ГЛАВА 2

Установка сервера Microsoft Internet Security and Acceleration Server 2000

Занятие 1. Планирование установки ISA-сервера 34

Занятие 2. Установка ISA-сервера 47

Занятие 3. Переход от Proxy Server 2.0 58

Закрепление материала 64

В этой главе

В этой главе рассказано о том, что требуется для установки ISA-сервера. Успех установки ISA-сервера во многом определяется планированием и предварительной подготовкой. Из этой главы вы узнаете, как подготовится к установке ISA-сервера, как оценить требования к сети и разработать соответствующую им сетевую структуру. Кроме того, здесь описаны процедуры инициализации предприятия, установки ISA-сервера и создания *таблицы локальных адресов* (Local Address Table, LAT), а также особенности планирования перехода от Proxy Server 2.0 к ISA-серверу (это особенно полезно администраторам).

Прежде всего

Для изучения материалов этой главы необходимо:

- выполнить процедуры установки, описанные в разделе «Об этой книге»;
- изучить материалы всех занятий главы 1.

Занятие 1. Планирование установки ISA-сервера

Прежде чем устанавливать ISA-сервер, необходимо заранее собрать информацию, которая понадобится вам в процессе установки. Следует изучить требования к сети и разработать соответствующую сетевую топологию, если, конечно, ее еще нет.

Изучив материал этого **занятия, вы** сможете:

- ✓ определять наиболее подходящий вариант установки ISA-сервера — в качестве изолированного сервера или массива;
- ✓ определять оптимальный режим работы ISA-сервера (брандмауэр, сервер кэширования или смешанный);
- ✓ определять оборудование, необходимое для выбранной конфигурации ISA-сервера;
- ✓ определять топологию сети для выбранной конфигурации ISA-сервера.

Продолжительность занятия — около 60 минут.

При планировании установки ISA-сервера следует взвесить требования к сети и практические ограничения, связанные с финансовыми затратами и производительностью, и решить:

- как устанавливать ISA-сервер — в качестве изолированного сервера или массива;
- в каком режиме должен работать ISA-сервер — как брандмауэр, как сервер кэширования или в смешанном режиме, то есть выполнять функции первого и второго;
- как организовать подключение к Интернету;
- планируется ли размещать во внутренней сети серверы, ресурсы которых публикуются в Интернете;
- какие изменения существующей структуры сети потребуются для установки ISA-сервера;
- сколько компьютеров необходимо перенастроить после установки ISA-сервера.

Планирование конфигурации оборудования и подключения

Аппаратную конфигурацию ISA-сервера и способ подключения к Интернету следует планировать в соответствии с ожидаемой сетевой нагрузкой. Далее описываются возможные конфигурации системы для различных вариантов использования ISA-сервера.

Минимальные требования к оборудованию

ISA-сервер работает на компьютере под управлением одной из версий Microsoft Windows 2000 Server. Кроме сетевого адаптера, который Windows 2000 использует для подключения ко внутренней сети, для подключения к Интернету на ISA-сервере следует предусмотреть дополнительный адаптер для внешней сети, модем или адаптер ISDN (Integrated Services Digital Network).

Далее перечислены минимальные требования к оборудованию, необходимому для работы ISA:

- компьютер с процессором Pentium II или аналогичным с рабочей частотой 300 МГц или выше, под управлением операционной системы Windows 2000 Server или Windows 2000 Advanced Server, с пакетом обновлений Service Pack 1 или более поздним или Microsoft Windows 2000 Datacenter Server;
- 256 Мбайт оперативной памяти;
- 20 Мбайт свободного дискового пространства;

- сетевой адаптер, совместимый с Windows 2000, для подключения ко внутренней сети;
- совместимый с Windows 2000 сетевой адаптер, модем или адаптер ISDN для подключения к Интернету;
- раздел с файловой системой NTFS на локальном жестком диске.

Для создания массива и применения политик предприятия в локальной сети нужна также служба каталогов Active Directory в Windows 2000.

Требования для удаленного администрирования

Для удаленного администрирования ISA-сервера с компьютера под управлением Windows 2000 Professional или любой версии Windows 2000 Server достаточно оснастки ISA Management. Для подключения к ISA-серверу компьютер, с которого выполняется удаленное администрирование, должен быть членом домена Windows 2000.

Кроме ISA Management, для управления ISA-сервером можно использовать установленную на нем службу сервера терминалов; управление осуществляется через удаленное подключение к ISA-серверу средствами клиента сервера терминалов.

Требования для брандмауэра

ISA-сервер, установленный как выделенный брандмауэр, выполняет роль безопасного шлюза в Интернет для внутренних клиентов. В этом режиме основным фактором, определяющим требования к проекту, является пропускная способность подключения — она должна быть достаточной для поддержки доступа внутренних клиентов в Интернет.

В таблице 2-1 перечислены требования к устройствам и подключению для различных значений пропускной способности, необходимой клиентам брандмауэра и SecureNAT.

Таблица 2-1. Требования к процессору и подключению к Интернету

Требования к пропускной способности	Тип процессора	Подключение к Интернету
1-25 Мбит/с	Pentium II, 300 МГц	T1, кабельный модем или xDSL
25-50 Мбит/с	Pentium III, 550 МГц	T3 или лучше
свыше 50 Мбит/с	По одному Pentium III, 550 МГц на каждые 50 Мбит/с	T3 или лучше

Требования для прямого кэширования

ISA-сервер, установленный как сервер прямого кэширования Web- и FTP-информации, централизованно хранит копии часто запрашиваемых в Интернете объектов. Кэшированные объекты доступны для браузеров всех клиентов внутренней сети организации. В этом режиме основным фактором, определяющим требования к проекту, является число клиентов, которым требуется доступ в Интернет. В таблице 2-2 перечислены аппаратные требования для предполагаемого числа внутренних клиентов, получающих доступ к объектам в Интернете.

Таблица 2-2. Требования к объему оперативной памяти и дискового пространства

Число пользователей	Компьютер ISA-сервера	Оперативная память (Мбайт)	Дисковое пространство, отведенное для кэширования
до 250	Один ISA-сервер с Pentium II, 300 МГц	256	от 2 до 4 Гбайт
до 2 000	Один ISA-сервер с Pentium III, 550 МГц	256	10 Гбайт
свыше 2 000	По одному ISA-серверу с Pentium III, 550 МГц на каждые 2000 пользователей. Используйте оснастку Performance Monitor (Производительность) для поиска «узких мест» и при необходимости добавьте дополнительные ISA-серверы в массив	по 256 на каждые 2 000 пользователей	по 10 Гбайт на каждые 2 000 пользователей

Для использования кэшируюших возможностей ISA-сервера установите его на компьютер, имеющий по крайней мере один раздел с файловой системой NTFS. Если дисковый том сервера содержит разделы файловой системы FAT (File Allocation Table), преобразуйте их в NTFS программой convert.exe, входящей в состав Windows 2000 Server. Преобразование не уничтожает данные на диске. Подробнее об использовании программы Convert можно узнать, выполнив в командной строке команду **convert /?**.

Требования для публикации и обратного кэширования

ISA-сервер, установленный между Web-сервером в частной сети организации и Интернетом, используется для предоставления доступа к размещенным на Web-сервере ресурсам, например Web-узлу электронной коммерции или информации для партнеров по бизнесу, В этом случае основним фактором, определяющим требования к проекту, является частота обращений внешних клиентов к опубликованным серверам.

В таблице 2-3 перечислены аппаратные требования для предполагаемого числа обращений внешних пользователей (из Интернета) при условии обратного кэширования.

Таблица 2-3. Аппаратные требования для обслуживания различного числа клиентских запросов

Число запросов в секунду	ISA-сервер	Оперативная память (Мбайт)
менее 500	Один ISA-сервер с Pentium II, 300 МГц	256
500-900	Один ISA-сервер с Pentium III, 550 МГц	256
более 900	По одному ISA-серверу с Pentium III, 550 МГц на каждые 800 запросов в секунду. Используйте оснастку Performance Monitor (Производительность) для обнаружения «узких мест» и при необходимости добавьте в массив дополнительные ISA-серверы	256 на сервер

ISA-сервер в составе массива

Если сетевая нагрузка требует применения нескольких компьютеров, ISA-серверы объединяются в массив. Массив представляет собой группу ISA-серверов, которые рассматриваются и управляются как единый логический объект.

Все серверы в составе массива имеют одинаковую конфигурацию. Это сокращает административные издержки, так как при настройке параметров массива конфигурируются все входящие в него серверы. Более того, в случае использования ISA Server Enterprise Edition вы вправе применить для массива политику предприятия, что позволяет централизованно управлять всеми массивами предприятия.

Для отдельных массивов предприятия разрешается назначать индивидуальные политики массива. Это позволяет разделить организацию на подразделения, чтобы, к примеру, предоставить клиентам одного массива неограниченный доступ в Интернет, а клиентам другого — ограниченый.

Кроме того, применение массива позволяет повысить производительность, сэкономив на оборудовании. В массивах запросы клиентов распределяются между несколькими ISA-серверами, благодаря чему сокращается время отклика на запрос. Распределение нагрузки между серверами массива позволяет добиться удовлетворительной производительности даже на посредственном оборудовании.

Компьютер, на котором устанавливается ISA-сервер в качестве члена массива, должен входить в домен Windows 2000. Кроме того, до начала установки необходимо инициализировать предприятие ISA-сервера. *Инициализацией предприятия* (enterprise initializing) называется процесс добавления обновлений схемы ISA-сервера в схему Active Directory.

Когда создания массивов ISA-серверов не требуется, ISA-сервер обычно устанавливается на изолированный сервер. В этом случае компьютер с ISA-сервером не обязательно должен входить в домен Windows 2000.

Требования для массива

Необходимо, чтобы все серверы в составе массива входили в один домен и сайт. Сайт — это несколько компьютеров, соединенных между собой быстрой сетью по протоколу TCP/IP (Transmission Control Protocol/Internet Protocol). Домен представляет собой совокупность назначенных администратором компьютеров, записи которых содержатся в общем хранилище каталога (Active Directory). Подробнее о доменах и сайтах — в справочной системе Windows 2000.

Примечание При установке серверов массива на компьютеры с Windows 2000 Advanced Server или Windows 2000 Datacenter Server рекомендуется (но не обязательно) использовать балансировку сетевой нагрузки между компонентами массива.

Изолированные серверы и массивы из одного сервера

Установить ISA-сервер в качестве члена массива можно даже на один компьютер. При установке сервера ISA Server Enterprise Edition в массив к нему обычно применяется политика предприятия. Кроме того, установка сервера в качестве члена массива упрощает расширение проекта в будущем, так как в него без проблем удается ввести дополнительные компьютеры.

В таблице 2-4 сравниваются особенности установки ISA-сервера как члена массива и как изолированного сервера.

Таблица 2-4. Сравнение особенностей массива и изолированного сервера

	Массив	Изолированный сервер
Масштабируемость	Один и более компьютеров	Только один компьютер
Необходимость работы с Active Directory	Устанавливается только в домены Windows 2000 со службой каталогов Active Directory. В то же время клиенты в локальной сети могут оставаться в домене Windows NT 4.0	Active Directory не требуется. Разрешается устанавливать в домены Windows NT 4.0. Информация о конфигурации хранится в реестре
Политика предприятия	Возможность применять единую политику ко всем массивам предприятия	Не применяется

Настройку параметров массивов разрешается выполнять индивидуально в каждом подразделении организации. При этом и массиве подразделения применяются собственные политики, общие для всех серверов данного массива.

Режимы работы ISA-сервера

До начала установки ISA-сервера выберите один из трех режимов его работы: в качестве брандмауэра (Firewall), сервера кэширования (Cache) или смешанный режим (Integrated).

В режиме брандмауэра и смешанном режиме ISA-сервер обеспечивает сетевую безопасность, параметры которой определяются правилами обмена между корпоративной сетью и Интернетом. Кроме того, эти режимы позволяют публиковать ресурсы внутренних серверов, предоставляя доступ к хранящимся на них данным пользователям Интернета.

В режиме сервера кэширования и смешанном режиме ISA-сервер позволяет повысить производительность сети и снизить использование пропускной способности, локально храня часто запрашиваемые из Интернета объекты. Также эти режимы дают возможность направлять запросы из Интернета к различным внутренним Web-серверам.

Возможности ISA-сервера зависят от выбранного режима. В таблице 2-5 перечислены возможности режимов брандмауэра *л* сервера кэширования. В смешанном режиме доступны все возможности.

Таблица 2-5. Сравнение возможностей режимов брандмауэра и сервера кэширования

Возможность	Режим брандмауэра	Режим кэширования
Политика доступа	Да	Да, но только для протокола HTTP
Оповещения	Да	Да
Фильтры приложений	Да	Нет
Настройка кэша	Нет	Да
Политики предприятия	Да	Да
Фильтры пакетов	Да	Нет
Мониторинг в реальном времени	Да	Да
Отчеты	Да	Да
Публикация серверов	Да	Нет
Web-публикация	Да	Да

Подключение к Интернету

Выбор подходящего *интернет-провайдера* (Internet Service Provider, ISP) — первый шаг при подключении организации к Интернету. Из-за высокой конкуренции в этой сфере провайдеры предлагают клиентам множество способов доступа в Интернет, в том числе по линиям DSL (Digital Subscriber Line), посредством кабельных модемов, спутниковой связи, по телефонным линиям и линиям T1. При выборе следует учесть стоимость подключения, его пропускную способность и надежность.

Существует два вида подключения ISA-сервера к Интернету — прямое (постоянное) или по телефонной линии. Для прямого подключения, а также для подключения при помощи DSL или кабельного модема требуется адаптер для внешней сети. Для подключения по телефонной линии необходим модем или адаптер ISDN.

Для ISA-сервера, публикующего ресурсы серверов, которые должны быть всегда доступны из Интернета, необходимо зарезервировать статические IP-адреса у интернет-провайдера и по крайней мере одно доменное имя в регистрирующей организации, аккредитованной в ICANN (Internet Corporation for Assigned Names). Список таких организаций публикуется в Интернете по адресу *http://www.icann.org/registrars/accredited-list.html*. При этом для доступа к вашим внутренним серверам лучше использовать *полные доменные имена* (Fully Qualified Domain Name, FQDN), состоящие из имени компьютера (узла), например «www», и зарегистрированного доменного имени, например «microsoft.com».

После регистрации доменного имени вы можете поручить своему интернет-провайдеру сопровождение и администрирование соответствующих записей системы DNS (Domain Name System), обеспечивая доступность имени пользователям Интернета.

Публикация и подключение

Для публикации ресурсов внутренних серверов необходимо получить IP-адреса, которым сопоставлены имена доменов или серверов. Когда внешние клиенты запрашивают Web-узел или Домен, DNS-сервер находит IP-адрес, соответствующий запрашиваемому имени Web-узла. Как правило, это IP-адрес ISA-сервера или сервера в сети периметра (DMZ). Альтернативное решение заключается в использовании внутреннего DNS-сервера, разрешающего запросы внешних клиентов.

ISA-сервер в сети

ISA-сервер обеспечивает безопасность и подключение сетевых служб, работающих на одном или нескольких серверах. Далее речь пойдет об особенностях сетей, которые следует учитывать при установке ISA-сервера.

Домен Windows NT 4.0

ISA-сервер можно установить в качестве изолированного сервера в домене Windows **NT** 4.0. В этом случае дополнительного конфигурирования не требуется.

Кроме того, для подключения и обеспечения безопасности пользователей и клиентов домена Windows **NT** 4.0 используются массивы. При этом массив ISA-серверов устанавливается в отдельном домене Windows 2000, после чего между доменом Windows **NT** 4.0 и доменом ISA-сервера настраиваются доверительные отношения.

Информация о конфигурации ISA-сервера

Информация о конфигурации ISA-сервера, установленного на изолированный сервер, хранится в реестре.

Информация о конфигурации ISA-сервера в составе массива размещается в базе данных Active Directory. Другими словами, применение массивов ISA-серверов требует установки Active Directory в домене Windows 2000, членом которого ISA-сервер является.

Сервер подключения к Интернету

До появления ISA-сервера многие организации использовали *общий доступ для подключения к Интернету* (Internet Connection Sharing, 1CS). ISA-сервер заменяет ISC, предоставляя компаниям дополнительные возможности. Кроме подключения частной сети к Интернету, ISA-сервер обеспечивает надежную безопасность и кэширование.

Внимание! **Не** устанавливайте и не включайте ICS на компьютере с ISA-сервером, Если служба ICS была установлено ранее, удалите ее до установки ISA-сервера.

Сервер удаленного доступа

До появления ISA-сервера многие организации использовали сервер удаленного доступа Windows 2000 Server для подключения удаленных клиентов к сетевым службам и компьютерам. ISA-сервер обеспечивает подключение удаленных клиентов и дополнительные возможности сервера удаленного доступа наряду с надежной и гибкой системой безопасности. Фильтры пакетов сервера удаленного доступа заменяются фильтрами пакетов ISA-сервера. Кроме того, ISA-сервер использует записи удаленного доступа сервера удаленного доступа и расширяет их функциональность.

ISA-сервер в сетях различной топологии

ISA-сервер применяется в сетях различной топологии. В этом разделе описывается несколько типовых конфигураций сети. Несмотря на то, что в действительности структура сети обычно отличается от описанной, изложенные адесь основные подходы и методы конфигурирования помогут вам при планировании сетевой топологии вашей организации.

Сеть малого офиса

В сети малого офиса ISA-сервер располагается между локальной (LAN) или глобальной (WAN) сетью и Интернетом. Сегмент локальной сети малого офиса, как правило, содержит менее 250 клиентов, и в нем используется IP-протокол и подключение к интернет-провайдеру по телефонной линии. Один ISA-сервер обеспечивает подключение и безопасность для всей сети, как показано на рис. 2-1.

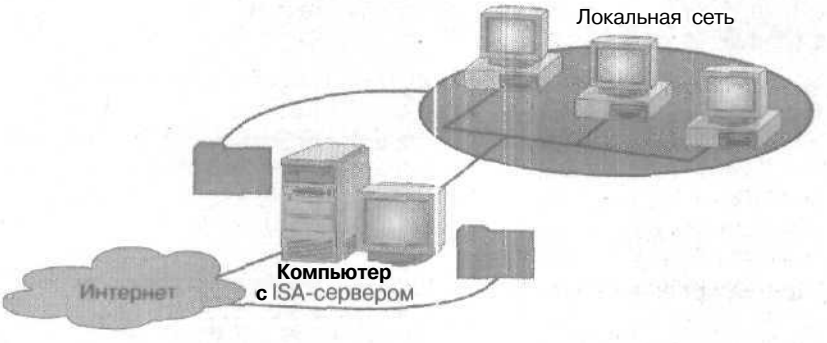


Рис. 2-1. Проект для малого офиса

На рис. 2-1 показано решение для небольшой организации, массив которой содержит только один компьютер с ISA-сервером. Чтобы обеспечить возможность расширения в будущем, сервер следует установить как член массива.

Если организация немного больше, можно использовать массив из нескольких ISA-серверов. Принимая во внимание, что значительная часть клиентов располагается в одном местоположении и входит в один домен, единственный массив ISA-серверов способен обслуживать всю организацию. Число компьютеров в массиве зависит от требований к пропускной способности и кэшу.

Сеть предприятия

На рис. 2-2 показана сеть большой корпорации со штаб-квартирой в США и двумя отделениями — в Канаде и Великобритании- Во всех трех местоположениях установлены массивы, состоящие из одного и более ISA-серверов. В штаб-квартире действует политика предприятия, определяющая правила доступа для всех клиентов. Сетевой администратор штаб-квартиры отвечает за применение корпоративной политики и ее соблюдение во всех отделениях. При этом администраторам отделений разрешается создавать только более строгие правила.

Структура сети предприятия

Канадское отделение подключено к штаб-квартире через маршрутизатор, а британское — посредством *виртуальной частной сети* (Virtual Private Network, VPN).

На рис. 2-2 показана структура сети корпорации.

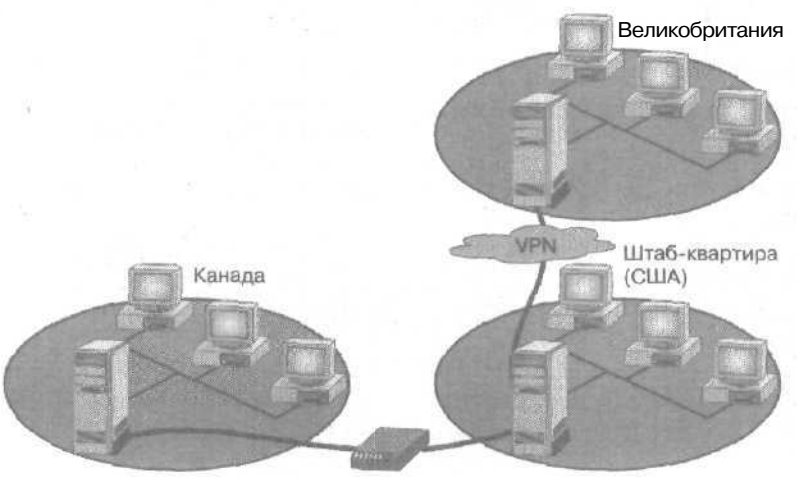


Рис. 2-2. Структура сети корпорации

Каждый ISA-сервер в составе массива в штаб-квартире оснащен двумя сетевыми интерфейсами: один сетевой адаптер подключен к внутренней сети, а другой — к Интернету. В этом проекте возможно применение прямого подключения к интернет-провайдеру посредством маршрутизатора и линии T1 или E1 с резервным подключением по телефонной линии на случай выхода из строя основной.

Канадский ISA-сервер работает в режиме сервера кэширования и подключен к вышестоящему ISA-серверу в штаб-квартире. Канадский сервер также оснащен двумя сетевыми адаптерами, один из которых подключен к локальному маршрутизатору, а другой — к маршрутизатору в штаб-квартире.

Массив ISA-серверов в Великобритании работает в смешанном режиме, выполняя роли брандмауэра и кэширующего сервера. Кроме того, эти ISA-серверы настроены для маршрутизации запросов к местным ресурсам Интернета непосредственно в Интернет.

Проекты, предполагающие публикацию в Web

Функция публикации Web-узлов в ISA-сервере нужна организациям, желающим безопасно публиковать в Интернете ресурсы своих защищенных интрасетей. В этом случае ISA-сервер обеспечивает безопасность Web-сервера организации, на котором располагаются Web-узлы электронной коммерции или информация для деловых партнеров. Для внешних пользователей ISA-сервер выглядит как Web-сервер, в то время как последний сохраняет доступ к службам внутренней сети.

Опубликованный Web-сервер располагается на том же компьютере, что и ISA-сервер, или на отдельной машине.

Web-сервер, совмещенный с ISA-сервером

На рис. 2-3 показано одно из распространенных решений для Web-публикации, в котором Web-сервер размещается на том же компьютере, что и ISA-сервер.

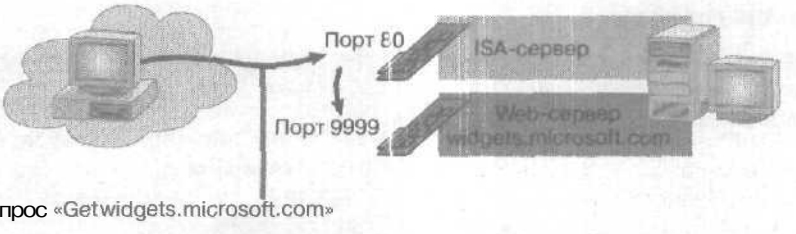


Рис. 2-3. Web-сервер, совмещенный на одном компьютере с ISA-сервером

В этой конфигурации сети ISA-сервер ожидает входящие запросы на порту 80 адаптера внешнего интерфейса.

По умолчанию Web-сервер также ожидает входящие запросы на порту 80. Во избежание конфликта Web-сервер необходимо перенастроить на другой порт, после чего изменить правило Web-публикации ISA-сервера так, чтобы принятые запросы перенаправлялись на соответствующий порт Web-сервера.

Вместо этого вы можете указать в параметрах сервера IIS (Internet Information Services) другой IP-адрес для входящих запросов. Например, если задать IP-адрес для входящих запросов — 127.0.0.1, они будут приниматься только с локального компьютера, то есть с ISA-сервера.

Web-сервер в локальной сети

На рис. 2-4 показан пример, в котором Web-серверы размещены за ISA-сервером.

Два Web-серверы расположены во внутренней сети, защищенной ISA-севером. Когда пользователь Интернета запрашивает объект в example.microsoft.com/Marketing или example.microsoft.com/Development запрос направляется ISA-серверу, который затем пересылает его соответствующему Web-серверу

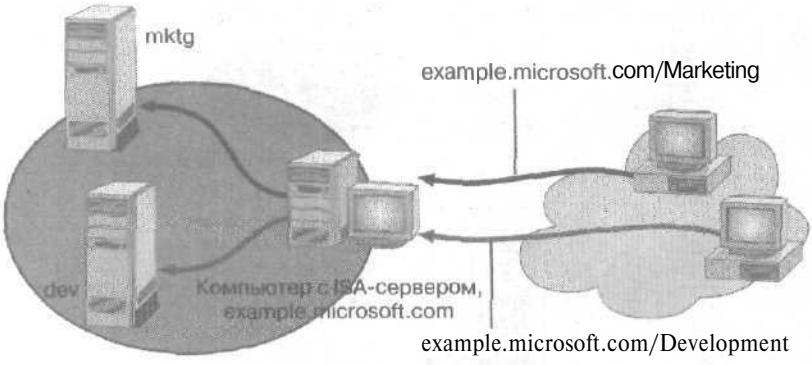


Рис. 2-4. Web-серверы, расположенные за ISA-сервером

Обратите внимание, что, когда внешние клиенты запрашивают объекты с Web-серверов, они фактически получают доступ только к ISA-серверу. Таким образом, он предотвращает доступ внешних пользователей в частную сеть. При этом IP-адреса Web-серверов не раскрываются, а клиенты из Интернета получают запрошенное у Web-сервера содержимое с IP-адреса ISA-сервера.

Проекты, предполагающие использование сервера Exchange

Как правило, в проектах с ISA-сервером требуется защитить данные, пересылаемые между почтовыми серверами по протоколу SMTP (Simple Mail Transfer Protocol). Например, ISA-сервер иногда обеспечивает безопасность Microsoft Exchange Server. При этом сервер Exchange может располагаться, как на одном компьютере с ISA-сервером, так и в локальной сети или в сети периметра (DMZ).

Сервер Exchange, совмещенный с ISA-сервером

На рис. 2-5 показан пример, когда ISA-сервер располагается на одном компьютере с сервером Exchange.

Рис. 2-5. Сервер Exchange, совмещенный с ISA-сервером

Сервер Exchange в локальной сети

На рис. 2-6 показан пример, когда сервер Exchange располагается в локальной сети, защищенной ISA-сервером.

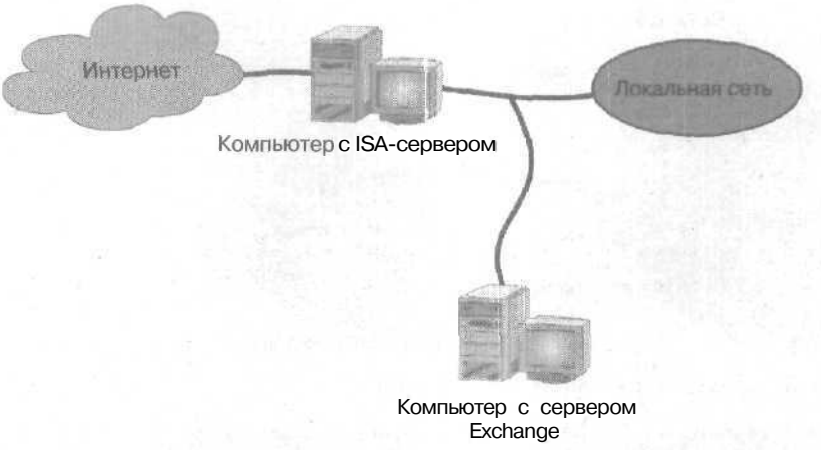


Рис. 2-6. Сервер Exchange в локальной сети под защитой ISA-сервера

Проекты, предполагающие использование сети периметра

Сеть периметра (perimeter network), или DMZ — это небольшая сеть, отделенная как от Интернета, так и от частной сети организации. Внешние пользователи получают доступ только к расположенным в ней серверам, и не допускаются во внутреннюю корпоративную сеть. Кроме того, организация, как правило, предельно ограничивает доступ во внутреннюю сеть с компьютеров в сети периметра.

Сеть периметра, называемую также *экранированной подсетью* (screened subnet), обычно используют для размещения почтовых и Web-серверов компании. Далее показаны два варианта структуры сети периметра:

- вариант *«сдвоенных»* (back-to-back) ISA-серверов, один из которых используется для подключения сети периметра к Интернету, а другой — для подключения внутренней сети к сети периметра (рис. 2-7);
- вариант с одним ISA-сервером с тремя адаптерами, обеспечивающим безопасность как сети периметра, так и локальной сети.

Корпоративные Web-серверы размещают в сети периметра, чтобы их ресурсы были доступны из Интернета. Вместе с тем, сеть периметра препятствует доступу к каким-либо другим данным на компьютерах в локальной сети. По этой причине злоумышленник, даже если он преодолеет защиту сети периметра, сможет скомпрометировать только расположенные в ней серверы.

Сеть периметра со сдвоенными ISA-серверами

В этом варианте подключение сети периметра к Интернету и локальной сети обеспечивается двумя ISA-серверами, расположенными по разные стороны сети периметра. Соответствующая структура сети показана на рис. 2-7.

В этой сети два ISA-сервера подключены друг к другу, при этом один подключен к Интернету, а второй — к локальной сети. Оба ISA-сервера работают в режиме брандмауэра или в смешанном режиме, что существенно снижает риск компрометации, так как для того, чтобы попасть во внутреннюю сеть, злоумышленнику придется взломать обе системы.

Рис. 2-7. **Сеть периметра со сдвоенными ISA-серверами**

Сеть периметра с одним ISA-сервером с тремя адаптерами

В этом варианте на одном ISA-сервере (или на каждый компьютер в составе массива) установлены три сетевые карты. Соответствующая структура сети показана на рис. 2-8.

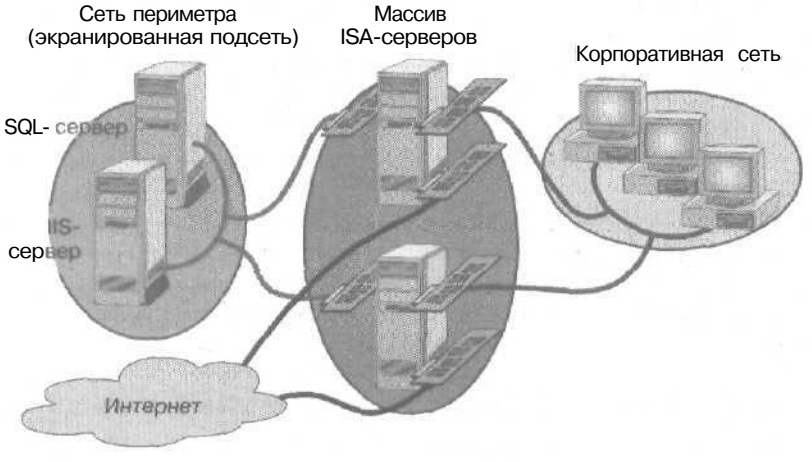


Рис. 2-8. Сеть периметра с одним ISA-сервером с тремя адаптерами

Резюме

Подготовка к установке ISA-сервера начинается с оценки требований к сети и разработки соответствующей сетевой топологии. Определяя требования к оборудованию для ISA-сервера, следует предусмотреть некоторую избыточность ресурсов для ожидаемой сетевой нагрузки. Для брандмауэра важно учесть пропускную способность, которая потребуется для доступа внутренних клиентов в Интернет, для кэширующего сервера — количество клиентов с Web-браузерами, запрашивающих ресурсы из Интернета, а для публикации и обратного кэширования — частоту обращений внешних клиентов к объектам публикующих серверов. После оценки требований необходимо выбрать режим работы ISA-сервера; в качестве брандмауэра (Firewall), сервера кэширования (Cache) или смешанный (Integrated) режим. Если сетевая нагрузка требует применения нескольких компьютеров, используются не изолированные ISA-серверы, а массивы.

ISA-серверы применяются в сетях с различными топологиями. В проектах для малого офиса один ISA-сервер размещается между корпоративной локальной сетью и Интернетом. В более крупных и географически распределенных предприятиях в каждом местоположении располагается массив из одного или нескольких ISA-серверов.

При публикации защищенных брандмауэром ресурсов опубликованные почтовые или Web-серверы разрешается размещать на одном компьютере с ISA-сервером или на другом компьютере в частной сети. Для повышения безопасности опубликованные серверы размещаются в сети периметра.

Занятие 2. Установка ISA-сервера

До начала полной установки ISA-сервера следует установить сеть и настроить подключения согласно выбранной сетевой топологии. Если в проекте используется массив или политики предприятия, необходимо инициализировать предприятие, то есть внести в Active Directory информацию схемы массива. В процессе установки ISA-сервера вам предстоит создать *таблицу локальных адресов* (Local Address Table, LAT), содержащую диапазоны адресов внутренней сети.

Изучив материал этого занятия, вы сможете:

- ✓ подготовить компьютер к установке ISA-сервера;
- ✓ выполнить инициализацию предприятия и пояснить ее необходимость;
- ✓ создать таблицу LAT и описать ее функции;
- ✓ выполнить установку ISA-сервера;
- ✓ устранить неполадки, возникающие при установке ISA-сервера.

Продолжительность занятия — около 50 минут.

Подготовка к установке ISA-сервера

До установки ISA-сервера на компьютере необходимо установить все нужные устройства и настроить программное обеспечение.

Установка сетевого адаптера

Решите, какое подключение к интернету следует использовать: прямое (при помощи T1, T3, xDSL или кабельного модема) или по телефонной линии. Для прямого подключения необходимо установить и настроить адаптер внешней сети.

Свяжитесь со своим интернет-провайдером и узнайте у него корректные параметры протокола TCP/IP для адаптера внешней сети, а именно: маску подсети и IP-адреса для этого адаптера, основной шлюз и серверы DNS. В некоторых случаях интернет-провайдеры назначают адреса клиентов динамически, с использованием серверов DHCP (Dynamic Host Configuration Protocol).

Как правило, на ISA-сервере настраивается лишь один основной IP-шлюз. Укажите его IP-адрес в параметрах для адаптера внешней, а не внутренней сети. При этом поле основного шлюза адаптера внутренней сети оставьте пустым.

Подробнее о настройке параметров сетевых адаптеров — в справочной системе Windows 2000 Server.

Параметры TCP/IP

При настройке параметров TCP/IP любого сетевого адаптера необходимо указать постоянный IP-адрес и маску подсети ISA-сервера в локальной сети. Так как внутренние клиенты используют IP-адрес адаптера внутренней сети ISA-сервера в качестве основного шлюза, его назначение не должно выполняться средствами DHCP. Вместе с тем адреса внешних адаптеров могут быть как статическими (назначаемыми вручную), так и динамическими (назначаемыми DHCP-сервером), то же касается основного шлюза и адресов DNS-серверов.

Windows 2000 различает установленные адаптеры по их MAC-адресам (Media Access Control). Чтобы проверить корректность настройки и MAC-адреса сетевых адаптеров ISA-сервера, выполните в командной строке команду **ipconfig** /all.

После настройки адаптеров и назначения IP-адресов проверьте соединение с другими компьютерами в сети с помощью утилиты Ping. О правильности настройки адаптера внутренней сети ISA-сервера свидетельствуют отклики клиентов внутренней сети в ответ на ping-запрос, отправляемый с компьютера ISA-сервера, а о корректности настройки адаптера внешней сети свидетельствует отклик на ping-запрос вышестоящего шлюза в Интернете, DNS-сервера интернет-провайдера или произвольного адреса в Интернете. После тестирования сетевых соединений проверьте разрешение имен, для чего воспользуйтесь утилитой nslookup, позволяющей находить IP-адрес, соответствующий определенному Web-адресу, например nslookup **www.microsoft.com**.

Установка модема или ISDN-адаптера

Если ISA-сервер подключается к Интернету не напрямую через адаптер внешней сети, а по телефонной линии, на сервере следует установить модем или адаптер ISDN.

В Windows 2000 в некоторых ISDN-адаптерах оба ISDN-канала недоступны. Обычно работой второго канала управляют драйверы ISDN-карт, а не служба RRAS (Routing and Remote Access). Следует позаботиться о том, чтобы сетевой адаптер позволял использовать оба канала и интернет-провайдер поддерживал подключение к обоим.

Подробнее об установке адаптера ISDN или модема — в справочной системе Windows 2000 Server.

Таблица маршрутизации в Windows 2000

До начала установки ISA-сервера на компьютере следует определить таблицу маршрутизации, в которой необходимо указать все диапазоны IP-адресов внутренней сети. Для просмотра и управления записями в таблице маршрутизации воспользуйтесь утилитой route в Windows 2000. Для этих целей также используется консоль Routing and Remote Access (Маршрутизация и удаленный доступ) в Windows 2000, однако только при наличии работающей службы RRAS. В дальнейшем, *во* время установки ISA-сервера на основе таблицы маршрутизации Windows 2000 создается таблица локальных адресов (LAT). Ошибки, допущенные в процессе создания таблицы маршрутизации, можно впоследствии исправить вручную в LAT.

При наличии правильно составленной таблицы локальных адресов ISA-сервер способен безошибочно определить, какой сетевой адаптер следует использовать для доступа в ту или иную часть внутренней сети. В результате ошибок в таблице маршрутизации таблица локальных адресов ISA-сервера строится некорректно. В таком случае обращение клиента к внутреннему IP-адресу будет перенаправляться в Интернет или через брандмауэр.

При необходимости отредактируйте LAT вручную, указав все сети, в том числе доступные через внутренние маршрутизаторы. Это позволит клиентам ISA-сервера и брандмауэра корректно определять, когда использовать ISA-сервер, а когда подключаться к ресурсу напрямую.

Установка ISA-сервера

Запуск установки выполняется из окна установки ISA-сервера, которое открывается при загрузке дистрибутивного компакт-диска в дисковод. Окно установки ISA-сервера показано на рис. 2-9.

- Если ISA-сервер устанавливается как первый сервер в составе массива, перед установкой необходимо запустить утилиту инициализации предприятия ISA-сервера (ISA Server Enterprise Initialization).
- Если ISA-сервер устанавливается как изолированный сервер или это не первый ISA-сервер в сети, выберите установку ISA-сервера (Install ISA Server).

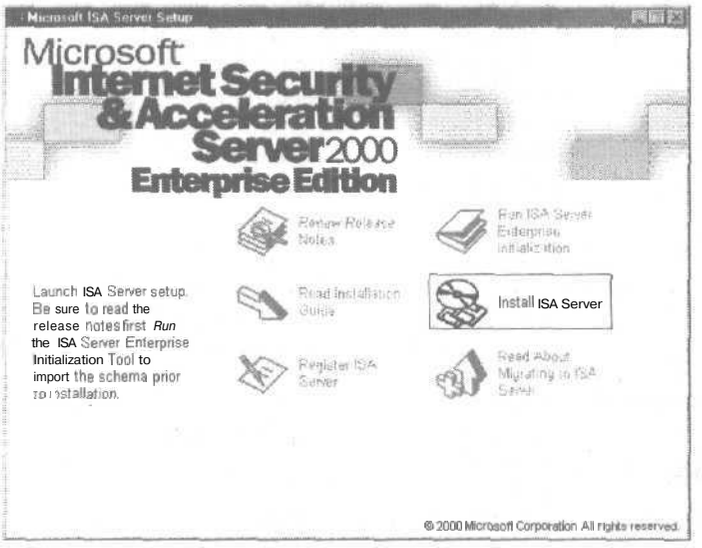


Рис. 2-9. Окно установки ISA-сервера

Инициализация предприятия

Версия ISA Server Enterprise Edition поддерживает создание массивов ISA-серверов. Установке ISA-сервера в массив предшествует внесение обновлений схемы ISA-сервера в схему Active Directory. Для этого используется утилита инициализации предприятия ISA-сервера, которая запускается из окна установки ISA-сервера, показанного на рис. 2-10.

После добавления обновлений схемы ISA-сервера при всех последующих установках ISA-сервера на компьютеры домена используется обновленная схема Active Directory.

Примечание Для установки обновления схемы ISA-сервера требуются права члена группы Enterprise Admins (Администраторы предприятия). Подробнее о правах пользователей и групп — в справочной системе Windows 2000 Server.

После инициализации предприятия схема Active Directory содержит объекты схемы ISA-сервера, что позволяет вам создать массив и установить ISA-сервер в качестве его члена.

Примечание Массив создается в процессе установки первого сервера— его члена. На репликацию информации, добавленной в Active Directory, потребуется определенное время, поэтому перед созданием следующего массива рекомендуется выждать определенное время.

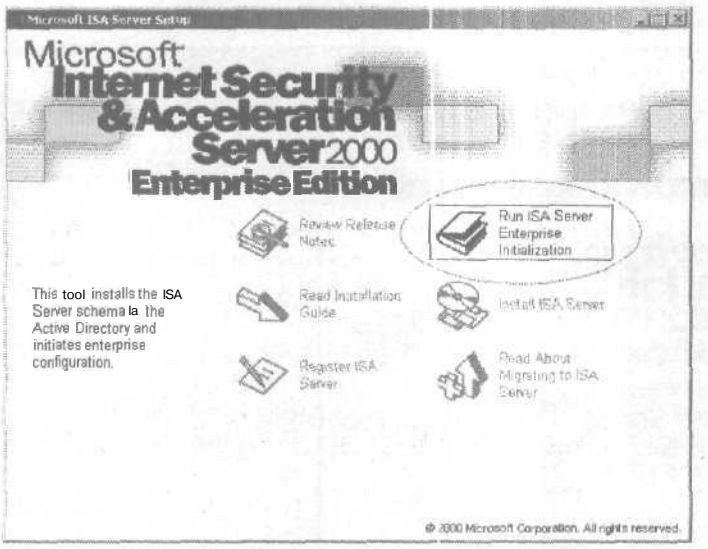


Рис. 2-10. Запуск инициализации предприятия

Процедура установки

Далее перечислены сведения, предоставляемые в процессе установки ISA-сервера.

Внимание! До начала установки ISA-сервера обязательно установите пакет обновлений Windows 2000 Service Pack I или более поздний.

1. **Ключ CD** — это идентификационный номер продукта 880-4486616.
2. **Варианты установки.** Существует три варианта установки: *стандартная установка* (Typical installation), *полная установка* (Full installation) и *выборочная установка* (Custom installation). В таблице 2-6 перечислены компоненты, устанавливаемые во время стандартной установки. При полной установке устанавливаются все компоненты, а выборочная установка позволяет администратору указать нужные компоненты.

Таблица 2-6. Компоненты ISA-сервера

Вариант	Компоненты	Предусмотрена ли в стандартной установке	Описание
ISA services (службы ISA-сервера)	Нет	Да	Управление доступом сетевых служб для межсетевого трафика
Add-in services (дополнительные службы)	H.323 Gatekeeper (служба привратника H.323)	Да	Поддержка доступа клиентов NetMeeting из Интернета и других безопасных сетей к клиентам во внутренней сети
	Message Screener (просмотр сообщений)	Нет	Просмотр входящего SMTP-трафика ISA-сервера

Таблица 2-6. *(окончание)*

Вариант	Компоненты	Предусмотрена ли в стандартной установке	Описание
Administration tools (средства администрирования)	**Administration Tools (средства администрирования)**	**Да**	**Централизованное управление компонентами ISA-сервера и другими дополнительными службами**
	H.323 Gatekeeper Administration Tools (средства администрирования H.323 Gatekeeper)	Нет	Расширение оснастки ISA Management для управления маршрутизацией вызовов NetMeeting внутри организации и между организацией и Интернетом

3. **Выбор массива.** При выполненной инициализации предприятия вы можете добавить устанавливаемый сервер в любой выбранный массив. В противном случае ISA-сервер устанавливается как изолированный сервер.
4. **Режим.** Выберите режим работы ISA-сервера: в качестве брандмауэра (Firewall), сервер кэширования (Cache) или смешанный (Integrated).
5. **Конфигурация кэша.** При установке ISA-сервера для работы в смешанном режиме или в режиме сервера кэширования следует указать диски, на которых вы собираетесь расположить кэш, а также его размер.

На рис. 2-11 показано диалоговое окно настройки параметров кэша.

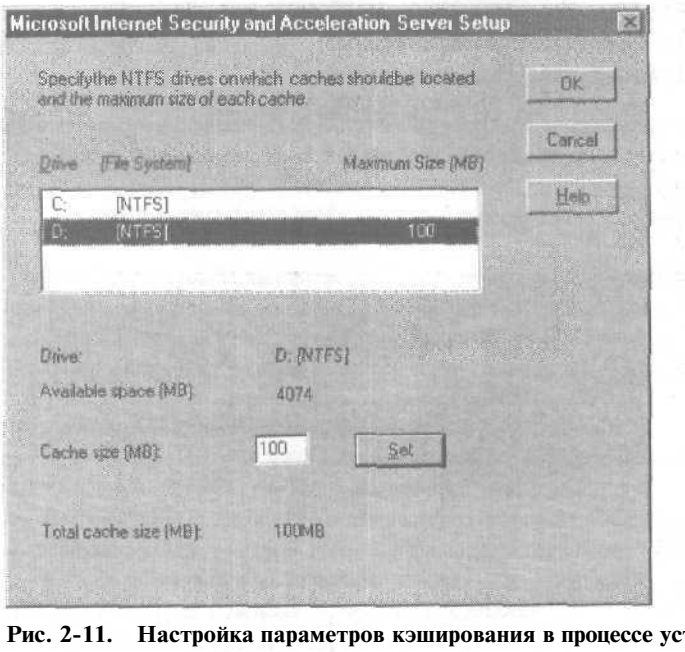


Рис. 2-11. Настройка параметров кэширования в процессе установки

6. Конфигурация таблицы локальных адресов. При установке ISA-сервера для работы в режиме брандмауэра или смешанном режиме необходимо указать диапазоны адресов в LAT.

Создание таблицы локальных адресов

Таблица локальных адресов, или LAT, создается во время установки ISA-севера для работы в режиме брандмауэра или смешанном режиме. В эту таблицу вносятся все диапазоны внутренних IP-адресов в локальной сети, отделенной ISA-сервером от Интернета. ISA-сервер использует LAT для управления подключениями компьютеров во внутренней сети с внешними сетями.

Как правило, LAT содержит все IP-адреса, обращение к которым выполняется через адаптеры внутренних сетей ISA-сервера, а также диапазоны частных IP-адресов, определенные IANA (Internet Assigned Numbers Authority). Диалоговое окно добавления записей в LAT во время установки показано на рис. 2-12.

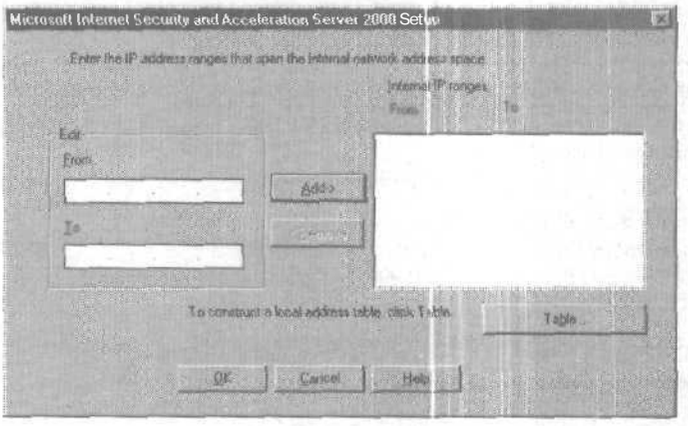


Рис. 2-12. LAT содержит диапазоны адресов внутренней сети

Для создания LAT мастер установки ISA-сервера использует данные из таблицы маршрутизации Windows 2000. Кроме того, вы вправе добавить в LAT диапазоны частных IP-адресов, определенные IANA в документе Request for Comments (RFC) 1918. Эти блоки адресов зарезервированы только для использования в частных интрасетях и никогда не используются в Интернете.

По умолчанию LAT составляют адреса, известные как *частные IP-адреса* (private IP-address). Они перечислены в локальной таблице маршрутизации. ISA-сервер считывает таблицу локальных адресов Windows 2000 Server особым образом, поэтому может оказаться, что LAT не содержит всех нужных адресов. В этом случае их надо добавить вручную. В LAT также иногда добавляют адреса не относящиеся к локальным.

Управление и поддержка LAT выполняется централизованно на компьютере ISA-сервера. Клиенты брандмауэра автоматически загружают и получают обновления LAT через заранее установленные промежутки времени. Запрашивая объект, клиент брандмауэра проверяет LAT. Если запрашиваемый IP-адрес содержится в ней, клиент брандмауэра запрашивает объект напрямую. В противном случае клиент обращается к ISA-серверу, чтобы тот запросил объект от своего имени.

Клиенты SecureNAT (Secure Network Address Translation — безопасное преобразование сетевых адресов) не хранят локальные копии LAT. По этой причине любые запросы объектов клиентами SecureNAT проходят через ISA-сервер. Если запрос обращен к внешнему IP-адресу, ISA-сервер переадресует его от лица клиента.

Таблица маршрутизации Windows 2000

В процессе создания таблицы локальных адресов ISA-сервер использует таблицу маршрутизации Windows 2000, определяя, какие диапазоны адресов внутренней сети следует считать внутренними. Если таблица маршрутизации составлена некорректно, ISA-сервер добавит в LAT ошибочные данные. В результате клиентские запросы к внутренним IP-адресам могут попадать в Интернет или «утекать» через брандмауэр. Для конфигурирования таблицы маршрутизации используется утилита маршрутизации Windows 2000. Созданная с ее помощью корректная таблица маршрутизации Windows 2000 позволит установщику ISA-сервера создать верную таблицу LAT.

Стандартные параметры ISA-сервера

На новом ISA-сервере многим параметрам присваиваются значения по умолчанию. Они перечислены в таблице 2-7.

Таблица 2-7. **Стандартные параметры ISA-сервера**

Компонент	Стандартные параметры
Таблица локальных адресов	Содержит записи, внесенные во время установки ISA-сервера
Параметры политики предприятия	При создании нового массива к нему применяются параметры по умолчанию политики предприятия
Фильтрация пакетов	Включена в режиме брандмауэра и смешанном режиме и отключена — в режиме сервера кэширования
Управление доступом	Если параметры политики предприятия не запрещают «разрешающие» правила массива, применяются правила узлов и содержания по умолчанию, которое предоставляют всем клиентам круглосуточный доступ к любому содержанию всех узлов. Однако так как не определено ни одно правило протокола, никакой трафик через ISA-сервер не возможен
Публикация	Запрещен любой доступ внешних клиентов к любым внутренним серверам. По умолчанию правило Web-публикации отвергает все подобные запросы
Маршрутизация	Все запросы клиентов Web-прокси пересылаются для выполнения в Интернет
Кэширование	Размер кэша равен указанному во время установки ISA-сервера. Кэширование HTTP и FTP включено. Активное кэширование отключено
Оповещения	Все оповещения активны, кроме оповещений об атаке со сканированием всех портов, отброшенных пакетах, нарушении протоколов и атаке типа «UDP-бомба»
Конфигурация	При установке или настройке клиентов брандмауэра или Web-прокси клиентов включается автоматическое обнаружение. Браузеры на клиентах брандмауэра конфигурируются при установке клиента брандмауэра

Устранение неполадок при установке ISA-сервера

Обычно при установке ISA-сервера проблем не возникает, однако, если это все же произойдет, прежде всего убедитесь в соответствии системы минимальным требованиям. Если причина не в оборудовании, изучите содержание журнала событий и выясните, нет ли

ошибок в сетевой конфигурации. Например, неправильная конфигурация DNS способна вызвать сбой инициализации предприятия, а некорректная LAT — ошибку при установке. Кроме того, при неполадках при инициализации предприятия проверьте, есть ли у вас полномочия члена группы Enterprise Admins (Администраторы предприятия), так как только этой группе предоставлено разрешение на запись в схему Active Directory.

Некоторые проблемы во время установки возникают из-за наличия на компьютере *общего доступа к подключению Интернета* (Internet Connection Sharing, ICS). До установки ISA-сервера отключите эту службу и перезагрузите компьютер.

Если указанными способами неполадку устранить не удается, проверьте целостность информации на дистрибутивном компакт-диске. За информацией об условиях обмена дефектных компакт-дисков обратитесь к представителю Microsoft.

Практикум. Установка ISA Server Enterprise Edition

Ваша задача — установить ISA-сервер на один компьютер. Чтобы обеспечить возможность расширения в будущем, сначала выполните инициализацию предприятия ISA-сервера, в процессе которой обновления схемы ISA-сервера добавляются в схему Active Directory. Это даст возможность установить массив ISA-серверов, настроить предприятие ISA-сервера и применить многоуровневую политику к брандмауэру или кэширующему серверу.

Выполните оба упражнения на компьютере Server1. (IP-адрес этого компьютера во внутренней сети должен быть 192.168.0.1)

Примечание Для установки ISA-сервера необходим пакет исправлений Windows 2000 Service Pack 1 или более поздний. Установи ге его до начала упражнения, если до сих пор вы это не сделали.

Задание 1. Инициализация предприятия

В этом упражнении вы должны инициализировать предприятие — внести обновления схемы ISA-сервера в схему Active Directory. По завершении инициализации можно устанавливать массивы ISA-серверов и применять политики на уровне предприятия. Обратите внимание, что служба каталогов Active Directory не допускает удаления объектов схемы и процесс инициализации предприятия является необратимым,

► **Инициализация предприятия**

1. Войдите в систему сервера Server1 под учетной записью Administrator (Администратор).
2. Вставьте дистрибутивный компакт-диск с Microsoft Internet Security and Acceleration Server 2000 Enterprise Edition в дисковод.

   Если окно установки ISA-сервера не открылось автоматически, найдите в корне компакт-диска файл ISAAutorun.exe и запустите его.
3. В окне установки ISA-сервера выберите **Run ISA Server Enterprise Initialization** (запустить инициализацию предприятия [SA-сервера).

   Откроется информационное окно **ISA Enterprise Initialization** с предупреждением о том, что в Active Directory будет установлена схема ISA-сервера и что это действие является необратимым.
4. Щелкните кнопку **Yes.**

   Откроется диалоговое окно **ISA Enterprise Initialization.**

5. В диалоговом окне инициализации предприятия выберите переключатель **Use Array Policy Only** (использовать только политику массива).
6. Установите флажок **Allow Publishing Rules** (разрешить правила публикации).

   Если вы хотите публиковать ресурсы внутренних серверов и предоставлять доступ к ним внешним пользователям (пользователям в Интернете), установите флажок **Allow Publishing Rules.** В противном случае на ISA-сервере не удастся установить правила Web-публикации и публикации серверов.
7. Сбросьте флажок **Force Packet Filtering On The Array** (принудительная фильтрация пакетов в массиве).

   В большинстве случаев флажок **Force Packet Filtering On The Array** оставляют: он позволяет на всех массивах предприятия постоянно поддерживать фильтрацию. В этом случае администраторы массивов не смогут ее отключить.
8. Щелкните кнопку OK.

   Откроется информационное окно **ISA Enterprise Initialization** с индикатором хода выполнения инициализации.

   По завершении инициализации откроется информационное окно **ISA Enterprise Initialization** с сообщением об успешном добавлении схемы ISA-сервера в схему Active Directory. Теперь можно устанавливать ISA-сервер в качестве члена массива.
9. Щелкните OK.

Задание 2. Установка ISA-сервера

В этом упражнении вы рассмотрите различные варианты установки ISA-сервера и затем выполните полную установку ISA-сервера на компьютере Server1.

▶ **Установка ISA-сервера**

1. Если компакт-диск с Microsoft Internet Security and Acceleration Server 2000 Enterprise Edition все еще находится в устройстве чтения, выберите в окне установки ISA-сервера **Install ISA Server.** Откроется окно **Microsoft Internet Security and Acceleration Server Enterprise Edition Setup.**
2. В информационном окне установки ISA-сервера щелкните **Continue**.
3. В ответ на приглашение ввести ключ CD ISA-сервера, введите идентификационный номер продукта **880-4486616** и щелкните OK. Откроется информационное окно с сообщением о назначенном идентификационном номере продукта.
4. Щелкните OK. Откроется информационное окно с текстом лицензионного соглашения.
5. Прочитайте лицензионное соглашение и щелкните **I Agree.**

   Откроется диалоговое окно установки ISA-сервера (Enterprise Edition) с тремя вариантами установки: **Typical Installation** (стандартная установка), **Full** Installation (полная установка) и **Custom Installation** (выборочная установка).
6. В диалоговом окне установки ISA-сервера выберите **Full Installation.**

   Откроется диалоговое окно **Microsoft Internet Security And Acceleration Server Setup** с вопросом, следует ли установить ISA-сервер как член массива.
7. Щелкните Yes, чтобы установить сервер как член массива. Откроется диалоговое окно **New Array** (новый массив).
8. В текстовом поле диалогового окна **New Array** выделите SERVER1 и введите имя нового массива MyArray.
9. Щелкните OK. Откроется диалоговое окно **Configure Enterprise Policy Settings** (настройка параметров политики предприятия).

10. Выберите переключатель **Use Custom Enterprise Policy Settings** (применить настраиваемую политику предприятия).
11. Выберите переключатель Use **Array Policy Only** (использовать только политику массива).
12. Убедитесь в том, что установлен флажок **Allow Publishing Rules** (разрешить правила публикации) и сброшен флажок **Force Packet Filtering On The Array** (принудительная фильтрация пакетов в массиве).
13. Щелкните **Continue.** Откроется диалоговое окно **Microsoft ISA Server Setup** (установка ISA-сервера) с предложением выбрать один из трех режимов: **Firewall** (брандмауэр), **Caching** (сервер кэширования) **и Integrated** (смешанный). По умолчанию переключатель установлен в положение **Integrated.**
14. Щелкните **Continue**. Откроется информационное окно, сообщающее об остановке службы публикации IIS. Служба публикации IIS останавливается из-за того, что по умолчанию она использует стандартный HTTP-порт 80. Этот же порт применяет ISA-сервер для Web-публикации. При наличии правил Web-публикации ISA-сервер ожидает запросы от внутренних и внешних клиентов на портах 80 и 8080.
15. Щелкните OK. Откроется диалоговое окно установки параметров кэша, с предложением выбрать диск для записи кэшируемых данных. По умолчанию мастер установки находит самый большой раздел NTFS и устанавливает кэш, равный 100 Мбайт, если на диске свободно не менее 150 Мбайт. Несмотря на то, что минимальный размер кэша равен 5 Мбайт, рекомендуется выделять не менее 100 Мбайт и предусмотреть дополнительно по 0,5 Мбайт для каждого клиента Web-прокси — полученное число округляется до большего целого значения.
16. Укажите, что единственный кэш размером 105 Мбайт располагается на диске C; для чего щелкните кнопку Set и в текстовом поле **Cache Size** (размер кэша) введите размер кэша.
17. Щелкните OK. Откроется диалоговое окно диапазонов IP-адресов с предложением ввести все IP-адреса адресного пространства внутренней сети. Эта информация используется для создания LAT.
18. Щелкните кнопку **Construct Table** (создать таблицу). Откроется диалоговое окно таблицы локальных адресов.
19. В диалоговом окне таблицы локальных адресов сбросьте флажок **Add the following private ranges** (добавить следующие диапазоны частных адресов).
20. Убедитесь, что установлен флажок **Add address ranges based on the Windows 2000 routing table** (добавить диапазоны адресов из таблицы маршрутизации Windows 2000).
21. Установите флажок **192.168.0.1** в нижней панели. Если в нижней панели появятся дополнительные флажки, сбросьте их все.
22. Щелкните OK. Откроется информационное окно **Setup** Message с подтверждением, что LAT успешно создана.
23. Щелкните **OK**, чтобы закрыть информационное окно, и щелкните еще раз OK, чтобы продолжить. После остановки служб ISA-сервер установщик перейдет к копированию нужных файлов на Server1. Этот процесс занимает несколько минут. По окончании установки откроется информационное окно **Launch ISA Management Tool** (запустить оснастку ISA Management).
24. Прочитайте текст, появляющийся в информационном окне. Мастер **Getting Started** (с чего начать) подскажет вам первые шаги по настройке ISA-сервера.
25. Щелкните OK. Откроется информационное окно установки ISA-сервера, информирующее об успешном завершении установки.

26. Щелкните **OK.** Откроется консоль управления ISA. Быстро «пробегите» через страницы мастера **Getting Stared,** щелкая кнопку **Next** и читая текстовые сообщения. Не меняйте никаких параметров.

Резюме

Перед установкой ISA-сервера необходимо настроить оборудование и подключить компьютер к сети. После настройки адаптеров и IP-адресов проверьте связь с другими компьютерами при помоши утилиты ping.

Если планируется устанавливать ISA-сервер в массив, следует добавить обновления схемы ISA-сервера в схему Active Directory. Для установки обновлений схемы ISA-сервера применяется утилита Enterprise Initialization (инициализация предприятия).

При установке ISA-сервера необходимо ввести ключ компакт-диска, а также выбрать вариант установки, указать, войдет ли сервер в состав массива, а также параметры кэша и таблицы локальных адресов. На основании данных таблицы локальных адресов ISA-сервер определяет, какие диапазоны адресов внутренней сети следует считать внутренними.

При устранении неполадок установки ISA-сервера сначала проверьте, соответствует ли оборудование требованиям и работоспособно ли оно, Если проблемы не в оборудовании, следует убедиться в корректности конфигурации сети. Если с сетью также все в порядке, следует проверить, достаточно ли у текущей учетной записи разрешений на инициализацию предприятия, а также не установлена ли на компьютере служба ICS.

Занятие 3, Переход от Proxy Server 2.0

ISA-сервер, обладая богатыми новыми возможностями, существенно отличается от Microsoft Proxy Server 2.0. При этом отличия касаются как конфигурации сервера, так и процедур обновления. На этом занятии мы перечислим основные факторы, которые должны учитывать администраторы при переходе к Microsoft ISA Server.

Изучив материал этого занятия, вы сможете:

- ✓ осуществить переход от Proxy Server 2.0 к одному ISA-серверу;
- ✓ осуществить переход от Proxy Server 2.0 к массиву ISA-серверов.

Продолжительность занятия — около 20 минут.

Переход от Microsoft Proxy Server 2.0

По сравнению с Proxy Server сервер ISA обеспечивает большую безопасность работы *с* Интернетом, лучше выполняет Web-кэширование, отличается гибкостью управления и отличной расширяемостью. Для упрощения перехода к этой, более совершенной, платформе следует выполнить простую процедуру переноса всех пользователей Microsoft Proxy Server 2.0 на новый сервер. Большинство правил, сетевых параметров, конфигураций мониторинга и кэша автоматически переносятся на ISA-сервер. Кроме того, в разнородной клиентской среде ISA-сервер наряду с собственным программным обеспечением для клиентов брандмауэра продолжает поддерживать клиентов Winsock Proxy.

Внимание! До установки ISA-сервера выполните полное архивирование текущих параметров Proxy Server 2.0. Для этого откройте Internet Services Manager (Диспетчер служб Интернета), щелкните правой кнопкой значок архивируемого сервера и в контекстном меню выберите команду **Backup/Restore Configuration** (Создать резервную копию конфигурации/ Восстановить конфигурацию с резервной копии).

Операционная система

ISA-сервер устанавливается на компьютеры под управлением операционных систем Windows 2000 Server, Windows 2000 Advanced Server *с* пакетом обновлений Service Pack 1 или более поздним или Microsoft Windows 2000 Datacenter Server.

Proxy Server на Windows 2000

Чтобы установить ISA-сервер на компьютере с Proxy Server 2.0 под управлением Windows 2000, просто запустите установку ISA-сервера, и программа установки распознает имеющуюся версию прокси-сервера. Соответствующее диалоговое окно показано на рис. 2-13. Щелкните **OK,** чтобы заменить старую версию.

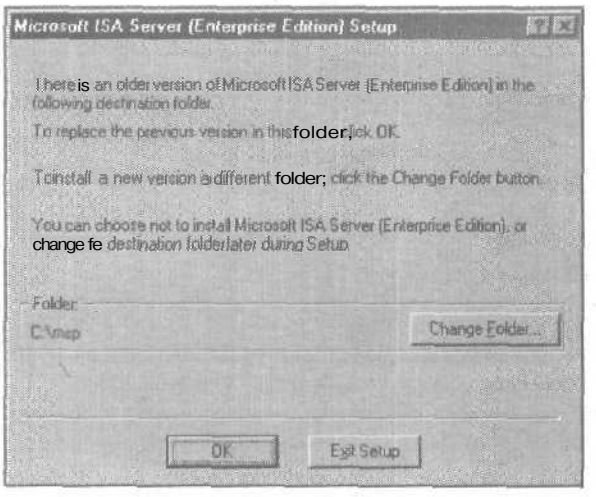


Рис. 2-13. Замена старой версии ISA-сервера

Далее мастер установки предложит перенести параметры и политику Proxy Server 2.0 на устанавливаемый ISA-сервер (рис. 2-14). Щелкните кнопку **Yes.**

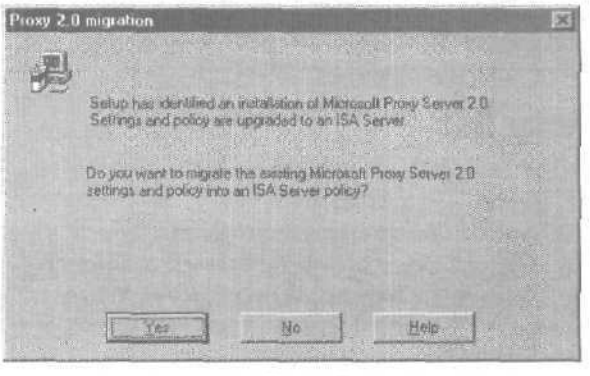


Рис. 2-14. Переход от Proxy Server 2.0

Proxy Server на Windows NT 4.0

Если текущая версия Microsoft Proxy Server 2.0 установлена на компьютере с Windows NT 4.0, выполните приведенные далее инструкции.

1. Остановите и отключите все службы Proxy Server, выполнив в командной строке несколько раз команду

   ```
   net stop <имя_службы>
   ```

   Службы, которые необходимо остановить, перечислены в таблице 2-8.

Таблица 2-8. Службы Proxy Server

Отображаемое имя	Имя службы
Microsoft Winsock Proxy Service (служба Winsock Proxy)	Wspsrv
Microsoft Proxy Server Administration (служба администрирования прокси-сервера)	Mspadmin
Proxy Alert Notification Service (служба оповещения прокси-сервера)	Mailalrt
World Wide *Web* Publishing Service (служба Web-публикации)	w3svc

2. Обновите операционную систему до Windows 2000 Server или более поздней версии. Проигнорируйте сообщения о том, что Proxy Server не работает с Windows 2000.
3. Запустите установку ISA-сервера. Так как основные службы, необходимые для работы брандмауэра, остановлены, рекомендуется на время установки отключить компьютер от Интернета.

Примечание Прямой переход от Proxy Server 1.0, BackOffice Server 4.0 или Small Business Server 4.0 не поддерживается. ISA-сервер не работает с протоколом IPX.

Внимание! Автоматический возврат к Proxy Server 2.0 после начала установки ISA-сервера невозможен.

Массивы серверов Proxy Server 2.0

При переходе от Microsoft Proxy Server 2.0 ISA-сервер устанавливается как член массива или изолированный сервер.

На изолированный ISA-сервер переносится большинство правил и других элементов конфигурации, созданных в Proxy Server. При переходе к массиву перенос правил Proxy Server определяется параметрами по умолчанию политики предприятия ISA-сервера.

Перед началом перехода от массива серверов Proxy Server удалите из его состава все компьютеры. Благодаря репликации все компьютеры массива содержат идентичные наборы правил, поэтому все серверы сохранят одинаковые конфигурации сети (например параметры набора номера по требованию) и мониторинга (например оповещения).

После удаления всех серверов из массива каждый Proxy Server обновите до ISA-сервера. Чтобы сохранить прежнюю конфигурацию массива, следует выполнить определенные условия.

1. При обновлении первого Proxy Server 2.0 во время установки ISA-сервера создайте новый массив.
2. При обновлении последующих серверов добавляйте их в созданный массив.

Переход к массиву

В случае перехода от одного сервера Рюху Server к массиву ISA-серверов способ переноса информации о конфигурации зависит от параметров по умолчанию предприятия массива ISA-серверов.

В отличие от Proxy Server, сервер ISA можно настроить для использования только политики предприятия, только политики массива или сочетания первого и второго. Перенос правил Proxy Server зависит от параметров политики предприятия. В таблице 2-9 опи-

сан порядок переноса политики **Proxy** Server для всех возможных вариантов конфигурации политики предприятия.

Таблица *2-9,* **Перенос параметров Proxy Server 2.0**

Варианты конфигурации политики предприятия	Разрешения администратора предприятия	Компоненты, переносимые на ISA-сервер
Использование только политики массива	Да/Нет	Все существующие правила Proxy Server переносятся в политику массива
Использование только политики предприятия	Да	Все существующие правила Proxy Server. Политика предприятия для нового массива настраивается на использование только политики массива
Использование только политики предприятия	Нет	Не переносится ни одно из правил Proxy Server. Новый массив использует исключительно политику предприятия
Использование политики предприятия и массива	Да	Все существующие правила Proxy Server. Политика предприятия для нового массива настраивается на использование только политики массива
Использование политики предприятия и массива	Нет	Только те правила Proxy Server, которые преобразуются в запрещающие (фильтры доменов, но не протоколы). Политика предприятия для нового массива настраивается на использование политики предприятия совместно с политикой массива (более строгой)

Если политика предприятия разрешает правила публикации, параметры публикации Proxy Server переносятся в политику массива.

Если политика предприятия не допускает правил публикации, то вы, имея разрешение администратора предприятия, можете изменить параметры политики предприятия и разрешить публикации, после чего параметры публикации прокси-сервера переносятся в политику массива.

Перенос конфигурации Proxy Server 2.0

При переходе от Proxy Server к ISA-серверу переносится большинство правил, сетевых параметров, конфигурации мониторинга и кэша. В этом разделе рассказано, каким образом осуществляется перенос информации о конфигурации.

Цепочки прокси-серверов

Поддерживаются смешанные цепочки (иерархии) серверов Proxy Server и ISA.

Запросы клиентов Web Proxy

В отличие от Proxy Server, который ожидает HTTP-запросы клиентов на порту 80, ISA-сервер во время установки настраивается на прослушивание запросов на порту 8080. По этой причине все нижестоящие члены цепочки (или браузеры) должны, обращаясь к ISA-

серверу, направлять запросы на порт 8080. Впрочем, ничто не запрещает настроить ISA-сервер на прослушивание на порту 80.

Публикация

Proxy Server требует, чтобы опубликованные серверы были клиентами Winsock Proxy. ISA-сервер позволяет публиковать внутренние серверы без установки на них дополнительного программного обеспечения или конфигурирования. Для ISA-сервера опубликованные серверы являются клиентами SecureNAT. Правила Web-публикации и правила публикации серверов устанавливаются на ISA-сервере, обеспечивая безопасность ресурсов внутренней сети и их доступность для определенных внешних клиентов. При этом изменения конфигурации опубликованного сервера не требуется.

Кэш

Конфигурация кэша Proxy Server переносится на ISA-сервер, в том числе данные о диске, на котором размещается кэш, размер и другие свойства.

Содержание кэша Proxy Server не переносится, так как на ISA-сервере реализован совершенно другой механизм хранения данных кэша. При установке ISA-сервера старый кэш удаляется, а новый механизм кэширования использует существующие параметры кэша и диска.

Примечание На удаление объемного кэша может потребоваться некоторое время.

SOCKS

ISA-сервер содержит фильтр SOCKS-приложений, позволяющий клиентским SOCKS-приложениям соединяться с сетью, используя для определения прав клиента на запрос подходящий набор элементов политики предприятия. Перенос SOCKS-правил Proxy Server в политику ISA-сервера не поддерживается.

Правила и политики

В таблице 2-10 показано, какие правила и другая конфигурационная информация Proxy Server переносится на ISA-сервер.

Таблица 2-10. Перенос конфигурационной информации на ISA-сервер

Proxy Server 2.0	ISA-сервер
Фильтры доменов	Правила узлов и содержания
Параметры разрешений Winsock	Правила протоколов
Параметры публикации	Правила Web- публикации
Статические фильтры пакетов	Разрешающие или блокирующие фильтры IP-пакетов
Правила маршрутизации Web Proxy	Правила маршрутизации

Для новых правил при необходимости создаются элементы политики. Кроме того, переносится дополнительная информация: таблица LAT, параметры автоматического набора номера, оповещения, параметры журнала и конфигурации клиентов.

Резюме

ISA-сервер расширяет функциональность Proxy Server 2.0, обеспечивая более надежную безопасность, а также более совершенные возможности кэширования, управления и расширяемости. Если в системе уже имеется Proxy Server 2.0, вы вправе осуществить переход к ISA-серверу, а не выполнять установку «с нуля». Переход позволяет перенести большую часть сушествуюшеи конфигурации на устанавливаемый ISA-сервер, в том числе правила Proxy Server, элементы политики, параметры сети, конфигурацию мониторинга и кэша. Однако содержание кэша не переносится.

Существует два варианта перехода от Proxy Server к ISA-серверу: к изолированному ISA-серверу или к новому массиву ISA-серверов. При переходе от массива компьютеров с Proxy Server к массиву ISA-серверов следует удалить из массива все компьютеры, в процессе установки первого ISA-сервера создать новый массив и далее при установке ISA-сервера на все остальные компьютеры присоединять их к созданному массиву. При переходе от одного Proxy Server к новому массиву ISA-серверов перенос информации о конфигурации определяется стандартными параметрами предприятия массива ISA-серверов. Создавая новые правила, новые элементы политик добавляют по мере необходимости.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Ответы для самопроверки — в приложении А «Вопросы и ответы» в конце книги.

1. Какую аппаратную конфигурацию (частоту процессора, объем оперативной и дисковой памяти) вы порекомендуете для компьютера, где предполагается установить ISA-сервер, который будет работать в смешанном режиме, обрабатывать 500–900 запросов в секунду и обслуживать менее 2000 пользователей?

2. Каковы требования к установке ISA-сервера в массив?

3. Каковы преимущества сети периметра?

4. Что следует предпринять для совмещения на одном компьютере ISA-сервера и Web-сервера?

5. Каково назначение таблицы LAT?

6. Что следует предпринять, чтобы после перехода от Proxy Server к ISA-серверу браузеры клиентов кэширующего сервера подключались к ISA-серверу?

ГЛАВА 3

Настройка безопасного доступа в Интернет

Занятие 1. Настройка доступа локальных клиентов в Интернет 66

Занятие 2. Настройка подключений ISA-сервера по телефонной линии 78

Занятие 3, Конфигурирование механизма автоматического обнаружения ISA-серверов 85

Занятие 4. Устранение неполадок, возникающих при подключении клиентов к ISA-серверу 92

Закрепление материала 97

В этой главе

После установки Microsoft Internet Security and Acceleration Server 2000 (ISA-сервера) в режиме брандмауэра доступ всех клиентских компьютеров в Интернет блокируется. В этой главе рассказано о последовательности действий при конфигурировании безопасного доступа клиентов в Интернет: изучении потребностей клиентов, определении необходимости установки клиента брандмауэра, настройке Web-браузера на использование ISA-сервера в качестве прокси-сервера и создании правил протоколов, обеспечивающих прохождение через брандмауэр всего интернет-трафика или только трафика определенного типа. При настройке доступа клиентов иногда требуется сконфигурировать автоматическое обнаружение ISA-сервера, которое позволяет клиентам автоматически подключаться к ISA-серверам сети, а также настраивать подключения по телефонной линии. Кроме того, из этой главы вы узнаете о средствах и методах устранения неполадок, возникающих при подключении клиентов к Интернету.

Прежде всего

Для изучения материалов этой главы необходимо:

- согласно требованиям, изложенными в главе «Об этой книге», присвоить компьютеру Server1 IP-адрес 192.168.0.1, а компьютеру Server2 — 192.168.0.2. Кроме того, Server1 следует подключить к Интернету по телефонной линии;
- выполнить практические задания главы 2, установив ISA-сервер на Server1 в смешанном (Integrated) режиме в качестве единственного члена массива MyArray.

Замятие 1. Настройка доступа локальных клиентов в Интернет

После установки ISA-сервера следует настроить доступ клиентских компьютеров в Интернет. ISA-сервер обрабатывает все запросы клиентов на основании правил политики доступа и по мере необходимости динамически открывает и закрывает требуемые порты.

При организации безопасного доступа локальных клиентов в Интернет нужно в первую очередь выбрать способ их конфигурирования — как клиентов SecureNAT (secure network address translation — безопасное преобразование сетевых адресов) или как клиентов брандмауэра. Затем при необходимости следует настроить Web-браузеры клиентских компьютеров на использование службы Web-прокси ISA-сервера. И, наконец, после настройки клиентов создать правила протоколов. Они регулируют (разрешают или блокируют) трафик определенных протоколов Интернета через брандмауэр.

Изучив материал этого занятия, вы сможете:

- ✓ рассказать о различиях и требованиях различных типов клиентов: SecureNAT, брандмауэра и Web-прокси;
- ✓ конфигурировать клиентские компьютеры для обеспечения безопасного доступа в Интернет через ISA-сервер;
- ✓ настраивать Microsoft Internet Explorer для использования службы Web-прокси ISA-сервера;
- ✓ устанавливать на клиентский компьютер клиент брандмауэра.

Продолжительность занятия -- около 60 минут.

Клиенты ISA-сервера

ISA-сервер поддерживает три типа клиентов:

- клиенты брандмауэра — клиентские компьютеры, на которых установлено и работает программное обеспечение клиента брандмауэра (Firewall Client);
- клиенты SecureNAT — клиентские компьютеры, на которых не установлен клиент брандмауэра;
- клиенты Web-прокси — клиентские Web-приложения, использующие ISA-сервер.

В таблице 3-1 сравниваются эти три типа клиентов.

Таблица 3-1. Сравнение типов клиентов ISA-сервера

Характеристика	Клиент SecureNAT	Клиент брандмауэра	Клиент Web-прокси
Необходимость установки	Нет, но требуются определенные изменения E конфигурации сети	Да	Нет, но требуется настройка Web-браузера
Поддерживаемые операционные системы	Любая операционная система, поддерживающая протокол TCP/IP	Только Windows-платформы	Все платформы, но поддержка обеспечивается посредством Web-приложений
Поддерживаемые протоколы	Требуются фильтры приложений для протоколов с множественными подключениями	Все WinSock-приложения	HTTP, Secure HTTP (S-HTTP), FTP и Gopher

Таблица 3-1. *(окончание)*

Характеристика	Клиент SecureNAT	Клиент брандмауэра	Клиент Web-прокси
Поддержка аутентификации на уровне пользователей	**Нет**	**Да**	**Да**
Серверные приложения	**Не требуется ни установка дополнительного ПО, ни настройка**	**Требуется файл конфигурации**	**Не применяются**

Компьютеры, клиенты брандмауэра или SecureNAT, способны выступать и в качестве клиентов Web-прокси. Это объясняется тем, что сеансы клиентов Web-прокси (иными словами, Web-запросы от браузера, использующего ISA-сервер в качестве прокси-сервера) обращаются напрямую к службе Web-прокси. Все остальные сетевые запросы, как от клиентов брандмауэра, так и от клиентов SecureNAT, отправляются напрямую службе брандмауэра ISA-сервера.

Изучение потребностей клиентов

Перед установкой или настройкой клиентского программного обеспечения следует ознакомиться с потребностями организации: определить, какие приложения и службы нужны внутренним клиентам, решить, как публиковать серверы. Только после этого станет ясно, какие типы клиентов, поддерживаемые ISA-сервером, наилучшим образом удовлетворяют эти потребности.

Для каждого клиентского компьютера необходимо определить, устанавливать ли на нем клиент брандмауэра или сконфигурировать клиент SecureNAT- В таблице 3-2 перечислены условия, которыми следует руководствоваться при выборе типа клиента.

Примечание Сам по себе доступ в Интернет не обеспечивает ISA-серверу выход в сеть — для этого требуется настроить правила IP-пакетов.

Таблица 3-2. Выбор типа клиента ISA-сервера

Требование к сети	Рекомендуемый тип клиента	Причина выбора
Нежелательно устанавливать программное обеспечение на стороне клиента или дополнительно настраивать клиентские компьютеры	SecureNAT	В отличие от клиентов брандмауэра, для клиентов SecureNAT не нужно устанавливать NAT не нужно устанавливать мное обеспечение или выполнять особую настройку
ISA-сервер используется только для прямого кэширования Web-объектов	SecureNAT	Не требуется устанавливать какое-либо программное обеспечение или дополнительно настраивать клиентские компьютеры. Запросы клиентов проходят через службу брандмауэра ISA-сервера и затем кэшируются службой Web-прокси

(см. след стр.)

Таблица 3-2. *(окончание)*

Требование к сети	Рекомендуемый тип клиента	Причина выбора
Требуется создать правила доступа на уровне пользователей для управления доступом в Интернет не по протоколам Web	Клиент брандмауэра	При использовании клиентов брандмауэра для сеансов связи через Интернет без Web правила политики доступа настраиваются на уровне пользователей. Возможность настройки для клиентов Web-прокси правил, определяемых на уровне пользователей, предусмотрена как для клиентов SecureNAT, так и для клиентов брандмауэра. Однако эти правила действуют только при условии, что ISA-сервер настроен на прием от Web-приложений информации для аутентификации в каждом сеансе
Публикация серверов внутренней сети	SecureNAT	Внутренние серверы иногда публикуются как клиенты SecureNAT. При этом не нужно создавать никаких файлов конфигурации — достаточно лишь создать правило публикации сервера на ISA-сервере
Сеть поддерживает мобильных пользователей и компьютеры	Клиент брандмауэра	Клиенты SecureNAT не поддерживают автоматическое обнаружение ISA-сервера. При использовании конфигурации с автоматическим обнаружением все клиенты Web-прокси и брандмауэра находят соответствующий ISA-сервер самостоятельно
Клиентам требуется доступ (помимо Web-браузера) по протоколам с дополнительными (вторичными) подключениями, например FTP	Клиент брандмауэра	Клиенты SecureNAT не поддерживают протоколы с дополнительными подключениями
Необходима поддержка подключения вызова по требованию для клиентских сеансов, отличных от Web-сеансов	Клиент брандмауэра	Хотя сеансы Web-прокси и поддерживают автоматическое подключение сервера к клиентам по телефонной линии, только клиенты брандмауэра поддерживают вызов по требованию для сеансов, отличных от Web

Настройка клиентов SecureNAT

При использовании клиентов SecureNAT устанавливать специальное программное обеспечение на клиентский компьютер не требуется. Тем не менее вам придется проанализировать топологию своей сети и убедиться, что ISA-сервер имеет возможность обслуживать запросы клиентов.

В частности, требуется корректно настроить основной шлюз клиента SecureNAT. При конфигурировании основного шлюза надо определить, какой из перечисленных ниже типов сетевой топологии применяется.

- **Простая сеть.** В этом случае между клиентом SecureNAT и ISA-сервером отсутствуют маршрутизаторы;
- **Сложная сеть.** Подразумевает наличие одного или более маршрутизаторов, связывающих подсети клиента SecureNAT и ISA-сервера.

Настройка клиентов SecureNAT в простой сети

Настройка клиентов SecureNAT в простой сети заключается в том, что в качестве основного шлюза IP-адреса определяется внутренний интерфейс ISA-сервера. Эта операция выполняется вручную путем модификации параметров протокола TCP/IP на клиентском компьютере [для чего используется компонент Network (Сеть) панели Control Panel (Панели управления)] или автоматически средствами службы DHCP.

Настройка клиентов SecureNAT в сложной сети

При настройке клиентов SecureNAT в сложной сети достаточно в качестве основного шлюза клиента назначить адрес последнего маршрутизатора в цепочке между ISA-сервером и клиентом SecureNAT. Другими словами, основной шлюз клиента — это адрес маршрутизатора в его подсети. Это стандартная конфигурация, и обычно ее менять не требуется, то есть не нужны никакие изменения параметров клиентов SecureNAT.

Оптимальным считается вариант, когда основной шлюз маршрутизатора направляет трафик на ISA-сервер по кратчайшему пути. Кроме того, не следует настраивать маршрутизатор на запрет пересылки пакетов, направленных за пределы корпоративной сети, так как решение о порядке маршрутизации пакетов принимает сам ISA-сервер.

Дополнительная настройка SecureNAT в сетях с доступом по телефонной линии

Как в простых, так и в сложных сетях, подключенных к Интернету по телефонной линии, требуется дополнительно настраивать клиенты SecureNAT. Для организации доступа в Интернет помимо Web-браузера клиентского компьютера, на котором не установлен клиент брандмауэра, требуется выполнить следующие операции. Во-первых, следует создать в консоли ISA Management элемент политики подключения по телефонной линии. Во-вторых, нужно настроить свойства узла Network Configuration в оснастке ISA Management на использование этого подключения для маршрутизации к вышестоящим серверам. Более подробно об этом рассказано в занятии 2 этой главы.

Разрешение имен для клиентов SecureNAT

Клиенты SecureNAT запрашивают объекты как из локальной сети, так и из Интернета, поэтому им нужен доступ к серверам DNS, которые разрешают имена внешних и внутренних компьютеров.

Только доступ в Интернет

Если клиентам SecureNAT требуется доступ только в Интернет и не нужно разрешать DNS-имена внутри локальной сети, параметры TCP/IP таких клиентов следует настраивать на использование внешних DNS-серверов, расположенных в Интернете. Дополнительно придется создать правило протокола, разрешающее клиентам выполнять DNS-запросы.

Доступ в Интернет и в локальную сеть

Если клиенты SecureNAT запрашивают данные как из Интернета, так и с серверов локальной сети, то им нужен DNS-сервер в локальной сети. Следует настроить этот сервер на разрешение и внутренних адресов, и адресов Интернета. Альтернативный вариант – настроить параметры **TCP/IP** клиента внешнего DNS-сервера в качестве основного, а внутреннего — в качестве дополнительного DNS-сервера.

Клиенты брандмауэра

Клиент брандмауэра — компьютер, на котором установлено и работает ПО клиента брандмауэра. На клиенте брандмауэра работают Winsock-приложения, использующие службу брандмауэра ISA-сервера. Когда Winsock-приложение на клиенте брандмауэра запрашивает объект с определенного компьютера, клиент проверяет свою копию таблицы LAT (Local Address Table), пытаясь найти в ней запись о запрашиваемом компьютере. Если такой записи в LAT нет, запрос пересылается службе брандмауэра ISA-сервера. Служба брандмауэра обрабатывает запрос и при наличии необходимых разрешений переправляет его адресату. Клиенты брандмауэра могут отправлять на ISA-сервер информацию для аутентификации пользователя Windows.

После установки клиента брандмауэра имеется возможность выбрать сервер, к которому подключается клиент, указав имя другого сервера на ISA-сервере, к которому он подключен в настоящий момент, или изменив имя в параметрах клиента брандмауэра. Изменения вступают в силу после обновления конфигурации брандмауэра. Для централизованного управления конфигурацией клиента брандмауэра используется узел **Client** Configuration консоли ISA Management, в котором содержатся средства управления как самими клиентами брандмауэра, так и параметрами Web-браузера клиентов брандмауэра.

В примере на рис. 3-1 ISA-сервер содержит общую папку mspclnt с программой установки клиента брандмауэра. Клиент брандмауэра устанавливается на компьютеры под управлением Microsoft Windows Me, Windows 95, Windows 98, Windows NT 4.0 и Windows 2000. Также обеспечивается поддержка 16-разрядных приложений Winsock, но только в среде Windows 2000 и Windows NT 4.0. После установки и запуска программного обеспечения клиента брандмауэра компьютер работает как клиент брандмауэра.

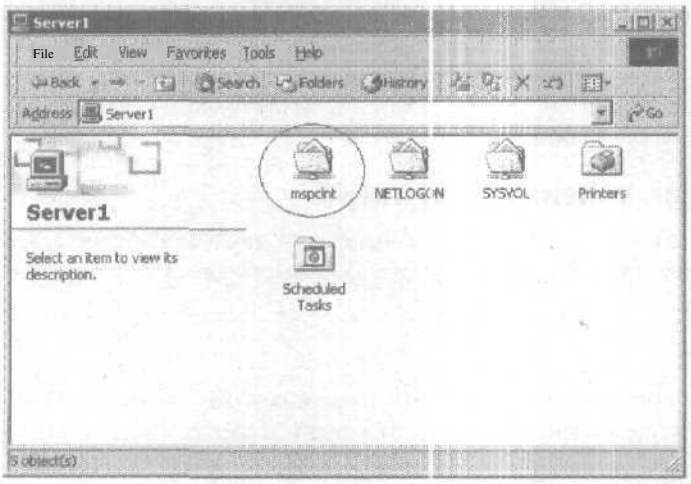


Рис. 3-1. Общая папка mspclnt содержит файлы для установки клиента брандмауэра

▶ **Установка клиента брандмауэра**

1. Выполните в командной строке на клиентском компьютере команду:

   `<путь>\Setup`

   где *<путь>* — путь к общедоступному каталогу с установочными файлами клиента брандмауэра ISA-сервера.

Примечание Установочные файлы клиента брандмауэра расположены в папке ISA-сервера с именем *<имя_ISA-сервера>*\MSPClnt.

2. Следуйте инструкциям программы установки.

Примечание Не устанавливайте клиент брандмауэра на ISA-сервер.

Параметры приложений клиента брандмауэра

Мастер установки клиента брандмауэра не выполняет автоматической настройки Winsock-приложений. Клиент брандмауэра работает с той же DLL-библиотекой Winsock, что и другие приложения — он перехватывает обращения приложений к этой DLL и определяет, нужна ли маршрутизация запроса на ISA Server.

При обработке Winsock-запросов клиент брандмауэра ищет файл Wspcfg.ini в каталоге клиентского Winsock-приложения. Обнаружив указанный файл, клиент брандмауэра ищет раздел [*<клиентское_приложение>*], где *<клиентское_приложение>* — имя Winsock-приложения без расширения .exe. Если такого раздела нет, клиент брандмауэра пытается найти раздел [Common Configuration]. Если ни одного из указанных разделов не обнаружено, клиент брандмауэра выполняет их поиск в файле Mspclnt.ini. Из первого найденного в указанной последовательности раздела, и только из него, извлекаются и используются параметры клиентского Winsock-приложения.

Дополнительная настройка клиента

Для большинства Winsock-приложений вполне достаточно конфигурации клиента брандмауэра по умолчанию. Однако в некоторых случаях требуется дополнительное конфигурирование клиента. Эта информация помещается в один из двух файлов.

- **Mspclnt.ini.** Это глобальный файл конфигурации клиента, который хранится в установочной папке клиента брандмауэра. Клиент периодически загружает с ISA-сервера файл Mspclnt.ini и записывает его поверх предыдущей версии. **Таким** образом, достаточно внести изменения в конфигурацию на ISA-сервере, чтобы они попали на клиентские компьютеры — это выполняется автоматически.

  Изменения в конфигурацию вносятся в узле **Client Configuration** консоли ISA Management. В области сведений нужно открыть свойства клиента брандмауэра, в диалоговом окне свойств клиента брандмауэра **Firewall Client Properties** — вкладку **Application Settings** (параметры приложения) и затем создать, изменить или удалить параметры приложения. Клиенты брандмауэра периодически загружают эти параметры.
- **Wspcfg.ini.** Этот файл расположен в папках клиентских приложений. ISA-сервер не перезаписывает этот файл, поэтому изменения в этом файле влияют лишь на конфигурацию данного клиента.

Пример файла Wspcfg.ini

Ниже приведен пример раздела [*WSP_Client_App*]файла конфигурации клиента для приложения WSP_Client_App.exe:

```
[<клиентское_приложение>]
Disable=0
NameResolution=R
LocalBindTcpPorts=7777
```

```
LocalBindUdpPorts=7000-7022, 7100-7170
RemoteBindTcpPorts=30
RemoteBindUdpPorts=3000-3050
ServerBindTcpPorts=100-300
ProxyBindIp=80:110.52.144.103, 82: 110.51.0.0
KillOldSession=1
Persistent=1
ForceProxy=i:172.23.23.23
ForceCredentials=1
NameResolutionForLocalHost=L
```

В таблице 3-3 перечислены параметры, которые обычно содержатся в файле конфигурации Winsock-приложения.

Таблица 3-3. Параметры клиента брандмауэра для Winsock-приложения в файле конфигурации

Запись	Описание
Disable	Допустимые значения: 0 или I. Значение 1 информирует об отключении службы брандмауэра для данного клиентского приложения
NameResolution	Возможные значения: L или R. По умолчанию имена в виде десятичных чисел, разделенных точками, или доменные имена Интернета перенаправляются для разрешения на ISA-сервер, а все остальные имена разрешаются на локальном компьютере. Если установлено значение R, все имена перенаправляются для разрешения на ISA-сервер, при значении L все имена разрешаются на лекальном компьютере
LocalBindTcpPorts	Порт TCP, список или диапазон портов для локальной привязки
LocalBindUdpPorts	Порт UDP, список или диапазон Портов для локальной привязки
RemoteBindTcpPorts	Порт TCP, список или диапазон портов для удаленной привязки
RemoteBindUdpPorts	Порт UDP, список или диапазон портов для удаленной привязки
ServerBindTcpPorts	Порт TCP, список или диапазон портов, которые поддерживают более одного подключения
ProxyBindIp	Указывает IP-адрес или список IP-адресов для привязки к определенному порту. Эта запись применяется, когда несколько серверов, использующих один и тот же порт, нужно привязать к одному и тому же порту, но по разным IP-адресам ISA-сервера. Синтаксис записи таков: `ProxyBind[p=[<порт>]:[<IP-адрес>], [<порт>]:[<IP-адрес>]` Номера портов указываются для обоих протоколов — TCP и UDP
KillOldSession	Возможные значения: 0 или 1. Если задано значение 1, то перед предоставлением приложению нового сеанса ISA-сервер завершает все возможно существующие ранее сеансы, относящиеся к «старому» экземпляру приложения. В частности, это значение полезно в ситуациях аварийного завершения приложения, которое не успевает закрыть прослушиваемый сокет. Тогда при закрытии прежнего сеанса ISA-сервер моментально обнаруживает, что приложение завершилось, и освобождает порт, занятый прежним сеансом

Таблица 3-3. *(окончание)*

Запись	Описание
Persistent	Возможные значения: 0 или 1. При установке значения I ISA-сервер может поддерживать состояние сервера, к которому выполняется запрос, даже если служба остановлена и перезапущена или если сервер не отвечает. В течение сеанса клиент периодически посылает на сервер специальное сообщение контроля связи. Если сервер не отвечает, клиент пытается восстановить состояние сокетов привязки и прослушивания до тех пор, пока сервер не перезапустится
ForceProxy	Используется для назначения определенного ISA-сервера конкретному Winsock-приложению. Синтаксис записи таков: `ForceProxy=[<тэг>]:[<запись>]` где *<тэг>* выбирается из двух значений: i означает IP-адрес, а n — имя. Поле *<запись>* содержит адрес или имя соответственно. Если указан тэг n, служба брандмауэра работает только поверх протокола IP
ForceCredentials	Используется, когда служба или серверное приложение Windows NT или Windows 2000 работает как клиентское приложение брандмауэра. Значение I инициирует применение альтернативных реквизитов пользователя, которые хранятся локально на компьютере, где работает служба. Запись реквизитов пользователя на клиентском компьютере выполняется средствами утилиты Credtool.exe, поставляемой в составе клиента брандмауэра. Реквизиты должны ссылаться на учетную запись пользователя, подлинность которой ISA-сервер способен проверить, то есть ее данные должны храниться либо локально на самом ISA-сервере, либо относиться к домену, с которым у ISA-сервера установлены доверительные отношения. Обычно устанавливается неограниченный срок действия учетной записи, в противном случае следует регулярно обновлять реквизиты пользователя
NameResolutionForLocalHost	Возможные значения: L (по умолчанию), P или E. Используется для указания метода разрешения имени локального (клиентского) компьютера при вызове функции API gethostbyname(). Имя компьютера LocalHost разрешается путем вызова функции Winsock API gethostbyname() со строкой LocalHost, пустой строкой или указателем NULL в качестве параметра. Winsock-приложения вызывают gethostbyname(LocalHost), чтобы определить свой локальный IP-адрес и передать его серверу Интернета. При значении параметра P функция gethostbyname() возвращает IP-адреса ISA-сервера, при значении L — IP-адреса локального компьютера. Если задано значение E gethostbyname() возвращает только внешние IP-адреса ISA-сервера, то есть IP-адреса, отсутствующие в LAT
ControlChannel	Возможные значения: Wsp.udp (по умолчанию) или Wsp.tcp. Определяет тип используемого канала управления

Служба Web-прокси

Служба Web-прокси (w3proxy) — служба Windows 2000, которая обрабатывает запросы любых Web-браузеров. Она позволяет обеспечить доступ к Web практически из любой операционной системы — Windows NT, Windows 95, Windows 98, Windows 2000, Macintosh и UNIX, Служба Web-прокси работает на прикладном уровне и выступает от имени клиентов, пересылая их запросы объектов Интернета по протоколам FTP, HTTP и Gopher. Служба Web-прокси также поддерживает протокол S-HTTP (Secure HTTP), обеспечивающий безопасные сеансы по SSL-каналам (Secure Sockets Layer).

Клиенты Web-прокси (как правило, браузеры) необходимо настроить для взаимодействия с ISA-сервером. Браузер анализирует URL-адреса узлов, запрашиваемых пользователем, и, обнаружив в адресе точки, полагает, что это полное доменное имя или IP-адрес удаленного узла, после чего пересылает HTTP-запрос на ISA-сервер для дальнейшей обработки.

Для наблюдения за состоянием службы Web-прокси, для ее запуска и останова используется консоль ISA Management, а точнее, элементы управления в папках **Monitoring и Service** (папка, вложенная в папку **Monitoring).**

При остановке службы Web-прокси информация из кэша не удаляется. При перезапуске службы на восстановление работоспособности кэша иногда требуется несколько секунд. При аварийном завершении работы Web-прокси ISA-сервер восстанавливает хранящуюся в кэше информацию. На это нужны дополнительные ресурсы, поэтому во время восстановления кэша производительность может несколько снизиться.

Настройка клиентов Web-прокси

Для настройки клиента Web-прокси не нужно устанавливать какое-либо программное обеспечение, однако иногда требуется перенастроить использующие прокси клиентские приложения на работу с ISA-сервером (рис, 3-2).

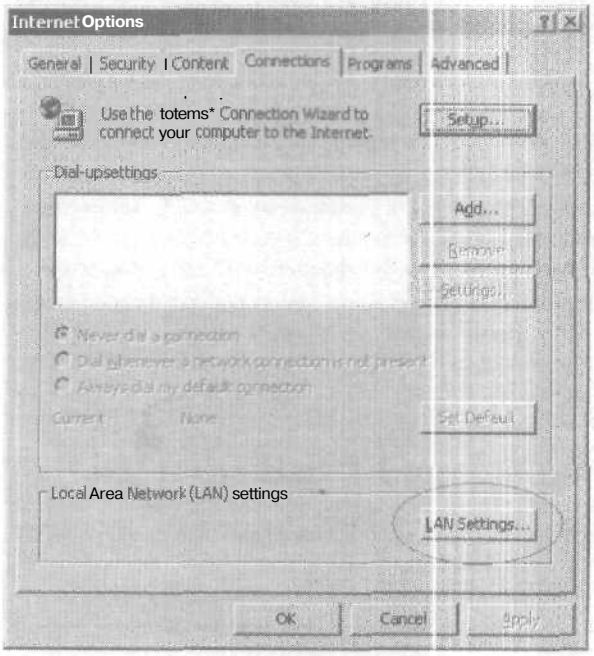


Рис. 3-2. Настройка параметров локальной сети Internet Explorer на использование ISA-сервера

Имеется возможность автоматически загружать с ISA-сервера сценарий конфигурирования клиента при каждом запуске браузера. Сценарий позволяет определить набор ISA-серверов и порядок обращения к ним в зависимости от URL-адреса запрошенного объекта.

Сценарий хранится по одному URL-адресу на каждом из ISA-серверов массива. Это облегчает настройку Web-браузеров, так как не нужно изменять конфигурацию каждого браузера. Возможность загрузки сценариев поддерживают браузеры Internet Explorer, начиная с версии 3.02, и Netscape версии 2.0 и более поздней.

По умолчанию сценарий настройки располагается по адресу:

`http://<имя_компьютера>/array.dll?Get.Routing.Script`

где *<имя_компьютера>* — имя ISA-сервера. ISA-сервер автоматически генерирует этот сценарий в соответствии с параметрами на вкладках **Direct Access и Backup Route** страницы свойств Web-браузеров в консоли ISA Management.

▶ **Ручная настройка Internet Explorer 5.0 на использование службы Web-прокси**

1. Запустите Internet Explorer.
2. В меню **Tools** (Сервис) выберите команду **Internet Options** (Свойства обозревателя).
3. На вкладке **Connections** (Подключение) щелкните кнопку LAN **Settings** (Настройка сети).
4. Установите флажок Use **a proxy server** (Использовать прокси-сервер).
5. В поле **Address** (Адрес) введите имя ISA-сервера или массива, а в поле **Port** (Порт) введите номер порта (обычно 8080).

Прямой доступ

Создание списка исключений Web-браузера позволяет обеспечить клиентам прямой доступ к компьютерам локальной сети. Вы также вправе указать, что все компьютеры, перечисленные в *таблице локального домена* (Local Domain Table, LDT), доступны для прямого обращения со стороны клиентов. В этом случае клиенты используют LDT для определения порядка разрешения имен — напрямую или через ISA-сервер.

Практикум 1. Организация безопасного доступа в Интернет клиентов Web-прокси

На этом занятии вы воспользуетесь возможностями безопасной маршрутизации ISA-сервера и настроите на компьютере Server2 безопасный доступ к Web через Server1. Поскольку, не имея явных указаний на пропуск пакетов, ISA-сервер запрещает прохождение трафика, необходимо создать правило протокола, разрешающее IP-трафик через брандмауэр ISA-сервера. Вы создадите такое правило. Обратите внимание, что правила протокола не делают ISA-сервер доступным для *входящего* трафика, что позволяет настроить *безопасный* доступ клиентов в Интернет без использования клиента брандмауэра.

Предполагается, что ISA-сервер уже подключен к Интернету по телефонной линии, а также настроено сетевое подключение Server1 и Server2 в соответствии с требованиями, перечисленными в разделе «Об этой книге».

Задание 1. Создание правила протокола

Сейчас вы создадите правило протокола, разрешающее безопасный доступ в Интернет.

▶ **Запуск мастера New Protocol Rule**

1. Войдите в систему сервера Server1 под учетной записью Administrator (Администратор).

2. Щелкните кнопку **Start** (Пуск), затем последовательно выберите пункты меню **Programs** (Программы), **Microsoft ISA Server и ISA Management.**
3. Откройте меню **View** и отметьте команду **Taskpad.**
4. В дереве консоли последовательно раскройте узлы Servers **and Arrays и MyArray.** При этом откроются узлы конфигурации компьютера Server1.
5. Раскройте узел **Access Policy** и выберите папку **Protocol Rules.**
6. В области сведений щелкните значок **Create a Protocol Rule.**

► **Создание правила протокола при помощи мастера** New **Protocol Rule**

1. В текстовом поле **Protocol Rule Name** введите **AllowIP** (разрешить IP-трафик).

Примечание Здесь решается упрощенная задача: разрешить всем внутренним клиентам доступ к любому IP-трафику. В реальности часто требуется ограничивать доступ определенных пользователей, групп пользователей или подмножеств клиентов к определенным протоколам.

2. Щелкните кнопку Next,
3. В окне **Rule Action** установите переключатель в положение **Allow** и щелкните **Next.**
4. На странице **Protocols** в поле со списком **Apply this** rule **to** выберите элемент **All IP traffic** и щелкните кнопку Next.
5. На странице **Schedule** (расписание) в поле со списком Use **This Schedule** выберите элемент **Always** и щелкните Next.
6. На странице **Client Type** установите переключатель в положение **Any Request** и щелкните кнопку Next.
7. На странице **Completing the New Protocol Rule Wizard** щелкните **Finish.** В области сведений появится только что созданное правило **AllowIP.**

Примечание Между созданием правила протокола и началом его действия иногда проходит определенное время, поэтому перед выполнением задания 2 подождите несколько минут или перезапустите ISA-сервер в соответствии с инструкциями в занятии 4 этой главы.

Задание 2. Настройка Internet Explorer на использование службы Web-прокси

В этом задании вы настроите Internet Explorer на взаимодействие со службой Web-прокси ISA-сервера. Для связи с интернет-провайдером используйте подключение по телефонной линии компьютера Server1.

1. Войдите в домен Domain01 с компьютера Server2 под учетной записью Administrator (Администратор).
2. Запустите Internet Explorer.
3. Если откроется окно мастера **Internet Connection Wizard** (Мастер подключения к Интернету), выполните при помощи этого мастера настройку подключения к Интернету по локальной сети.
4. В меню **Tools** (Сервис) выберите команду **Internet Options** (Свойства обозревателя).
5. На вкладке **Connections** (Подключение) щелкните кнопку LAN **Settings** (Настройка сети).
6. Сбросьте флажок **Use A Proxy Server** (Использовать прокси-сервер).
7. В поле **Address** (Адрес) введите 192.168.0.1, а в поле **Port** (Порт) — 8080.
8. Щелкните кнопку OK, чтобы закрыть диалоговое окно **Local Area Network** (LAN) **Settings** (Настройка локальной сети).
9. Щелкните OK, чтобы закрыть диалоговое окно **Internet Options** (Свойства обозревателя).

Теперь на компьютере Server2 должен стать доступным просмотр Web-узлов при помощи Internet Explorer.

Практикум 2. Установка клиента брандмауэра

Сейчас вы установите клиент брандмауэра. Если на компьютере его нет, служба брандмауэра применяет правила политики доступа только к IP-адресам внутренних клиентов. После установки клиента брандмауэра становится возможным применять правила политики доступа не только к IP-адресам, но и к отдельным пользователям и компьютерам. Клиенты брандмауэра повышают производительность за счет поддержки локальных копий LAT и LDT (Local Domain Table), встроенной поддержки протоколов с дополнительными подключениями, возможности дополнительной настройки параметров Winsock-приложений средствами глобального файла конфигурации клиента Mspclnt.ini и автоматического обнаружения **ISA-сервера.**

Задание. Установка клиента брандмауэра в локальной сети

Это задание выполняется на сервере Server2.

1. Откройте папку **My Network Places** (Мое сетевое окружение) и найдите в сети ресурс \\server1\mspclnt\.
2. Дважды шелкните значок **Setup** в папке \\server1\mspclnt\. Откроется окно мастера установки клиента брандмауэра.
3. Щелкните кнопку **Next.**
4. В окне **Destination Folder** (папка для установки) подтвердите предлагаемую по умолчанию папку для установки клиента и щелкните **Next.**
5. В окне **Ready to Install the Program** щелкните **Install.** Мастер выполнит установку клиента брандмауэра и откроет окно **Install Wizard Completed.**
6. Щелкните кнопку **Finish.**

Резюме

При организации безопасного доступа локальных клиентов в Интернет сначала на ISA-сервере настраивают правила протоколов, разрешающие пересылку трафика определенных протоколов через брандмауэр ISA-сервера на клиентские компьютеры. Затем следует определить вариант конфигурирования внутренних клиентов. При настройке их в качестве клиентов SecureNAT никакое ПО дополнительно устанавливать не надо, а при настройке в качестве клиентов брандмауэра нужно установить на компьютерах клиент брандмауэра.

Перед установкой или настройкой программного обеспечения на клиентских компьютерах оцените потребности организации. Клиент брандмауэра устанавливается, если требуется обеспечить поддержку мобильных пользователей, протоколов с дополнительными подключениями, применения политики доступа к аутентифицированным пользователям и вызовов по требованию в сеансах, не использующих Web. Клиенты SecureNAT применяются, когда ISA-сервер применяется для безопасной публикации Web-серверов, а также в случае установки ISA-сервера в режиме кэширования или если нежелательно устанавливать дополнительные ПО на клиентских компьютерах.

И клиенты брандмауэра, и клиенты SecureNAT работают в качестве клиентов Web-прокси. Служба Web-прокси (w3proxy) — это служба Windows 2000, обрабатывающая запросы приложений, совместимых с прокси. Для настройки клиентов Web-прокси не требуется дополнительное программное обеспечение, единственное, что нужно, — настроить Web-браузеры клиентских компьютеров на использование ISA-сервера в качестве прокси-сервера.

Занятие 7. Настройка подключений ISA-сервера по телефонной линии

ISA-сервер позволяет воспользоваться преимуществами брандмауэра и сервера кэширования даже при отсутствии подключения к Интернету по выделенной линии; ISA-сервер часто применяют для защиты и совместного использования всеми компьютерами локальной сети единственного подключении по телефонной линии.

Изучив материал этого занятия, вы сможете:

- ✓ создать на ISA-сервере подключения по телефонной линии;
- ✓ обеспечить полноценные безопасные подключения клиентов ISA-сервера к Интернету через подключение ISA-сервера по телефонной линии;
- ✓ настроить на ISA-сервере вызов по требованию.

Продолжительность занятия — около 30 минут.

Настройка подключений по телефонной линии

Для настройки записей подключений по телефонной линии нужно создать в консоли ISA Management элементы политики подключений по телефонной линии. Впрочем, для совместного использования подключения ISA-сервера клиентами брандмауэра и Web-прокси эта процедура необязательна. Тем не менее, если предполагается совместное использование подключения по телефонной линии службами, не относящимися к Web, например POP3 или NNTP, на компьютерах, не являющихся клиентами брандмауэра, необходимо настроить подключения по телефонной линии и маршрутизацию запросов, выполняемых по этим подключениям. Таким образом, подключения по телефонной линии обеспечивают доступ в Интернет клиентам SecureNAT, не являющимся клиентами Web-прокси.

Кроме обеспечения доступа в Интернет, создание подключений по телефонной линии позволяет определять для клиентов SecureNAT правила и политики на уровне отдельных подключений, а также указывать порядок связи ISA-сервера по ним.

И, наконец, только подключения по телефонной линии обеспечивают вызов по требованию клиентов Web-прокси и брандмауэра.

Каждая запись подключения по телефонной линии содержит следующую информацию:

- имя записи, настроенной на сервере удаленного доступа на всех серверах массива;
- имя пользователя и пароль для подключения к интернет-провайдеру.

Подключения по телефонной линии создаются лишь на основе подключений, ранее настроенных на всех ISA-серверах масс ива. Подробнее о создании сетевых подключений — в справочной системе Windows 2000.

Вы вправе создать несколько записей подключения по телефонной линии, но активной может быть только одна из записей массива. Она используется при автоматическом подключении ISA-сервера к Интернету при обслуживании запроса клиента.

► **Создание записи подключения по телефонной линии**

1. Откройте консоль ISA Management.
2. В дереве консоли последовательно раскройте узлы **Servers And Arrays,** MyArray **и Policy Elements.**
3. Щелкните правой кнопкой элемент **Dial-up Entries** и в контекстном меню последовательно выберите New и **Dial-Up Entry.** Откроется диалоговое окно New **Dial-up Entry.**

4. В текстовом поле **Name** введите имя записи подключения по телефонной линии.
5. (Не обязательно.) В поле **Description** введите описание подключения по телефонной линии.
6. В поле Use **the following network dial-up connection** (использовать следующее сетевое подключение по телефонной линии) введите или выберите имя существующего сетевого подключения Windows 2000 по телефонной линии, затем щелкните кнопку **Set Account** (настроить учетную запись).
7. В окне Set Account в поле **User** введите имя пользователя учетной записи для подключения к интернет-провайдеру.
8. В текстовых полях **Password и Confirm password** введите пароль учетной записи.
9. Щелкните **OK.** Произойдет возврат в диалоговое окно New **Dial-up Entry.**
10. Снова щелкните OK.

Перед конфигурированием записей подключений по телефонной линии следует учесть следующее:

- указываемое в записи сетевое подключение по телефонной линии необходимо заранее настроить на каждом из входящих в массив серверов;
- создаваемое подключение по телефонной линии становится активным и будет использоваться правилами маршрутизации при построении цепочек брандмауэров;
- указываемые имя и пароль должны совпадать с именем и паролем, которые вводятся при настроенном вручную подключении.

При наличии нескольких записей подключения по телефонной линии активная запись выбирается следующим образом.

1. Откройте оснастку ISA Management.
2. В меню **View** отметьте команду **Advanced.**
3. В дереве консоли раскройте узел **Policy Elements.**
4. Щелкните элемент **Dial-up Entries** (записи подключений по телефонной линии).
5. В области сведений щелкните правой кнопкой запись, которую нужно сделать активной, и выберите в контекстном меню **Set as Active Entry** (сделать активной записью).

Необходимо учесть следующие особенности активной записи:

- активную запись невозможно удалить;
- при выборе активной записи отключаются все существующие подключения по телефонной линии, используемые ISA-сервером для подключения.

Вызов по требованию

ISA-сервер можно настроить для автоматического подключения к Интернету по телефонной линии при выполнении простой маршрутизации и активного кэширования.

- Маршрутизация — если клиент запрашивает объект и маршрут к объекту требует установки подключения по телефонной линии, а политика доступа разрешает выполнение запроса, ISA-сервер подключается автоматически, используя активную запись.
- **Активное кэширование** — при включенном активном кэшировании ISA-сервер сам дозванивается в Интернет и получает часто используемую клиентами информацию.

Кроме того, ISA-сервер подключается к Интернету в тех случаях, когда не в состоянии точно определить, разрешает ли политика доступа выполнение клиентского запроса. Такая ситуация возникает, когда, к примеру в правилах политики доступа указано доменное имя, а клиент обратился по IP-адресу. Если правило маршрутизации требует для выполнения запроса подключиться к Интернету, ISA-сервер устанавливает связь по телефонной линии и разрешает имя запрашиваемого компьютера, после чего проверяет, разрешено ли выполнение запроса правилами политики доступа.

Примечание На вызов по требованию настраиваются только клиенты Web-прокси и брандмауэра. Для подключения к Интернету клиентов SecureNAT необходима предварительная установка подключения по телефонной линии.

Конфигурирование вызова по требованию

ISA-сервер можно настроить на автоматическое подключение к Интернету по требованию, например при запросе объекта, отсутствующего в кэше.

▶ **Настройка вызова по требованию**

1. Создайте сетевое подключение по телефонной линии. Подробнее о создании сетевых подключений — в справочной системе Windows 2000.
2. Создайте в консоли ISA Management запись подключения по телефонной линии.
3. Разрешите вызов по требованию для службы брандмауэра (о том, как это сделать, рассказано чуть позже). Эта операция необходима только для клиентов брандмауэра и не требуется для клиентов Web-прокси.
4. Включите автоматическое подключение для маршрутизации (об этом — ниже).
5. Убедитесь, что основной шлюз не настроен ни на одном внутреннем интерфейсе ISA-серверов массива.

▶ **Включение вызова по требованию для службы брандмауэра**

1. В дереве консоли ISA Management щелкните правой кнопкой мыши узел **Network Configuration** и выберите пункт меню **Properties.** Откроется окно **Network Configuration Properties** (рис. 3-3).

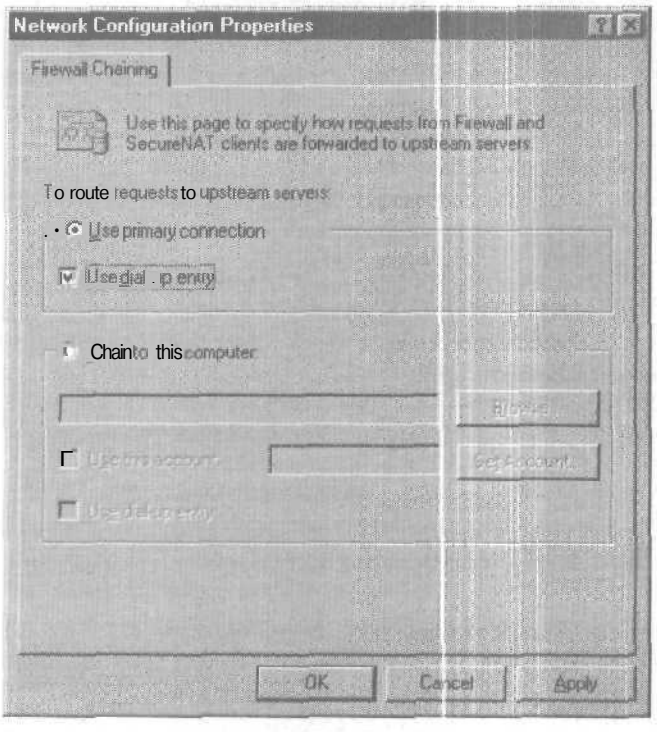


Рис. 3-3. **Окно свойств сети Network Configuration Properties**

2. На вкладке **Firewall Chaining** установите переключатель в положение Use **Primary Connection** (использовать основное подключение).
3. Установите флажок Use **dial-up entry** (использовать подключение по телефонной линии).

После настройки службы брандмауэра на использование записи подключения по телефонной линии при разрешении внешних запросов следует перейти к настройке службы брандмауэра на автоматическое подключение к Интернету по этой записи.

► **Включение вызова по требованию для маршрутизации**

1. В дереве консоли **ISA Management** в папке **Network Configuration** выделите элемент **Routing.**
2. В области сведений шелкните правой кнопкой мыши правило, которое требуется настроить, и выберите в контекстном меню команду **Properties.** Откроется окно свойств правила (рис. 3-4).
3. На вкладке **Action** установите переключатель **Retrieving them directly from the specified destination** (получать объекты прямо из указанного места назначения).
4. На этой же вкладке установите флажок **Use dial-up entry for primary route** (использовать в качестве основного маршрута подключение по телефонной линии).

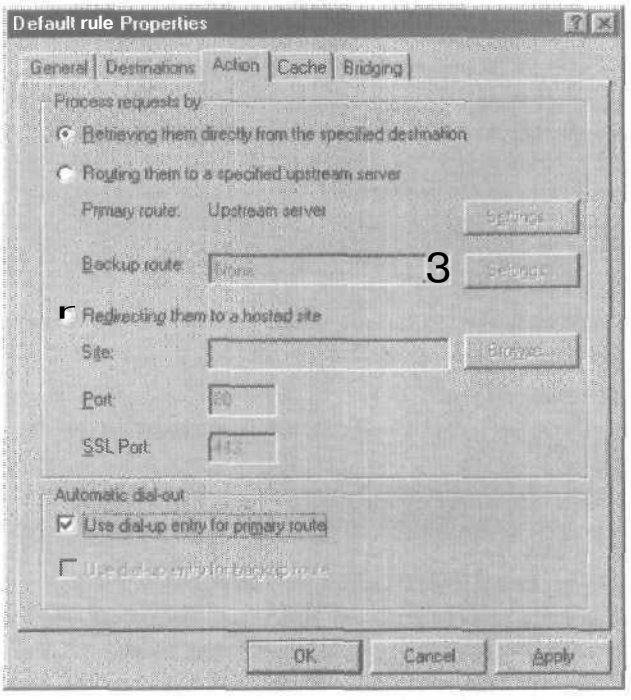


Рис. 3-4. Настройка правила маршрутизации для автоматического подключения

Ограничение подключений ISA-сервера ко внешним узлам

Существует возможность ограничивать подключения ISA-сервера к Интернету и выполнять их, только когда это действительно необходимо. Для этого в таблицу LDT средствами оснастки ISA Management вносятся имена всех внутренних компьютеров. Клиенты по таблице LDT определяют, как выполнять разрешение имени — напрямую или через ISA-сервер. Наличие LDT предотвращает подключение ISA-сервера к внешним DNS-серверам только для того, чтобы установить, что запрашиваемый компьютер является внутрен-

ним. Клиенты брандмауэра поддерживают регулярно обновляемую локальную копию LDT. Следует иметь в виду, что LDT проверяется только при запросах клиентов брандмауэра.

Закрытие подключений

После подключения ISA-сервера в Интернет связь поддерживается, пока не происходит одно из следующих событий:

- активизируется другое подключение;
- активным назначается другое сетевое подключение по телефонной линии;
- отключается запись, используемая для построения цепочки брандмауэров;
- становится доступным основной маршрут (в случае, когда текущее подключение осуществляется по резервному маршруту);
- останавливается служба брандмауэра.

Практикум. Настройка записи подключения по телефонной линии

На этом занятии вы настроите доступ клиента SecureNAT в Интернет через подключение ISA-сервера по телефонной линии.

Предполагается, что компьютер Server1 подключен к Интернету по телефонной линии. Кроме того, считается, что в соответствии с инструкциями занятия 1 этой главы создано правило протокола, разрешающее все виды IP-трафика, а на Server2 установлен и запущен клиент брандмауэра. И, наконец, в свойствах протокола **TCP/IP** на компьютере Server2 в качестве основного DNS-сервера задается внешний DNS-сервер интернет-провайдера, а в качестве дополнительного DNS-сервера — адрес 192.168.0.1.

Задание 1. Проверка подключении к Интернету

Сейчас вы изучите состояние сеанса клиента брандмауэра, после чего отключите клиент брандмауэра и проанализируете изменения в поведении сеанса.

▶ **Отключение клиента брандмауэра**

1. Войдите в домен DomainOl на Server1 и Server2 под учетной записью Administrator (Администратор).
2. На компьютере Server2 щелкните **Start** (Пуск) и выберите команду **Run** (Выполнить).
3. В открывшемся диалоговом окне **Run** (Выполнить) введите **cmd** и щелкните кнопку **OK.** Откроется окно командной строки.
4. Введите в командной строке **nslookup www.microsoft.com** и нажмите клавишу Enter.

   В окне командной строки отобразится информация об **IP-адресе,** соответствующем имени www.microsoft.com, согласно данным основного DNS-сервера.
5. На Server1 откройте консоль ISA Management и последовательно раскройте узлы **MyArray и Monitoring.**
6. Щелкните папку **Sessions.**
7. В меню **View** отметьте команду **Advanced.**
8. Щелкните правой кнопкой мыши область сведений и в контекстном меню выберите **Refresh.**
9. Найдите в области сведений текущий сеанс работы в Интернете системы Server2.

   Обратите внимание, что в окне указаны тип сеанса — **Firewall Session,** имя пользователя — **Administrator** и клиентский компьютер — **Server2.** При наличии активного клиента брандмауэра информация об учетной записи пользователя и имени компьютера предоставляется вместе со сведениями сеанса.

10. На компьютере Server2 отключите клиент брандмауэра: дважды щелкните значок **Firewall Client в Control Panel** (Панели управления), сбросьте флажок **Enable Firewall Client** и щелкните кнопку **OK.**
11. Снова откройте окно командной строки.
12. В командной строке снова введите **nslookup www.microsoft.com** и нажмите Enter.

    Вы получите сообщение о тайм-ауте DNS-запроса, так как компьютер Server2 стал клиентом SecureNAT, а клиенты SecureNAT еще не настроены на доступ в Интернет через подключение ISA-сервера по телефонной линии.

Задание 2. Создание подключения по телефонной линии

Это задание выполняется на Server1. Чтобы обеспечить клиентам SecureNAT доступ в Интернет через подключение ISA-сервера по телефонной линии, вы создадите элемент политики подключения по телефонной линии.

► **Создание элемента политики подключения по телефонной линии**

1. Откройте консоль ISA Management.
2. Перейдите в папку **Policy Elements.**
3. Щелкните правой кнопкой мыши узел **Dial-up Entries** и в контекстном меню последовательно выберите команды New и **Dial-up Entry.**

   Откроется диалоговое окно New **Dial-up Entry** (новое подключение по телефонной линии).
4. В поле **Name** введите имя подключения MyDialUp.
5. Щелкните кнопку **Select.** Откроется диалоговое окно выбора сетевого подключения по телефонной линии **Select Network Dial-up Connection.**
6. В поле **Network Dial-up Connection** выберите подключение по телефонной линии и щелкните OK.
7. В диалоговом окне New **Dial-up Entry** щелкните **Set Account.** Откроется диалоговое окно Set **Account.**
8. В соответствующих текстовых полях введите имя и пароль для подключения к интернет-провайдеру.
9. Щелкните кнопку OK.
10. В окне New **Dial-up Entry** также щелкните OK.

Теперь при выборе папки **Dial-up Entries** подключение по телефонной линии **MyDialUp** отображается в области сведений консоли ISA Management.

Задание 3. Настройка ISA-сервера на маршрутизацию через подключение по телефонной линии

Сейчас вы настроите клиенты SecureNAT на маршрутизацию запросов в Интернет через активное подключение по телефонной линии. Задание выполняется на компьютере Server1.

► **Настройка маршрутизации клиентов SecureNAT**

1. В дереве консоли ISA Management щелкните правой кнопкой мыши узел **Network Configuration** и в контекстном меню выберите команду **Properties.** Откроется диалоговое окно свойств сети **Network Configuration Properties.**
2. Убедитесь, что на вкладке **Firewall Chaining** выбран переключатель **Use Primary Connection** (использовать основное соединение).
3. Установите флажок **Use Dial-up Entry** (использовать запись подключения по телефонной линии) и щелкните кнопку **OK.**

В следующем задании вы перезапустите службу брандмауэра, чтобы привести в действие новую конфигурацию маршрутизации.

Задание 4. Перезапуск службы брандмауэра

Чтобы привести в действие новую конфигурацию маршрутизации, необходимо перезапустить службы брандмауэра и/или Web-прокси. Задание выполняется на компьютере Server1.

► **Перезапуск службы брандмауэра и/или Web-прокси**

1. В дереве консоли ISA Management раскройте узел **Monitoring.**
2. Щелкните узел **Services.**
3. В области сведений щелкните правой кнопкой мыши **Firewall Service** (службу брандмауэра) и в контекстном меню выберите **Stop.**
4. (Не обязательно.) В области сведений щелкните правой кнопкой мыши элемент **Web proxy** (Web-прокси) и в контекстном меню выберите **Stop.**
5. После полного останова службы брандмауэра (и/или Web-прокси), снова шелкните правой кнопкой **Firewall Service** и в контекстном меню выберите **Start.**

Перед выполнением следующего задания дождитесь, чтобы значок службы брандмауэра (и/или Web-прокси) стал зеленым

Задание 5. Просмотр информации об интернет-сеансе клиента SecureNAT

Сейчас вы выполните подключение клиента SecureNAT к Интернету, а затем на ISA-сервере просмотрите информацию о сеансе.

► **Подключение к Интернету клиента SecureNAT**

1. На компьютере Server2 откройте окно командной строки.
2. В командной строке введите **nslookup www.microsoft.com** и нажмите клавишу Enter.

   В окне отобразится сообщение об успешном выполнении команды несмотря на то, что Server2 стал клиентом SecureNAT.
3. В системе Serverl откройте консоль ISA Management,
4. В дереве консоли в папке **Monitoring** откройте папку **Sessions.**
5. Щелкните правой кнопкой область сведений и в контекстном меню выберите **Refresh.**
6. Найдите в области сведений текущий сеанс работы в Интернете системы Server2.

   Обратите внимание, что теперь указаны тип сеанса — **Firewall Session** и пустое имя пользователя, клиентский компьютер описан лишь IP-адресом — 192.168.0.2. В сведениях сеанса клиентов SecureNAT HI; предоставляется информации об учетной записи пользователя и имени компьютера.
7. На компьютере Server2 снова активируйте клиент брандмауэра.

Резюме

Для обеспечения безопасного доступа клиентов ISA-сервера в Интернет по телефонной линии необходимо создать элемент политики подключения по телефонной линии и настроить сеть на маршрутизацию запросов на вышестоящие серверы по этому подключению. Настройка записи подключения по телефонной линии на ISA-сервере позволяет клиентам SecureNAT получать доступ в Интернет по протоколам, не относящимся к Web, а также применять к политикам ISA-сервера правила на уровне отдельных подключений.

Создание подключений по телефонной линии также позволяет выполнять вызовы по требованию, то есть ISA-сервер способен самостоятельно подключаться к Интернету по телефонной линии, получив от клиента Web-прокси или брандмауэра запрос удаленного узла.

Занятие 3, Конфигурирование механизма автоматического обнаружения ISA-серверов

Автоматическое обнаружение ISA-сервера позволяет клиентам автоматически находить подходящий для обслуживания запросов ISA-сервер.

Изучив материал этого занятия, вы сможете:

- ✓ настраивать на клиентских компьютерах автоматическое обнаружение ISA-сервера;
- ✓ устранять неполадки автоматического обнаружения сервера клиентами.

Продолжительность **занятия** - около 30 минут.

Автоматическое обнаружение

Настройка ISA-сервера на подключение клиентов брандмауэра и Web-прокси — весьма несложная задача. Однако последующие изменения конфигурации зачастую поглощают массу времени, в частности, это касается мобильных пользователей, которым, как правило, постоянно требуется дополнительная настройка. При наличии автоматического обнаружения клиенты Web-прокси и брандмауэра самостоятельно находят нужный ISA-сервер. Таким образом, мобильные пользователи подключаются к нужному ISA-серверу самостоятельно, не создавая администраторам дополнительной работы.

Настройка автоматического обнаружения ISA-сервера заключается в последовательном выполнении ряда операций, в том числе публикации возможности автоматического обнаружения на ISA-сервере, включения автоматического обнаружения на клиентских компьютерах, конфигурирования на DHCP-серверах записи протокола WPAD (Web Proxy Auto-discovery Protocol) и обеспечения наличия на DNS-сервере записи A узла ISA-сервера и записи-псевдонима (CNAME) с именем WPAD, указывающей на ISA-сервер. Для корректной работы автоматического обнаружения необходимо предоставить клиентским компьютерам доступ к внутреннему DNS-серверу и/или DHCP-серверу.

Примечание Если вы планируете выполнять практикум в конце занятия, то не выполняйте перечисленные далее операции, а только просмотрите их.

► **Публикация механизма автоматического обнаружения**

1. В дереве консоли ISA Management щелкните правой кнопкой мыши нужный массив и в контекстном меню выберите **Properties.**
2. На вкладке **Auto Discovery** страницы свойств массива установите флажок **Publish automatic discovery information** (публиковать информацию об автоматическом обнаружении).
3. В поле Use **this port for automatic discovery requests** (использовать этот порт для запросов автоматического обнаружения) введите подходящий номер порта (по умолчанию используется порт 80) (рис. 3-5).

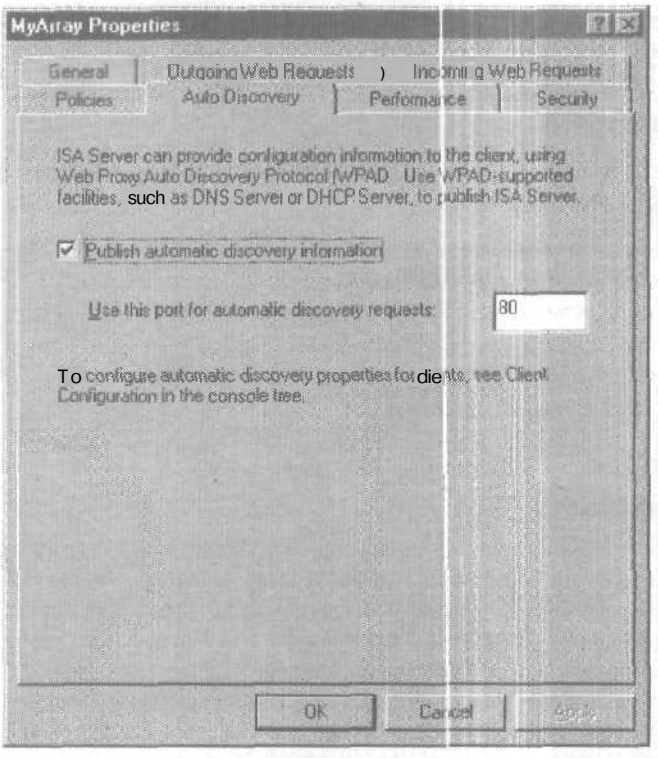


Рис. 3-5. **Публикация автоматического обнаружения путем настройки свойств массива**

▶ **Включение автоматического обнаружения на клиентах брандмауэра**

1. На клиентском компьютере откройте **Control Panel** (Панель управления).
2. Дважды щелкните значок **Firewall Client** и установите флажок **Automatically detect ISA server** (автоматически определять ISA-сервер).

После включения автоматического обнаружения выполняются перечисленные далее операции автоматического обнаружения ISA-сервера клиентами Web-прокси и брандмауэра.

1. При выполнении Winsock-запроса клиент подключается к DNS-серверу или DHCP-серверу,

   На DNS- или DHCP-сервере должна присутствовать запись протокола WPAD (Web Proxy Autodiscovery Protocol), указывающая на соответствующий ISA-сервер.
2. Запросы клиента обрабатываются ISA-сервером, указанным в записи WPAD DNS-сервера или DHCP-сервера.

Настройка WPAD и WSPAD на ONS- и DHCP-серверах

Автоматическое обнаружение позволяет клиентам брандмауэра или Web-прокси запрашивать объекты у ISA-сервера, настроенною на обслуживание подобных запросов. Если ISA-сервер не отвечает, клиент повторяет процедуру автоматического обнаружения.

ISA-сервер использует запись WPAD для определения подходящей записи WSPAD (Winsock Proxy Autodetect). Запись WSPAD не нужно явным образом конфигурировать на DNS-сервере.

Механизм автоматического обнаружения с использованием DNS-сервера поддерживает клиенты под управлением Windows 2000, Windows NT 4.0, Windows 98 и Windows Me.

▶ **Настройка DNS-сервера для автоматического обнаружения ISA-сервера**

1. В меню **Start** (Пуск) последовательно выберите пункты **Programs** (Программы), **Administrative Tools** (Администрирование) и DNS.
2. В дереве консоли щелкните правой кнопкой нужную зону прямого просмотра и в контекстном меню выберите New **Host.**
3. В поле **Name** введите имя ISA-сервера или массива.
4. В поле **IP Address** введите внутренний IP-адрес ISA-сервера.
5. Щелкните кнопку **Add Host** (добавить узел).

   В случае получения сообщения об ошибке, предупреждающего, что запись узла нельзя создать, так как эта запись уже существует, проигнорируйте сообщение, щелкнув кнопку OK.
6. В дереве консоли DNS щелкните правой кнопкой мыши нужную зону прямого просмотра и в контекстном меню выберите New **Alias** (новый псевдоним).
7. В текстовом поле **Alias Name** введите **WPAD.**
8. **Щелкните** кнопку **Browse** и выберите **Host** (A) нужного ISA-сервера.
9. Щелкните **OK.**

Кроме того, для клиентов под управлением Windows 2000, Windows 98 и Windows Me автоматическое обнаружение можно настроить на DHCP-сервере.

▶ **Настройка DHCP-сервера для автоматического обнаружения ISA-сервера**

1. В меню **Start** (Пуск) последовательно выберите пункты **Programs** (Программы), **Administrative Tools** (Администрирование) **и DHCP.**
2. В дереве консоли щелкните правой кнопкой мыши нужный DHCP-сервер и в контекстном меню выберите команду **Set Predefined Options.** Откроется диалоговое окно **Predefined Options and Values** (предопределенные параметры и значения),
3. Щелкните кнопку Add.
4. В поле **Name** введите **WPAD.**
5. В поле со списком **Data Type** выберите **String.**
6. В поле **Code** введите 252.
7. Щелкните кнопку OK.

   Откроется окно Predefined **Options and Values**, в котором в поле со списком **Option Name** выбрана запись 252 **WPAD.**
8. В текстовом поле **String** введите **http://<*строка*>/Wpad.dat**где <*строка*> определяется следующим образом:
   - WPAD — если DNS поддерживает разрешение запросов WPAD;
   - имя ISA-сервера или массива — если DNS не поддерживает разрешение запросов WPAD.
9. Щелкните кнопку OK.
10. В консоли DHCP щелкните правой кнопкой мыши **Scope Options или Server Options** и выберите в контекстном меню команду **Configure Options.**
11. Пролистайте поле со списком **Available Options** (доступные параметры) и установите флажок напротив **Option** 252 **WPAD.**
12. Щелкните кнопку OK.

Автоматическое обнаружение для клиентов брандмауэра

При настройке клиента брандмауэра в **Control Panel** (Панели управления) клиентского компьютера указывается либо конкретный ISA-сервер, либо конфигурируется автоматическое обнаружение. В последнем случае клиент автоматически определяет, к какому ISA-серверу надо подключаться. Существует также возможность централизованно настраивать автоматическое обнаружение ISA-сервера клиентами брандмауэра, эта операция выполняется в узле **Client Configuration** консоли ISA Management.

Проверка автоматического обнаружения для клиентов брандмауэра

После включения автоматического обнаружения на клиенте брандмауэра следует убедиться, что оно работает. Когда при включенном автоматическом обнаружении не удается обнаружить ISA-сервер или разрешить его имя, клиент брандмауэра рассматривается как клиент SecureNAT и сеанс клиента прекращает передавать на ISA-сервер информацию об учетной записи пользователя и имя клиентского компьютера. Чтобы определить, как клиентский компьютер подключается к ISA-серверу — как клиент SecureNAT или брандмауэра, следует инициировать с клиентского компьютера интернет-сеанс, не связанный с Web, например почтовый или новостной сеанс, или выполнить команду nslookup. Затем нужно средствами наблюдения за сеансами консоли ISA Management проверить, передаются ли имена пользователя и компьютера. Если да, то клиент работает как клиент брандмауэра и поддерживает автоматическое обнаружение. В противном случае клиент ведет себя, как клиент SecureNAT, и автоматическое обнаружение не действует.

Автоматическое обнаружение для клиентов Web-прокси

ISA-сервер обеспечивает поддержку автоматического обнаружения для клиентов Web-прокси. Автоматическое обнаружение конфигурируется в разделе LAN **Settings** настройки Internet Explorer, после чего при входе в Интернет перемещающиеся клиенты Web-прокси самостоятельно подключаются к нужному ISA-серверу. Для поддержки автоматического обнаружения клиентами Web-прокси устанавливать и запускать клиент брандмауэра не нужно.

Автоматическое обнаружение поддерживается браузером Internet Explorer, начиная с версии 5.0.

▶ **Настройка Microsoft Internet Explorer 5 на автоматическое обнаружение ISA-сервера**

1. Запустите Internet Explorer.
2. Последовательно выберите пункты меню **Tools** (Сервис) и **Internet Options** (Свойства обозревателя).
3. На вкладке **Connections** (Подключение) щелкните кнопку LAN **Settings** (Настройка сети).
4. Установите флажок **Automatically Detect Settings** (Автоматическое определение параметров).
5. Убедитесь, что флажок **Use a proxy server** (Использовать прокси-сервер) сброшен.

Устранение неполадок автоматического обнаружения

Если автоматическое обнаружение не работает, перед началом устранения неполадок следует ответить на некоторые вопросы.

1. Доступны ли локальные DNS- и/или DHCP-сервер клиентам и ISA-серверу?
2. Исправно ли сетевое соединение между клиентом, DNS-сервером, DHCP-сервером и ISA-сервером?

3. Опубликована ли возможность автоматического обнаружения на ISA-сервере?
4. **Для автоматического обнаружения брандмауэра.** Установлен и запушен ли клиент брандмауэра на клиенте? Установлен ли флажок, отвечающий за обнаружение брандмауэра, в диалоговом окне **Firewall Client Options в Control Panel** (Панель управления)?
5. **Для автоматического обнаружения Web-прокси.** Используется ли Internet Explorer версии не ниже 5.0? Настроено ли автоматическое определение параметров браузером Internet Explorer в диалоговом окне **Local Area Network (LAN) Settings** (Настройка локальной сети)?
6. **При автоматическом обнаружении средствами DHCP-сервера.** Корректно ли настроена запись WPAD на DHCP-сервере? Какие ОС установлены на клиентских компьютерах и относятся ли они к перечню: Windows 2000, Windows 98 или Windows Me? (Автоматическое обнаружение средствами DHCP не поддерживает клиенты под управлением Windows NT или Windows 95.)
7. **При автоматическом обнаружении средствами DNS-сервера.** Есть ли на DNS-сервере запись A узла ISA-сервера? Создана ли запись-псевдоним (CNAME) с именем WPAD, указывающая на ISA-сервер? Определен ли данный внутренний DNS-сервер в качестве дополнительного DNS-сервера в свойствах протокола TCP/IP?

Практикум. Настройка автоматического обнаружения

Вы выполните операции по настройке автоматического обнаружения ISA-сервера в сети. Так как в DNS уже содержится запись A узла локального компьютера и в используемой конфигурации из двух серверов нет DHCP, задания практикума небольшие.

Для выполнения заданий практикума следует установить и запустить клиент брандмауэра на компьютере Server2. Кроме того, *к* свойствах протокола TCP/IP компьютера Server2 в качестве основного DNS-сервера нужно указать внешний DNS-сервер интернет-провайдера, а в качестве дополнительного DNS-сервера — адрес компьютера Server1 (192.168.0.1). И, наконец, предполагается, что на ISA-сервере создано правило протокола, пропускающее весь IP-трафик.

Задание 1. Публикация информации для автоматического обнаружения

В этом задании вы опубликуете информацию для автоматического обнаружения на ISA-сервере.

1. Войдите в систему Server1 под учетной записью Administrator (Администратор).
2. Откройте консоль ISA Management.
3. Раскройте дерево консоли, щелкните правой кнопкой мыши узел **MyArray**, в контекстном меню выберите пункт **Properties.** Откроется диалоговое окно свойств массива MyArray.
4. Перейдите на вкладку **Auto Discovery.**
5. Установите флажок **Publish automatic discovery information**.
6. Убедитесь, что для запросов автоматического обнаружения используется порт 80, и щелкните кнопку **OK.**

   Откроется диалоговое окно **ISA Server Warning**.
7. Установите переключатель Save **the changes and restart the service(s)** (сохранить изменения и перезапустить службу).
8. Щелкните кнопку **OK**.

Задание 2. Создание записи-псевдонима (CNAME) WPAD в DNS

Для работы механизма автоматическою определения необходимо создать в DNS запись-псевдоним с именем WPAD, указывающую на ISA-сервер. Задание выполняется на Server1.

1. В меню Start (Пуск) последовательно выберите **Programs** (Программы), **Administrative Tools** (Администрирование) и DNS.
2. В дереве консоли DNS щелкните правой кнопкой мыши соответствующую зону прямого просмотра и в контекстном меню выберите New **Alias.** Если вы выполнили инструкции раздела «Об этой книге», это будет локальная зона прямого просмотра домена domain01.
3. В поле **Alias Name** введите **WPAD.**
4. В поле **Fully qualified name for target host** (полное имя узла-приемника) введите **server1.domain01.local**.
5. Щелкните кнопку **OK.**

Задание 3. Включение автоматического обнаружения на клиенте брандмауэра

Задание выполняется на компьютере Server2. Предполагается, что на Server2 установлен и запущен клиент брандмауэра.

1. Войдите в домен DomainOl с компьютера Server2 под учетной записью Administrator (Администратор).
2. Откройте **Control Panel** (Панель управления).
3. Дважды щелкните значок **Firewall Client.** Откроется диалоговое окно **Firewall Client Options**.
4. Установите флажок **Automatically detect ISA server** (автоматически обнаруживать ISA-сервер).
5. Щелкните кнопку **Update Now.** Откроется диалоговое окно, сообщающее об успешном выполнении операции.
6. Щелкните OK, чтобы закрыть информационное окно.
7. Щелкните OK, чтобы закрыть диалоговое окпо **Firewall Client Options.**

Задание 4. Проверка автоматического обнаружения

После настройки автоматического обнаружения следует убедиться в корректности его работы. Прежде всего на клиентских компьютерах следует активировать клиенты брандмауэра. Однако клиенты брандмауэра ведут себя соответствующим образом только при корректной работе механизма автоматического обнаружения, в противном случае они превращаются в клиентов SecureNAT.

Таким образом, корректность работы автоматического обнаружения выясняется путем проверки информации о сеансе клиента в консоли ISA Management. Если в информации о сеансе доступны имена пользователя и компьютера, то автоматическое обнаружение выполняется верно. Если же доступен лишь IP-адрес клиента, то автоматическое обнаружение настроено некорректно, и клиентский компьютер не обнаруживает ISA-сервер.

1. Войдите в систему Server2 под учетной записью Administrator (Администратор), откройте окно командной строки и введите:

   ```
   nslookup www.microsoft.com
   ```

   Появится сообщение о том, что компьютер успешно подключился к внешнему DNS-серверу.

2. В системе Server1 раскройте в дереве консоли ISA Management узел Monitoring и щелкните Sessions.
3. В меню View отметьте команду Advanced.
4. Щелкните правой кнопкой мыши в области сведений и в контекстном меню выберите команду Refresh.

В списке активных сеансов должен присутствовать интернет-сеанс системы Server2. Обратите внимание, что отображаются имя пользователя — Administrator — и имя клиентского компьютера — Server2. Информация для аутентификации успешно поступила на ISA-сервер, следовательно, клиент является клиентом брандмауэра и автоматическое обнаружение выполняется корректно.

Резюме

При корректной настройке автоматического обнаружения все клиенты Web-прокси и клиенты брандмауэра автоматически обнаруживают нужный ISA-сервер. Клиентам брандмауэра автоматическое обнаружение позволяет самостоятельно находить ISA-сервер для обслуживания их запросов. При использовании совместно со службой Web-прокси автоматическое обнаружение позволяет перемещающимся клиентам всегда находить нужный ISA-сервер при подключении к Интернету. Для нормальной работы автоматического обнаружения в сети необходимо соответствующим образом настроить DNS и/или DHCP. Для настройки автоматического обнаружения требуется: опубликовать возможность автоматического обнаружения на ISA-сервере, включить автоматическое обнаружение на клиентских компьютерах, настроить запись протокола WPAP на DHCP-серверах сети, убедиться, что DNS-сервер сети содержит как запись A узла ISA-сервера, так и запись псевдонима (CNAME) с именем WPAD, указывающую на ISA-сервер.

Занятие 4. Устранение неполадок, возникающих при подключении клиентов к ISA-серверу

Подключение к Интернету при помощи только что установленного ISA-сервера весьма несложно, но некоторые факторы способны усложнить конфигурацию, что и приводит к возникновению неполадок при подключении. В этом занятии рассматриваются наиболее типичные неполадки, возникающие при подключении клиентов и доступе в Интернет по телефонной линии.

Изучив материал этого занятия, вы сможете:

- ✓ устранять неполадки, возникающие при подключении клиентов к ISA-серверу;
- ✓ устранять неполадки подключений ISA-сервера по телефонной линии;
- ✓ перезапускать службы ISA-сервера после изменений в конфигурации.

Продолжительность занятия — около 20 минут.

Устранение неполадок при подключении клиентов

Неполадки подключения клиентов варьируются от неудовлетворительной производительности до полного отсутствия доступа клиентов SecureNAT, брандмауэра и Web-прокси в Интернет. Чтобы облегчить устранение неполадок впоследствии, постарайтесь не усложнять конфигурацию сети и отслеживать все изменения, вносимые после первоначальной успешной установки. Вообще говоря, наиболее эффективен систематический подход при выявлении неполадок, когда сначала проверяют наличие физического подключения, затем последовательно проверяют все более высокие уровни связи — вплоть до отдельных политик доступа на ISA-сервере.

При устранении неполадок мы советуем руководствоваться таблицей 3-4, в которой перечислены типичные ошибки в конфигурациях клиентов, которые препятствуют подключению к Интернету.

Таблица 3-4. Типичные ошибки в конфигурации клиентов

Неполадка	Причина	Способ устранения
Внутренние подключения клиентов брандмауэра работают слишком медленно	Клиенты не в состоянии разрешать локальные имена средствами внешнего DNS-сервера, так как на нем отсутствуют необходимые записи. Клиенты ожидают тайм-аута DNS-сервера до перехода к другим методам разрешения имен	На внутреннем DNS-сервере необходимо настроить имена и адреса всех внутренних узлов. Кроме того, если применяется фильтрация пакетов, нужно создать фильтр IP-пакетов, который использует предопределенный фильтр DNS Lookup, чтобы разрешить ISA-серверу отравлять запросы расположенных в Интернете DNS-имен
Клиенты SecureNAT не в состоянии подключиться к Интернету	ISA-сервер не в состоянии подключать к Интернету некорректно настроенные клиенты SecureNAT	Настройте основной шлюз и DNS-сервер на клиентах

Таблица 3-4. *(окончание)*

Неполадка	Причина	Способ устранения
Клиенты не в состоянии подключиться к внешним узлам с поддержкой SSL	Когда клиент подключается через Web-прокси к безопасному Web-узлу, ISA-сервер должен открыть туннель для соответствующего трафика, так как для последнего поддерживается сквозное шифрование. По умолчанию ISA-сервер разрешает туннельные подключения только по портам 443 и 563 (SecureNews). Попытки клиентов подключиться к защищенным узлам Интернета по другим портам блокируются	Чтобы разрешить открывать туннель для других портов, внесите соответствующие изменения в параметры COM-объекта администрирования ISA-сервера FPCProxyTunnelPortRange
Подключения клиентов SecureNAT перестают работать, когда вместо IP-адреса указываются имена компьютеров	Если клиент использует внутренний DNS-сервер, он не может разрешать доменные имена, расположенные в Интернете	Настройте DNS-сервер на пересылку запросов на внешний DNS-сервер (DNS-сервер Интернета). Альтернативный вариант — настроить клиенты на использование DNS-сервера, пересылающего запросы разрешения имен на внешний DNS-сервер
Клиенты SecureNAT не в состоянии подключиться по определенному порту, так как истекает время, отводимое на установку подключения, несмотря на наличие правила протокола, пропускающего весь IP-трафик	Клиентам SecureNAT разрешается подключаться только по протоколам, перечисленным в узле Protocol Definitions дерева консоли ISA Management. Кроме того, протокол не вправе создавать дополнительные (вторичные) подключения, если в фильтре соответствующего протокола они не разрешены	Если приложение использует только один порт, определите протокол, в котором этот порт является первичным. Если приложение подключается по нескольким портам, в том числе определяемым динамически, их следует определить в фильтре приложения
Сервер не в состоянии создать привязку или вьщелить определенный порт	Имеет место конфликт распределения портов — более одной службы (в число этих служб может входить и сам ISA-сервер) запрашивает привязку к определенному порту внешнего интерфейса	Вообще говоря, Microsoft не рекомендует запускать дополнительные службы совместно с основным брандмауэром. По возможности следует устанавливать другие службы на отдельные компьютеры, расположенные во внутренней сети, защищенной ISA-сервером. Создайте привязку другого сервера к внутреннему интерфейсу, чтобы внешний интерфейс прослушивался только ISA-сервером

Устранение неполадок при подключении по телефонной линии

Существует несколько основных причин неполадок при подключении по телефонной линии. Способы их устранения перечислены в таблице 3-5.

Таблица 3-5. Неполадки при подключении по телефонной линии

Неполадка	Причина	Способ устранения
Автоматическое подключение по телефонной линии к Интернету не получается, хотя ручное подключение выполняется без проблем	Указаны неправильные реквизиты пользователя в записи подключения по телефонной линии, а в сетевом подключении учетные данные указаны корректно	Введите правильные реквизиты в запись подключения по телефонной линии
	На ISA-сервере не разрешено использование подключения по тглефонной линии	Перенастройте сетевое подключение по телефонной линии, разрешив его применение всем пользователям. Подробнее об этом — в справочной системе Windows 2000
	Клиент является клиентом SecureNAT	Установите и запустите клиент брандмауэра
Подключение к Интернету заканчивается неудачей, так как номер уже набирается	Другая служба, установленная на компьютере, использует это подключение по телефонной линии	Попробуйте подключиться через некоторое время — ISA-сервер попытается установить подключение попозже. Если неполадка не устраняется, перезапустите службы ISA-сервера
Подключение по телефонной линии прервалось	Кто-то нечаянно прервал подключение	Перезапустите службы ISA-сервера — они автоматически выполнят повторное подключение
Подключение по телефонной линии никогда не разрывается, даже при отсутствии запросов, требующих установки подключения по телефонной линии	При получении клиентского запроса, адресуемого компьютеру локальной сети, ISA-сервер отправляет запросы разрешения имени как внутреннему, так и внешнему DNS-серверу	Настройте ISA-сервер на использование только внутренних DNS-серверов. Имейте в виду, что такое решение работоспособно, только когда внутренний DNS-сервер способен по мере необходимости переводить запросы разрешения имени на внешний DNS-сервер
Невозможно подключиться к Интернету по телефонной линии	Клиент является клиентом SecureNAT, а запись подключения по телефонной линии сконфигурирована не до конца	Установите на компьютер клиент брандмауэра. Также можно создать запись подключения по телефонной линии и настроить свойства сети на маршрутизацию к вышестоящим серверам через подключение по телефонной линии

Перезапуск служб после изменений в конфигурации

Если подключение к Интернету внезапно прервалось в момент использования клиентскими компьютерами, попробуйте перезапустить службы ISA-сервера: службу брандмауэра, Web-прокси или обе. Некоторые изменения в конфигурации ISA-сервера также требуют перезапуска одной или более служб ISA-сервера на всех серверах массива, в противном случае клиенты не смогут выполнять подключения. В случае таких изменений консоль ISA Management обычно (но не всегда, когда это нужно) открывает диалоговое окно, информирующее о необходимости перезапуска службы.

В таблице 3-6 перечислены изменения конфигурации, при которых необходим перезапуск служб.

Таблица 3-6. Изменения в конфигурации, при которых необходим перезапуск служб ISA-сервера

Изменение в конфигурации	Перезапускаемая служба
Установка, удаление, включение, выключение фильтра приложения	Служба брандмауэра
Увеличение или уменьшение размера кэша, добавление или удаление диска из кэша	Служба брандмауэра
Изменения в LAT, влияющие на внутреннее или внешнее состояние сетевого адаптера	Служба брандмауэра, служба Web-прокси
Включение или выключение фильтрации пакетов	Служба брандмауэра
Включение или отключение сетевого адаптера	Служба брандмауэра, служба Web-прокси
Изменение IP-адреса сетевого адаптера	Служба брандмауэра, служба Web-прокси
Изменения таблицы маршрутизации	Служба брандмауэра
Установка, включение, отключение, удаление или изменение порядка Web-фильтров	Служба Web-прокси
Изменение номеров портов Web-прокси	Служба Web-прокси
Изменение параметров службы брандмауэра в консоли ISA Management	Служба брандмауэра
Обновление сертификата SSL	Служба Web-прокси
Добавление сервера в массив, удаление сервера из массива	Служба Web-прокси
Изменения в сетевом интерфейсе привратника H.323 (Gatekeeper H.323)	Служба Gatekeeper H.323
Изменения в конфигурации сети, изменения в конфигурации цепочек брандмауэров	Служба брандмауэра

На рис. 3-6 показана панель заданий **Monitor Servers And Services,** в которой осуществляется запуск и останов служб ISA-сервера.

▶ **Запуск службы**

1. В дереве консоли ISA Management щелкните узел **Services.**
2. В меню **View** отметьте команду **Advanced.**
3. В области сведений щелкните правой кнопкой мыши нужную службу и в контекстном меню выберите команду **Start.**

► **Останов службы**

1. В дереве консоли ISA Management щелкните узел **Services.**
2. В меню **View** отметьте команду **Advanced.**
3. В области сведений щелкните правой кнопкой мыши нужную службу и в контекстном меню выберите команду Stop.

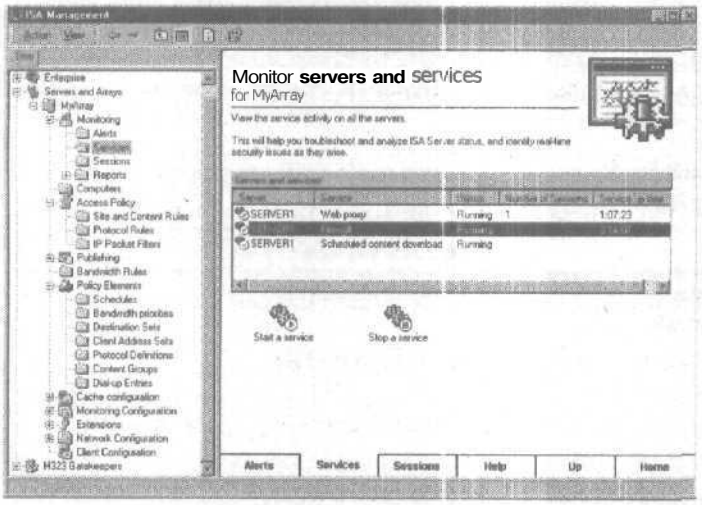


Рис. 3-6. Запуск и останов служб ISA-сервера в режиме панели заданий (taskpad). Управление службами также выполняется в режиме Advanced

Резюме

Неполадок подключения обычно очень мало, если не усложнять конфигурацию ISA-сервера и тщательно отслеживать все изменения, вносимые после первоначальной установки. При устранении неполадок, возникающих при подключении, рекомендуется систематический подход. Воспользуйтесь описанными в этом занятии методами устранения типовых неполадок.

Кроме того, многие неполадки при подключении клиентов возникают из-за изменений в конфигурации ISA-сервера. После внесения изменений в конфигурацию ISA-сервера необходимо перезапустить одну или несколько служб ISA-сервера на всех серверах массива.

Закрепление материала

9 | Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Ответы для самопроверки — в приложении А «Вопросы и ответы» в конце книги.

1. Вы устанавливаете ISA-сервер и настраиваете его службы брандмауэра и Web-кэширования в двух филиалах компании. Требуется изучить потребности пользователей и дать рекомендации по настройке клиентских компьютеров. В каждом из филиалов работает по 20 сотрудников, кроме того, в штате предусмотрены 10 специалистов по обслуживанию, которые курсируют между филиалами и подключают свои портативные компьютеры к любому доступному порту Ethernet. Расположение офисных компьютеров в филиалах более или менее постоянное, и нет необходимости определять для них особые правила доступа. Требуется добиться максимальной эффективности установки и последующего сопровождения ISA-сервера. Какие компьютеры вы порекомендуете сконфигурировать как клиенты брандмауэра (если таковые вообще нужны), а какие — как клиенты SecureNAT?

2. Чем отличаются файлы Mspclnt.ini и Wspcfg.ini на компьютерах — клиентах брандмауэра?

3. Какие действия выполняются в процессе обслуживания запроса клиента при активном механизме автоматического обнаружения?

4. Можно ли путем настройки записей подключений ISA-сервера по телефонной линии обеспечить совместное использование клиентами Web-прокси безопасного подключения к Интернету по телефонной линии?

5. Ваша организация недавно перешла с выделенного подключения к Интернету на подключение по телефонной линии. При этом вы отключили внешний сетевой адаптер и настроили запись подключения по телефонной линии на существующее подключение по телефонной линии. Однако, когда ISA-сервер дозванивается до провайдера через это подключение, никто из клиентов не в состоянии установить связь с Интернетом. Что вы порекомендуете предпринять в первую очередь для устранения этой неполадки?

ГЛАВА 4

Конфигурирование безопасного доступа в Интернет с использованием политик доступа

Занятие 1. Создание политик доступа на ISA-сервере 101

Занятие 2. Создание элементов политики 107

Занятие 3. Настройка правил протоколов 117

Занятие 4. Настройка правил узлов и содержимого 127

Занятие 5. Настройка фильтров IP-пакетов 137

Занятие 6. Настройка ISA-сервера на обнаружение внешних атак и вторжений 147

Закрепление материала 152

В этой главе

При настройке политики безопасности доступа в Интернет необходимо учитывать конфигурацию конкретной сети и требования по безопасности. Последние отличаются для разных пользователей, компьютеров, IP-адресов источников и адресатов и зависят от времени поступления запросов, протоколов, запрашиваемых Web-узлов и типов содержимого. Для создания политики доступа, учитывающей все эти особенности сети, необходимо знать, как ISA-сервер обрабатывает запросы клиентов. В процессе конфигурирования политики доступа создаются элементы политики, отвечающие особенностям вашей сети, например расписания или подмножества клиентов. Затем выполняется настройка трех типов правил, определяющих политику доступа: правил протоколов, правил узлов и содержимого и фильтров IP-пакетов. Для предотвращения внешних вторжений в сеть рекомендуется включить механизм выявления вторжений на брандмауэре.

Прежде всего

Для изучения материалов этой главы необходимо:

- сконфигурировать компьютеры, как описано в разделе «Об этой книге». Компьютер Server1 следует установить в качестве контроллера домена, а компьютер Server2 — в качестве члена домена. Компьютеру Server1 следует назначить IP-адрес 192.168.0.1, а компьютеру Server2 — IP-адрес 192.168.0.2. Кроме того, необходимо обеспечить подключение Server1 к Интернету по телефонной линии;
- выполнить все задания глав 1–3.

Занятие 1. Создание политик доступа на ISA-сервере

Одна из основных функций ISA-сервера — подключение локальной сети к Интернету и зашита от опасных данных, поступающих из внешних источников. Чтобы настроить безопасное подключение к Интернету в соответствии с потребностями конкретной сети, на ISA-сервере определяют политику доступа, разрешающую внутренним клиентам доступ лишь к определенным узлам Интернета. Такая политика совместно с правилами маршрутизации определяет порядок взаимодействия работы клиентов в Интернете.

Изучив материал этого занятия, вы сможете:

- ✓ рассказать о том, как ISA-сервер обрабатывает исходящие запросы;
- ✓ рассказать о принципах обработки ISA-сервером запросов, прошедших аутентификацию клиентов брандмауэра и Web-прокси;
- ✓ определять уровень системной безопасности ISA-сервера.

Продолжительность занятия — около 30 минут.

Управление исходящими запросами

Обрабатывая исходящий запрос и определяя возможность доступа, ISA-сервер руководствуется правилами маршрутизации, правилами узлов и содержимого и правилами протоколов. Пересылка запроса разрешается только при наличии правила протоколов и правила узлов и содержимого, разрешающих запрос, и отсутствии правил, запрещающих прохождение такого запроса. После установки ISA-сервера в режиме брандмауэра или в смешанном режиме активизируется определенное по умолчанию правило узлов и содержимого, разрешающее доступ ко всем узлам и типам содержимого. Однако никаких правил протоколов при установке ISA-сервера не создается.

Правила протоколов и правила узлов и содержимого регулируют доступ к содержимому и применяются к целым подмножествам адресов клиентов, определяемых по их IP-адресам (то есть диапазонам IP-адресов), или к конкретным пользователям или их группам. Порядок обработки запросов ISA-сервером определяется типом клиентов (клиенты SecureNAT, брандмауэра или Web-прокси) и конфигурацией самого сервера.

При обработке исходящих запросов правила и фильтры пакетов применяются в следующей последовательности:

1. правила протоколов;
2. правила узлов и содержимого;
3. фильтры IP-пакетов;
4. правила маршрутизации или конфигурация цепочки (иерархии) брандмауэров.

Порядок обработки исходящего Web-запроса показан на рис. 4-1.

Прежде всего ISA-сервер проверяет правила протоколов. Он пропускает запрос только при наличии правила протоколов, разрешающего прохождение запроса, и при отсутствии правил протоколов, запрещающих его.

После проверки правил протоколов ISA-сервер обращается к правилам узлов и содержимого. Запрос пропускается только при наличии правила узлов и содержимого, разрешающего данный запрос, и при отсутствии правил узлов и содержимого, запрещающих его.

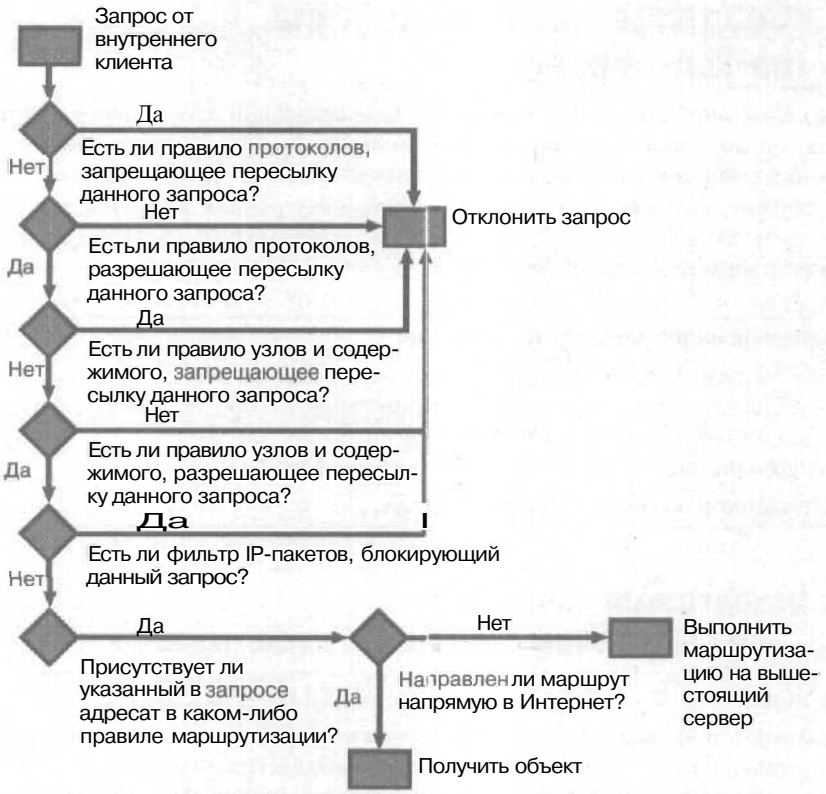


Рис. 4-1. Порядок обработки запроса на доступ к объекту

После проверки правил узлов и содержимого ISA-сервер определяет, есть ли фильтр IP-пакетов, который блокирует данный запрос. Обратите внимание, что, в отличие от правил протоколов и правил узлов и содержимого, наличие фильтров IP-пакетов, разрешающих клиентский запрос, не требуется.

Внимание! При доступе в Интернет поведение ISA-сервера существенно отличается от поведения клиентов. Для разрешения полноценного доступа самого ISA-сервера необходимы фильтры IP-пакетов. В отличие от клиентов, чтобы получить доступ в Интернет с компьютера ISA-сервера, одной настройки разрешающих правил протоколов и правил узлов и содержимого недостаточно. Однако, поскольку фильтры IP-пакетов статические, а не динамические, как правила, обычно не предполагается использовать компьютер, на котором установлен ISA-сервер, для доступа в Интернет. Поэтому в книге рассказано лишь об обеспечении безопасного доступа в Интернет клиентов (а не самого) ISA-сервера. (Настройка фильтров IP-пакетов подробно рассматривается в занятии 5 этой главы.)

И, наконец, ISA-сервер проверяет правила маршрутизации (если объект запрашивается клиентом Web-прокси) или конфигурацию иерархии брандмауэров (если объект запрашивается клиентом SecureNAT или брандмауэра), чтобы определить порядок обслуживания запроса.

Допустим, ISA-сервер установлен в смешанном режиме или в режиме брандмауэра на компьютере с двумя сетевыми картами, одна из которых подключена к Интернету, а дру-

гая — к локальной сети. Корпоративные правила разрешают доступ всем пользователям ко всем узлам. В этом случае в политике достаточно предусмотреть лишь два правила доступа:

- **правило протоколов,** разрешающее всем внутренним пользователям применение любых протоколов в любое время;
- **правило узлов и содержимого,** разрешающее всем пользователям доступ к содержимому всех узлов в любое время. Обратите внимание, что это правило разрешает доступ внутренних клиентов в Интернет, но не внешних — к локальной сети.

Настройка политики доступа

Политики доступа ISA-сервера состоят из правил узлов и содержимого, правил протоколов и фильтров IP-пакетов. На изолированных серверах создаются изолированные политики доступа. В массивах создают и применяют политику доступа уровня массива, политику доступа уровня предприятия или сочетание этих двух политик.

Правила политики доступа применяются к клиентам всех типов: к клиентам брандмауэра, SecureNAT и Web-прокси.

Правила и аутентификация

Правила протоколов и правила узлов и содержимого разрешают или запрещают конкретным пользователям доступ к определенным администратором протоколам, узлам Интернета или содержимому. Когда правила настроены и приведены в действие, прежде чем пропустить клиентский запрос через брандмауэр, ISA-сервер выполняет его аутентификацию. Эта процедура различна для клиентов SecureNAT, брандмауэра и Web-прокси.

Примечание В отличие от правил политики, применяемых к определенным пользователям и группам, правила, действующие на клиентские компьютеры, применяются ко всем клиентам SecureNAT, брандмауэра и Web-прокси. Правила, применяемые к клиентским компьютерам, настраиваются для подмножеств адресов клиентов (диапазонов IP-адресов), а не имен компьютеров. Так как все типы клиентов сообщают ISA-серверу IP-адрес клиентского компьютера, они автоматически предоставляют информацию, необходимую для применения подобных правил.

Клиенты SecureNAT и аутентификация

Запросы клиентов SecureNAT — это все не связанные с Web запросы в Интернет, поступающие с компьютеров, на которых не установлен клиент брандмауэра. Например, почтовые запросы и запросы новостей считаются сеансами SecureNAT, если на соответствующих клиентских компьютерах нет активного клиента брандмауэра.

Выполняя запрос, клиенты SecureNAT не сообщают ISA-серверу имя пользователя или компьютера, Поэтому при наличии правила политики доступа, предусматривающего аутентификацию, ISA-сервер отвергает все запросы по SecureNAT.

Допустим, политика доступа состоит из правил протоколов и правил узлов и содержимого, разрешающих доступ в любое время ко всем узлам по всем протоколам членам группы Domain Users (Пользователи домена). В этом случае все почтовые запросы пользователя John, выполненные с клиента SecureNAT, блокируются, даже если он является членом группы Domain Users. Причина в том, что клиенты SecureNAT не поддерживают аутентификацию, которую требуют правила политики доступа. Чтобы получить доступ в Интернет по протоколам, отличным от протоколов Web, пользователю John следует установить на своем компьютере клиент брандмауэра.

Клиенты брандмауэра и аутентификация

Клиенты брандмауэра при запросе сообщают ISA-серверу имя пользователя и компьютера. Поэтому к сеансам клиентов брандмауэра можно применять требующие аутентификацию правила политики доступа, а запросы таких клиентов, не связанные с Web, не отвергаются так категорически, как это происходит с клиентами SecureNAT.

Допустим, что политика доступа состоит из правил протоколов и правил узлов и содержимого, разрешающих доступ в любое время ко всем узлам по любому протоколу членам группы Domain Users. Если пользователь John выполнит почтовый запрос с компьютера — клиента брандмауэра, запрос пройдет через ISA-сервер только при том единственном условии, что John входит в группу Domain Users. Однако если на сервере есть еще одно правило протоколов, запрещающее доступ пользователю John, ISA-сервер заблокирует такой, не связанный с Web, запрос.

Клиенты Web-прокси и аутентификация

По умолчанию доступ клиентов Web-прокси осуществляется анонимно, но есть два условия, при которых им требуется предоставлять идентификационную информацию. При выполнении хотя бы одного из следующих условий правила, определенные для конкретных пользователей или групп, применяются к сеансам клиентов Web-прокси:

- стандартные (по умолчанию) свойства ISA-сервера изменены, теперь требуется аутентификация исходящих Web-запросов (по умолчанию проверка подлинности не нужна);
- политика доступа содержит разрешающее правило (правило протоколов или правило узлов и содержимого), определенное для конкретных пользователей или групп.

  Любое разрешающее правило, определенное для конкретных пользователей или групп, требует от клиентов Web-прокси предоставлять свои реквизиты при создании сеанса. Аналогичные запрещающие правила политики доступа не оказывают влияния на клиентов Web-прокси, если только нет разрешающего правила, для которого аутентификация обязательна.

Допустим, что стандартные свойства исходящих Web-запросов не изменялись, а политика доступа состоит из следующих правил:

- правила протоколов, разрешающего доступ всем запросам по всем протоколам в любое время;
- правила протоколов, запрещающего пользователю John доступ по любому протоколу;
- правила узлов и содержимого, разрешающего доступ ко всем адресатам всех запросов в любое время.

В этом случае Web-запрос пользователя John не заблокируется, так как нет разрешающего правила, которое могло бы потребовать идентификационные реквизиты у клиентов Web-прокси. Однако если добавить в эту политику правило протоколов или правило узлов и содержимого, разрешающее полный доступ всем членам группы Domain Users, все Web-запросы пользователя John будут блокироваться.

► **Включение требования аутентификации при всех Web-запросах**

1. В дереве консоли ISA Management щелкните правой кнопкой мыши нужный массив и в контекстном меню выберите команду **Properties.**
2. На вкладке **Incoming Web Requests** (входящие Web-запросы) или **Outgoing Web Requests** (исходящие Web-запросы) установите флажок **Ask unauthenticated users for identification.**

Примечание Изменения вступят в силу только после перезагрузки ISA-сервера.

Системная безопасность ISA-сервера (блокировка изменений системной конфигурации)

В состав ISA-сервера входит мастер ISA Server Security Configuration, который применяется для определения требуемых параметров безопасности системы на всех серверах массива, то есть различного уровня *блокировок для предотвращения изменений системной конфигурации* (system hardening). Он позволяет выбрать один из трех уровней безопасности системы:

- **Dedicated** — применяется, когда ISA-сервер используется исключительно в качестве брандмауэра и на нем не работают никакие другие интерактивные приложения;
- **Limited Services** — применяется, когда ISA-сервер используется как брандмауэр и сервер кэширования. В этом случае можно защитить ISA-сервер дополнительным брандмауэром;
- **Secure** — применяется, когда на компьютере кроме ISA-сервера установлены и другие серверы, например IIS (Internet Information Services), серверы баз данных, серверы SMTP

Чтобы запустить мастер ISA Server Security Configuration, выберите папку **Computers** в дереве консоли ISA Management, в области сведений щелкните правой кнопкой мыши значок нужного сервера и в контекстном меню выберите команду **Secure** (рис. 4-2).

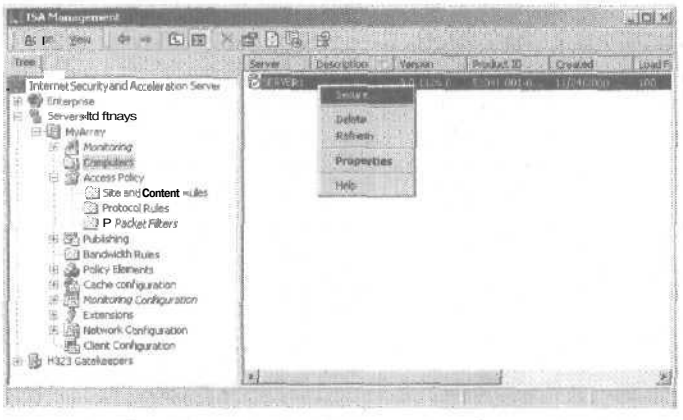


Рис. 4-2. Запуск мастера ISA Server Security Configuration

▶ **Настройка уровня безопасности системы**

1. В дереве консоли ISA Management шелкните папку **Computers.**
2. В области сведений шелкните правой кнопкой мыши нужный компьютер и в контекстном меню выберите команду **Secure.**
3. Последовательно выполняйте инструкции мастера.

Мастер Getting Started

В составе ISA-сервера поставляется мастер Getting Started (рис. 4-3), который позволяет создать политики доступа, отвечающие особенностям вашей сети. Выполнив все инструкции мастера, вы получите настроенное безопасное подключение сети к Интернету через ISA-сервер.

Мастер Getting Started предназначен для:

- настройки параметров политики предприятия (только в массивах);
- создания элементов политики уровня предприятия (только в массивах);
- создания правил протоколов уровня предприятия (только в массивах);
- создания правил узлов и содержимого уровня предприятия (только в массивах);
- создания элементов политики уровня массива;

- создания правилпротоколов уровня массива;
- создания правил узлов и содержимого уровня массива;
- установки уровня безопасности системы;
- настройки фильтрации пакетов;
- настройки маршрутизации и построения иерархии брандмауэров;
- создания политики кэширования.

Мастером Getting Started можно воспользоваться в любой момент после настройки политики доступа,

Запуск мастера Getting Started

1. В консоли ISA Management откройте меню **View** и отметьте команду **Taskpad**.
2. В дереве консоли выберите узел **Internet Security And Acceleration Server.**
3. В области сведений щелкните значок **Getting Started Wizard.**
4. Последовательно выполняйте инструкции мастера, отображаемые в области сведений.

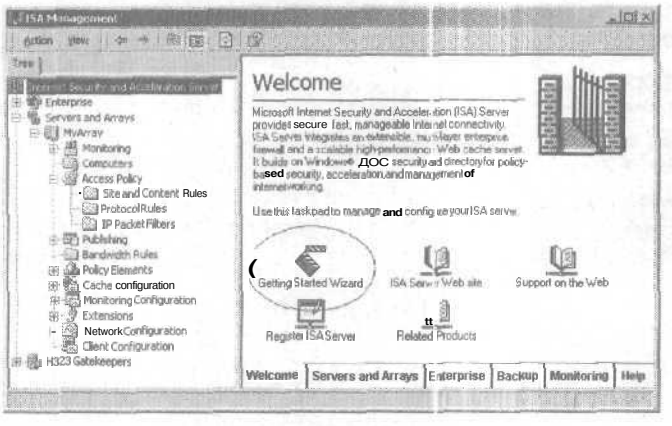


Рис. 4-3. Запуск мастера Getting Started

Резюме

На ISA-сервере создаются политики доступа, состоящие из правил узлов и содержимого, правил протоколов и фильтров IP-пакетов. Клиентские запросы пропускаются только при наличии правила узлов и содержимого и правила протоколов, разрешающих данный тип запросов, и отсутствии правил, запрещающих такие запросы.

Выполняя запрос, клиенты SecureNAT не сообщают ISA-серверу имя пользователя или компьютера, поэтому при наличии правила политики доступа, предусматривающего аутентификацию, ISA-сервер отвергает все подобные запросы. Клиенты брандмауэра предоставляют информацию для идентификации пользователя; на порядок обработки поступающих от них исходящих запросов влияет членство в группах и права пользователей. При запросе содержимого клиентами Web-прокси информация для аутентификации передается на ISA-сервер только в том случае, когда ISA-сервер требует от пользователей предоставлять идентификационные сведения или если существует разрешающее правило политики, требующее выполнять аутентификацию.

Для повышения безопасности системы в состав ISA-сервера входит мастер ISA Server Security Configuration, который позволяет установить на всех серверах массива нужные параметры безопасности системы. Кроме того, для облегчения настройки безопасности и политики доступа применяют мастер Getting Started, который позволяет создавать политики доступа для конкретной сети.

Занятие 2, Создание элементов политики

Политики доступа, создаваемые на ISA-сервере, определяют, каким видам трафика, в какое время, из каких источников и к каким адресатам разрешается проходить через брандмауэр. Параметры политики доступа, такие как тип содержимого, расписание, подмножество клиентов или адресатов, называются *элементами политик*. Это «кирпичики», из которых строятся правила политики. Пользователю разрешается определять собственные элементы политики и настраивать параметры правил в соответствии с потребностями конкретной сети.

Изучив материал этого занятия, вы сможете:

- ✓ создавать и настраивать элементы политики на ISA-сервере.

Продолжительность занятия — около 45 минут.

Элементы политики

Элементы политики — это параметры или строительные блоки правил политики. Создавая правило, которое запрещает какому-то подмножеству клиентов доступ к определенному Web-содержимому в указанные временные рамки, вы используете такие элементы политик, как подмножество клиентов, Web-содержимое и расписание. ISA-сервер позволяет создавать элементы политики и затем использовать их в правилах. Элементы политики создаются на уровне предприятия или на уровне массива. Существуют следующие типы элементов политики:

- расписания;
- приоритеты пропускной способности;
- подмножества адресатов;
- подмножества адресов клиентов;
- определения протоколов;
- группы содержимого;
- записи подключений по телефонной линии.

Элементы политики уровня массива и уровня предприятия

Когда при использовании ISA Server Enterprise Edition требуется определить политику доступа на уровне предприятия, определяют элементы политики уровня предприятия. В дальнейшем они применяются при создании правил уровня предприятия.

При совместном использовании политик уровня массива и уровня предприятия вы вправе применять в правилах уровня массива элементы политики уровня предприятия.

На изолированных серверах разрешается создавать только элементы политики уровня массива.

Настройка расписаний

Для определения времени действия создаваемого правила используют расписание.

ISA-сервер содержит два предустановленных расписания:

- **Weekends** (выходные) — суббота и воскресенье;
- **Workhours** (рабочее время) — с 9 до 17 часов, ежедневно, с понедельника по пятницу.

Кроме того, ISA-сервер позволяет создавать настраиваемые расписания (рис. 4-4).

Их обычно используют в следующих правилах:

- правилах узлов и содержимого;
- правилах протоколов;
- правилах пропускной способности.

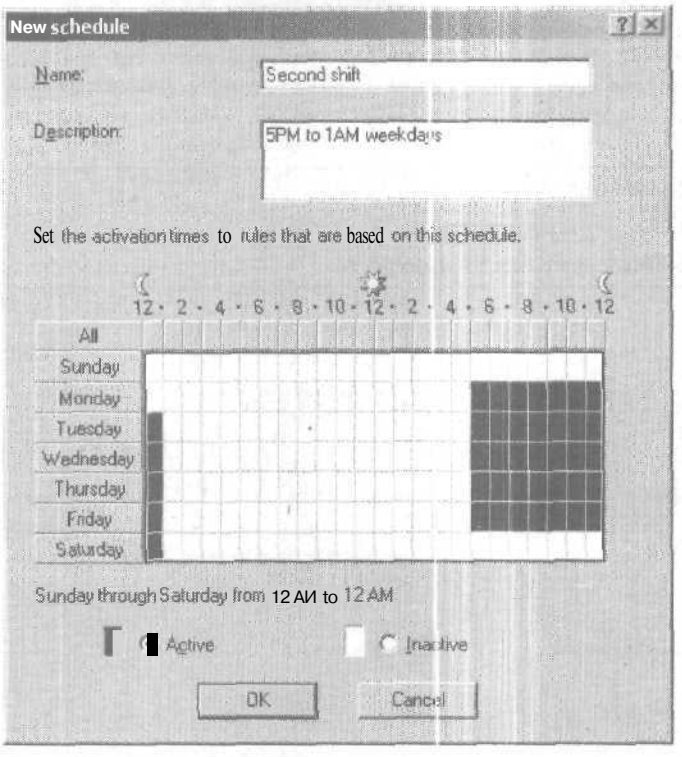


Рис. 4-4. Настройка расписания

► **Создание расписания**

1. В дереве консоли ISA Management щелкните правой кнопкой мыши узел **Schedules,** в контекстном меню последовательно выберите команды **New** и **Schedule.**
2. В поле **Name** укажите имя нового расписания,
3. *(При необходимости.)* В поле **Description** укажите описание расписания.
4. Для настройки расписания воспользуйтесь таблицей расписания:
   - щелкните ячейку таблицы, чтобы выбрать определенный час определенного дня недели;
   - щелкните кнопку дня в левом столбце, чтобы выбрать день недели целиком.
   - щелкните кнопку часа в верхнем ряду, чтобы выбрать один и тот же час для всех дней недели.
5. Щелкните переключатель **Active,** чтобы правило действовало в выбранное время, или переключатель **Inactive,** чтобы правило в выбранное время не применялось.

   В таблице расписаний темная ячейка означает, что правило активно, а светлая — что неактивно.

Настройка подмножеств адресатов

Подмножество адресатов — это одно или нескольких имен компьютеров, IP-адресов, доменных имен или диапазонов IP-адресов. В подмножествах адресатов разрешается указывать пути. Они могут состоять не только из одного или нескольких компьютеров, но и из отдельных папок на конкретных компьютерах. Существует несколько способов выбора подмножеств адресатов в правилах — ко всем компьютерам, за исключением определенных подмножеств адресатов, или только к определенному подмножеству адресатов. При определении подмножества адресатов разрешается в любом порядке указывать как доменные имена, так и IP-адреса адресатов. Для указания всех узлов выбранного домена используются знаки подстановки. Например, чтобы выбрать все компьютеры домена microsoft.com, достаточно определить адресат с адресом *.microsoft.com. Следует иметь в виду, что допускается единственный знак подстановки (*) и лишь в начале доменного имени. Пример определения подмножества адресатов показан на рис. 4-5. В подмножестве адресатов разрешается также указать путь, чтобы позволить или запретить клиентам доступ к определенным папкам. В пути разрешаются знаки подстановки.

При определении адресатов соблюдайте следующие правила. Имена компьютеров, пути и имена файлов нечувствительны к регистру. Чтобы включить в подмножество все файлы папки, достаточно указать: /<*путь*>/<*имя_папки*>/*. Чтобы выбрать в папке определенный файл, определите путь так: /<*путь*>/<*имя_папки*>/<*имя_файла*>. Правила применяются к внутренним или внешним подмножествам адресатов. Внутренние подмножества адресатов — это группы компьютеров внутри локальной сети, а внешние подмножества — компьютеры вне локальной сети.

Подмножества адресатов применяются в следующих правилах:

- правилах узлов и содержимого;
- правилах пропускной способности;
- правилах Web-публикации;
- правилах маршрутизации.

В правилах узлов и содержимого и правилах пропускной способности подмножества адресатов обычно содержат компьютеры, не относящиеся ко внутренней сети. В правилах Web-публикации подмножества адресатов обычно состоят из компьютеров внутренней сети. В правилах маршрутизации исходящих Web-запросов подмножества адресатов обычно содержат имена внешних компьютеров (расположенных в Интернете), а в правилах маршрутизации входящих Web-запросов подмножества адресатов состоят из имен внутренних компьютеров.

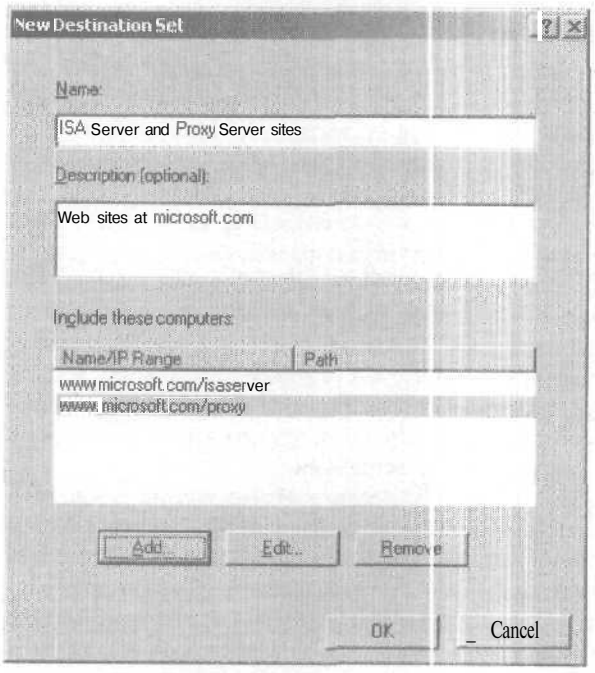


Рис. 4-5. Настройка подмножества адресатов

▶ **Настройка подмножества адресатов**

1. В дереве консоли ISA Management щелкните правой кнопкой мыши узел **Destination Sets** и в контекстном меню последовательно выберите пункты New и Set.
2. В поле **Name** укажите имя нового подмножества адресатов.
3. *(При необходимости.)* В поле **Description** введите описание подмножества адресатов.
4. Щелкните кнопку **Add**, установите переключатель в положение **Destination** (адресат) и укажите в соответствующем текстовом поле имя компьютера или его полное доменное имя.
5. *(При необходимости.)* Щелкните переключатель **IP addresses** и затем в полях **From и To (optional) укажите** соответствующие IP-адреса.
6. В поле **Path** введите путь, существующий на указанных компьютерах.

Подмножества адресов клиентов

Подмножества адресов клиентов содержат один или более компьютеров. Можно применять правила к одному или нескольким подмножествам адресов клиентов или ко всем адресам, за исключением определенных подмножеств.

Подмножества адресов клиентов указываются в следующих типах правил:

- правилах узлов и содержимого;
- правилах протоколов;
- правилах пропускной способности;
- правилах публикации серверов;
- правилах Web-публикации.

Создание подмножества адресов клиентов

1. В дереве консоли ISA Management щелкните правой кнопкой мыши узел **Client Address Sets** (подмножества адресов клиентов), в контекстном меню последовательно выберите пункты New и Set.
2. В поле **Name** введите имя подмножества.
3. *(При необходимости.)* В поле **Description** введите описание подмножества.
4. Щелкните кнопку Add.
5. В поле From введите минимальный IP-адрес, входящий в подмножество.
6. В поле To введите максимальный IP-адрес, входящий в подмножество.

Пример создания подмножества адресов клиентов показан на рис. 4-6.

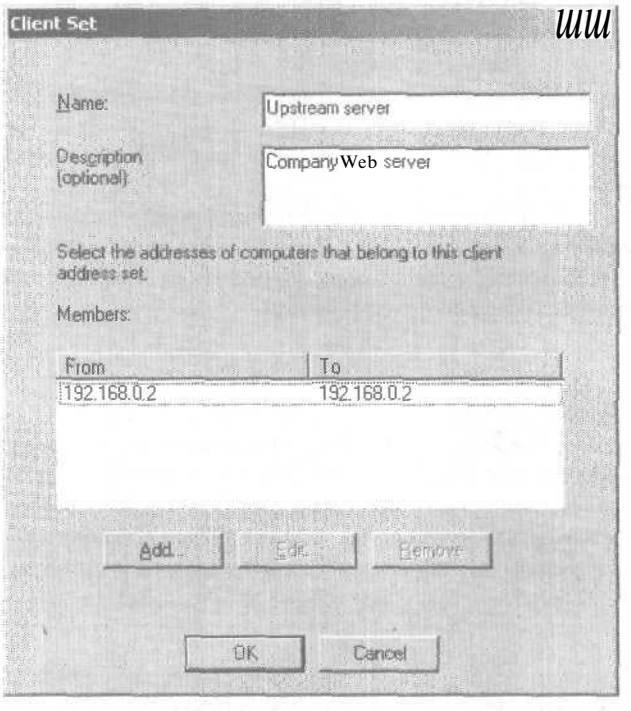


Рис. 4-6. Создание подмножества адресов клиентов, состоящего из одного компьютера

Пользователи и группы в качестве клиентов

Существующие в Microsoft Windows 2000 пользователи и группы пользователей рассматриваются как типы клиентов ISA-сервера. При создании правил обычно указывают, к каким внутренним клиентам применяется правило. Клиенты определяются либо как пользователи и группы Windows 2000, либо как подмножества IP-адресов.

При настройке правил, применяемых к клиентам SecureNAT, необходимо указывать адреса клиентов, а не имена пользователей и групп. Так как в противном случае при выполнении правила ISA-сервер не сможет распознать клиент SecureNAT и отклонит запрос. При настройке правил, применяемых к клиентам брандмауэра, разрешается определять клиентов как подмножества адресов, так и совокупности пользователей и групп. Для корректировки состава пользователей и групп Windows 2000 применяются оснастки Computer Management (Управление компьютером) и Active Directory Users and Computers (Active Directory — пользователи и компьютеры).

Настройка определений протоколов

В составе ISA-сервера поставляется большое количество предустановленных определений протоколов, которые используются при создании правил протоколов или правил публикации серверов. В правилах публикации серверов применяются определения протоколов для входящего трафика. Кроме того, определения протоколов иногда устанавливают в фильтрах приложений. Определения протоколов назначают как во время, так и после установки ISA-сервера. Кроме того, администраторы вправе расширять перечень определений протоколов, создавая собственные определения средствами оснастки ISA Management.

Пользовательские определения протоколов доступны для редактирования или удаления. Определения протоколов, устанавливаемые вместе с фильтрами приложений, нельзя изменять, но разрешается удалять, а изменение и удаление определений протоколов, поставляемых в составе ISA-сервера, невозможно. При создании определений протоколов указываются следующие параметры:

- **Port number** — порт (число от 1 до 65535), используемый в основном подключении;
- **Low-level protocol** — низкоуровневый протокол: TCP или UDP;
- **Direction** — направление; возможны значения Send, Receive, Send Receive, Receive Send для протокола UDP и Outbound и Inbound для протокола TCP;
- **Secondary connections (дополнительные** подключения, при необходимости) — диапазон номеров портов, протокол и направление, используемые для дополнительных подключений или пакетов, передаваемых после первоначального подключения. Разрешается определить одно или несколько дополнительных подключений.

Направление трафика

При создании определения протокола администратор вправе определить направление трафика. Для протокола TCP направление трафика задает направление первоначальной передачи, а для протокола UDP — направление потока данных. Допустим, вы создали правило протоколов, разрешающее внутренним клиентам инициировать передачу данных по протоколу TCP через порт 80, и указали направление Outbound. Тогда сервер, с которым взаимодействует клиент, сможет ответить на запрос клиента, но не в состоянии инициировать передачу данных.

▶ **Создание определения протокола**

1. В дереве консоли ISA Management щелкните правой кнопкой мыши узел **Protocol Definitions**, в контекстном меню последовательно выберите пункты New и **Definition.**
2. В окне мастера New Protocol Definition укажите имя определения протокола и щелкните кнопку **Next**.
3. На странице **Primary Connection Information** (рис. 4-7) укажите порт, тип протокола и направление основного подключения и щелкните кнопку Next.
4. На странице **Secondary Connections** укажите, использует ли протокол дополнительные подключения. Если да, то укажите диапазон портов, тип протокола и направление дополнительных подключений.
5. Щелкните кнопку Next, а затем кнопку **Finish,** чтобы завершить работу с мастером.

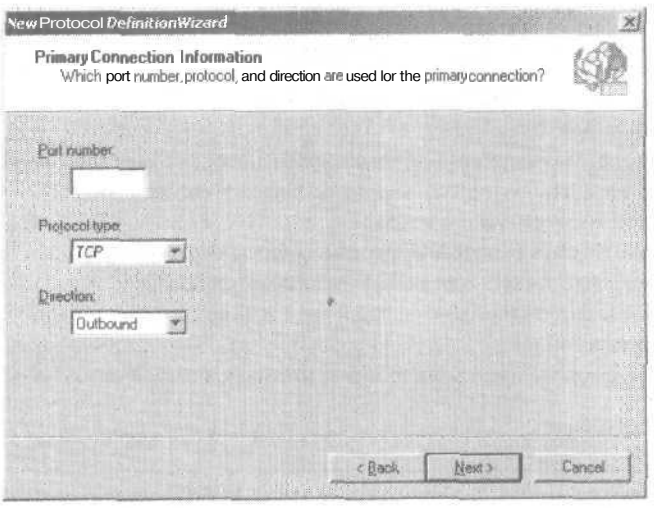


Рис. 4-7. Настройка определения протокола

Настройка групп содержимого

Группы содержимого (content groups) — это классификация информационного наполнения по типам MIME (Multipurpose Internet Mail Extensions) и расширениям имен файлов. Их применяют для ограничения доступного информационного наполнения при создании правил узлов и содержимого или правил пропускной способности. Это позволяет более четко регулировать политику безопасности, ограничив доступ не только к конкретными адресатам, но и к определенной информации.

Группы содержимого применяются только к трафику HTTP и туннелируемому трафику FTP, передаваемым через службу Web-прокси.

При запросе клиентом содержимого по протоколу FTP ISA-сервер определяет расширение файла запрашиваемого объекта, после чего проверяет наличие правил, применяемых к группам содержимого, в которых указано данное расширение файла. Если нужное правило находится, запрос обрабатывается в соответствии с правилом.

При запросе клиентом содержимого по протоколу HTTP ISA-сервер отправляет запрос на Web-сервер. При возврате объекта Web-сервером ISA-сервер определяет тип MIME объекта или расширение его файла по информации заголовка, передаваемой Web-сервером. Далее ISA-сервер проверяет наличие правил, применяемых к группам содержимого, в которые входит это расширение. Если нужное правило реализовано, запрос обрабатывается в соответствии с ним.

Группы содержимого не применяются для обработки данных, пересылаемых по безопасному протоколу HTTP (S-HTTP или HTTPS).

При создании групп содержимого рекомендуется указывать как типы MIME, так и расширения файла содержимого. Например, чтобы включить в группу содержимого все файлы приложения Director, выберите следующие расширения файлов и типы MIME:

- .dir;
- .dxr;
- .dcr;
- application/x-director.

В составе ISA-сервера поставляются следующие предустановленные группы содержимого: Application, Application Data Files, Audio, Compressed Files, Documents, HTML Documents, Images, Macro Documents, Text, Video и VRML.

► **Создание группы содержимого**

1. В дереве консоли ISA Management щелкните правой кнопкой мыши узел **Content Groups** и **в** контекстном меню последовательно выберите команды **New** и **Content Group.**
2. В поле Name укажите имя новой группы содержимого.
3. *(При необходимости.)* В поле **Description** укажите описание группы содержимого.
4. В поле со списком **Available types** выполните одну из следующих операций:
   - чтобы выбрать существующий тип содержимого, выберите в поле со списком нужное расширение файла или тип MIME;
   - чтобы добавить новый тип содержимого, укажите новое расширение файла или тип MIME.
5. Щелкните кнопку Add,

Примечание Создавая группы содержимого, указывайте как типы MIME содержимого, так и расширения файлов.

Пример группы содержимого приведен на рис. 4-8.

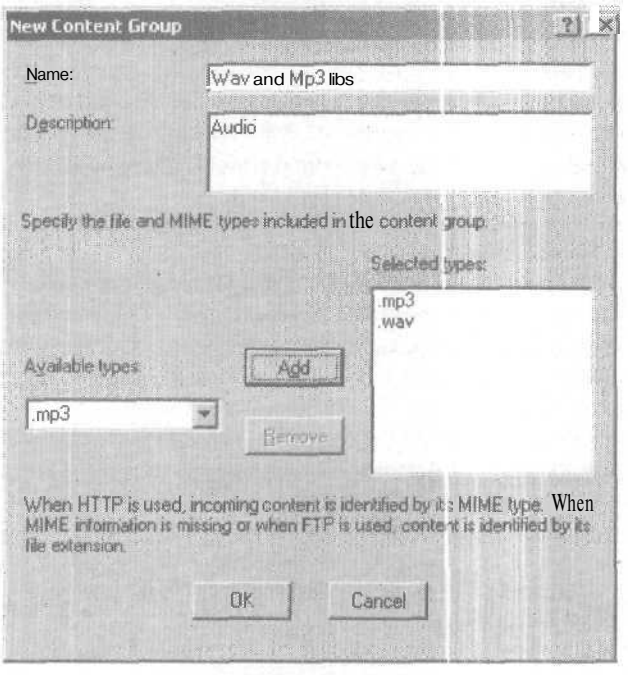


Рис. 4-8. Создание группы содержимого

Практикум. Создание элементов политики

Вы создадите два элемента политики — расширенное расписание рабочего времени и подмножество адресатов, которые в дальнейшем можно использовать при определении правил политики доступа.

Весь практикум выполняется на компьютере Server1.

Задание 1. Создание расписания

В этом задании вы создадите расширенное расписание рабочего времени Expanded Work Hours — с 6 утра до 8 вечера, по рабочим дням.

▶ **Создание расширенного расписания рабочего времени**

1. Откройте консоль ISA Management.
2. В дереве консоли последовательно раскройте узлы **Servers and Arrays,** MyArray **и Policy Elements.**
3. В узле **Policy Elements** щелкните правой кнопкой мыши его подузел **Schedules** и в контекстном меню последовательно выберите пункты New и Schedule. Откроется диалоговое окно **New Schedule.**
4. В поле **Name** введите Expanded **Work Hours.**
5. **В поле Description** выделите клетки, соответствующие времени с 6 утра-до 8 вечера с понедельника по пятницу.
6. Щелкните кнопку **Sunday,** чтобы выделить всю строку, выберите переключатель **Inactive.** Выделенная область таблицы окрасится в белый цвет.
7. Щелкните кнопку **Saturday,** чтобы выделить всю строку, а затем установите переключатель **Inactive.**
8. Выделите прямоугольную область таблицы с 12 ночи до 6 утра, с понедельника по пятницу и щелкните переключатель **Inactive.**
9. Выделите прямоугольную область таблицы с 8 вечера до 12 ночи, с понедельника по пятницу и щелкните переключатель **Inactive.**
10. Щелкните кнопку OK.
11. Щелкните узел Schedules.

    В области сведений отобразится расписание **Expanded** Work **Hours.** Обратите внимание, что в области сведений кроме нового расписания указаны предустановленные расписания **Weekends и Work hours.**

Задание 2. Создание подмножества адресатов

Вы создадите подмножество адресатов, состоящее из одного Web-узла.

▶ **Создание подмножества адресатов**

1. В дереве консоли ISA Management последовательно раскройте узлы **Servers and Arrays, MyArray и Policy Elements.**
2. В узле **Policy Elements** щелкните правой кнопкой мыши его подузел **Destination Sets** и в контекстном меню последовательно выберите пункты New и Set. Откроется диалоговое окно **New Destination Set.**
3. В поле **Name** введите **Microsoft Online Seminars** (онлайновые семинары Microsoft).
4. В поле **Description** введите ***Мультимедийный*** **практикум на microsoft.com.**
5. Щелкните кнопку Add. Откроется диалоговое окно **Add/Edit Destination.**
6. Убедитесь, что переключатель находится в положении **Destination, и в поле Destination** введите **www.microsoft.com/seminar.**

7. Щелкните кнопку OK. Вы вернетесь в диалоговое окно **New Destination Set.**
8. Щелкните кнопку OK.
9. В дереве консоли выберите узел **Destination Sets.**

   В области сведений ISA Management отобразится только что созданное подмножество адресатов **Microsoft Online Seminars.**

Резюме

Создание настраиваемых элементов политики позволяет применять правила политики к конкретным компонентам сети. К элементам политики относятся расписания, приоритеты пропускной способности, подмножества адресатов, подмножества адресов клиентов, определения протоколов, группы содержимого и записи подключений по телефонной линии. Элементы политики настраиваются в консоли ISA Management и затем используются при создании и настройке правил политики доступа, маршрутизации, публикации и пропускной способности.

Расписания создаются, когда требуется применять правила во время, не соответствующее предустановленным расписаниям ISA-сервера Work hours и Weekends. Подмножество адресатов — это одно или нескольких имен компьютеров, IP-адресов, доменных имен или диапазонов I P-адресов, Подмножества адресов клиентов служат для группировки клиентских компьютеров по IP-адресам. В определениях протоколов указываются номер порта протокола, низкоуровневый транспортный протокол, направление и параметры дополнительных подключений. В группах содержимого перечисляются типы MIME и расширения файлов.

Занятие 3. Настройка правил протоколов

Настройка правил протоколов необходима, когда нужно предоставить клиентам внутренней сети доступ в Интернет. Совместно с правилами узлов и содержимого и фильтрами IP-пакетов правила протоколов формируют политику доступа. Правила протоколов определяют, трафик каких протоколов, от каких клиентов и в какое время разрешается пропускать через ISA-сервер.

Изучив материал этого занятия, вы сможете:

- ✓ рассказать, как действуют правила протоколов;
- ✓ привести примеры предустановленных правил протоколов ISA-сервера;
- ✓ создавать и настраивать правила протоколов на ISA-сервере.

Продолжительность занятия — около 40 минут.

Правила протоколов

Правила протоколов определяют, какие протоколы разрешается использовать клиентами при доступе в Интернет. Они разрешают или запрещают использование одного или нескольких определений протоколов. Правила протоколов применяются ко всему IP-трафику или к некоторому подмножеству определений протоколов.

Для клиентов SecureNAT правила протоколов применимы ко всем компьютерам или к подмножествам компьютеров, состоящих из IP-адресов машин. Для клиентов брандмауэра правила протоколов применяются ко всем компьютерам, к подмножествам компьютеров (подмножествам их IP-адресов) или к определенным пользователям и группам Windows 2000.

▶ **Создание правила протоколов**

1. В дереве консоли ISA Management щелкните правой кнопкой мыши узел **Protocol Rules** и в контекстном меню последовательно выберите пункты **New** и **Rule**.
2. В окне мастера New Protocol Rule введите имя правила протоколов, затем щелкните кнопку **Next.**
3. На странице **Rule Action** укажите, разрешает или запрещает запрос данное правило, и щелкните кнопку Next.
4. На странице **Protocols** укажите протоколы, к которым применяется правило, и щелкните кнопку Next.
5. На странице **Schedule** укажите, когда применяется правило, и щелкните кнопку Next,
6. На странице **Client Type** укажите, к каким клиентам применяется правило, и щелкните кнопку **Next.**

Примечание Если в массиве действует политика предприятия, разрешается создавать только запрещающие правила.

Администратор может в любой момент внести изменения в ранее созданные правила. Для этого достаточно открыть в консоли ISA Management диалоговое окно свойств правила протоколов и выполнить нужные операции.

▶ **Изменение правила протоколов**

1. В дереве консоли ISA Management выберите узел **Protocol Rules.**
2. Откройте меню **View** и отметьте команду **Advanced.**

3. В области сведений щелкните правой кнопкой мыши нужное правило и в контекстном меню выберите **Properties.**
4. На вкладке **Protocol** выполните одно из следующих действий:
   - если правило предполагается применять ко всем протоколам, даже не определенным явно на ISA-сервере, выберите в поле со списком **All IP Traffic** (весь IP-трафик);
   - если требуется применить правило только к выбранным протоколам, укажите в поле со списком **Selected protocols**;
   - если требуется применить правило ко всему IP-трафику, за исключением выбранных протоколов, щелкните в поле со списком **All IP** traffic **except selected.**
5. В случае выбора **Selected protocols или All IP traffic excepted selected** отметьте *в* списке **Protocols** одно или несколько определений протоколов.

Примечание Если нужного определения протокола в списке нет, создайте его, щелкнув кнопку New.

Пример настройки правила протоколов

Предположим, требуется запретить группе пользователей применение MSN Messenger в рабочее время. Если на всех клиентских компьютерах установлен клиент брандмауэра, достаточно создать правило протоколов, реализующее эту политику, указав параметры правила следующим образом:

- на странице **Rule Action** установите переключатель в положение **Deny;**
- на странице **Protocol** выберите в поле со списком **Selected Protocols** и отметьте протокол MSN **Messenger;**
- на странице **Schedule в** поле со списком **Use this schedule** выберите расписание **Work Hours;**
- на странице **Client Type** установите переключатель в положение **Specific users and groups** (рис. 4-9);
- на странице **Users and groups** выберите нужную группу пользователей.

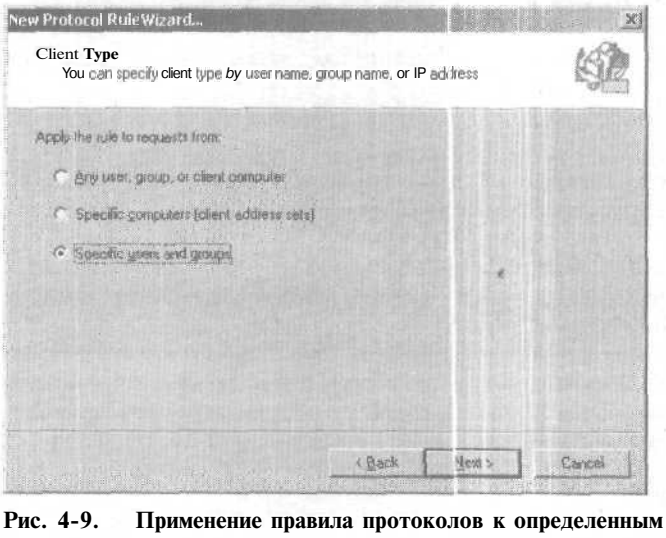


Рис. 4-9. Применение правила протоколов к определенным пользователям

Доступные протоколы

ISA-сервер поставляется с 86-ю предустановленными определениями общеизвестных протоколов, в том числе наиболее популярных протоколов Интернета. Администраторы вправе добавлять дополнительные протоколы или изменять существующие. Следует иметь в виду, что, если ISA-сервер установлен в режиме сервера кэширования, правила протоколов применяются только к протоколам HTTP, HTTPS, Gopher и FTP.

При запросе объекта клиентом по определенному протоколу ISA-сервер проверяет правила протоколов. Запрос отклоняется, если есть правило протоколов, запрещающее обмен по данному протоколу. Более того, запрос обрабатывается, только если существует правило протоколов, явно разрешающее клиенту использовать данный протокол, и существует правило узлов и содержимого, разрешающее доступ к запрашиваемому объекту. Другими словами, для разрешения доступа необходимо выполнить следующее.

1. Создать правило протоколов, указывающее, какими протоколами разрешено пользоваться для доступа к данным адресатам.
2. Создать правило узлов и содержимого, определяющее, каким клиентам разрешен доступ к данным подмножествам адресатов. При установке ISA-сервера в смешанном режиме или режиме брандмауэра по умолчанию становится активным правило, разрешающее доступ ко всем узлам и типам содержимого.

Фильтры приложений и доступность протоколов

ISA-сервер отображает информацию о 86-ти предустановленных и определенных администратором протоколах в папке Protocol Definitions узла Policy Elements. При просмотре списка определений протоколов в области сведений ISA Management видно, что одни из них определены ISA-сервером, а другие — фильтрами приложений (рис. 4-10).

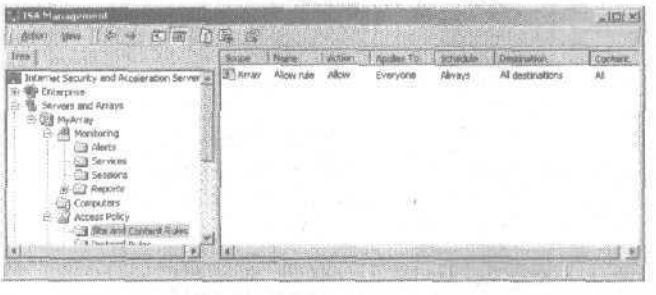


Рис. 4-10. Протоколы, определенные ISA-сервером и фильтрами приложений

Для протоколов, создаваемых и устанавливаемых фильтрами приложений, при отключении исходного фильтра приложения отключаются и все соответствующие определения протоколов, то есть трафик по таким протоколам блокируется. Например, отключение фильтров потоковых мультимедийных данных приведет к блокировке всего трафика по протоколам Windows Media и Real Networks.

Не исключено, что некоторые фильтры приложений работают с протоколами, определяемыми ISA-сервером, а не самим фильтром приложения. При отключении фильтра приложения такие определения протоколов не отключаются. Например, если отключить фильтр SMTP, пакеты SMTP все равно будут пропускаться, так как протокол SMTP определен ISA-сервером, а не фильтром SMTP.

Порядок выполнения правил

В отличие от правил маршрутизации правила протоколов не сортируются по приоритетам, но запрещающие правила приоритетнее разрешающих. Например, если создать два правила, одно из которых разрешает использование всех протоколов, а другое — запрещает использование протокола SMTP, протокол SMTP станет недоступным.

Правила протоколов уровня массива и уровня предприятия

Правила протоколов создаются как на уровне массива, так и на уровне предприятия. Когда политику массива разрешено использовать в качестве дополнения к политике предприятия, в правилах протоколов политики массива разрешается лишь налагать дополнительные ограничения на правила протоколов уровня предприятия. Другими словами, если в массиве действует политика предприятия, правила протоколов уровня массива запрещают использование протоколов (разрешить ничего нельзя).

Web-протоколы

При выборе узла Protocol Rules в дереве консоли ISA Management в области сведений, отображаемой в режиме панели заданий (Taskpad), можно создавать правила протоколов, разрешающие пользователям доступ в Интернет только по определенным Web-протоколам. Для этого нужно щелкнуть значок Create Protocol **Rule for Internet** Access. В таблице 4-1 перечислены определения этих Web-протоколов, устанавливаемые либо в составе самого ISA-сервера, либо в составе фильтров приложений, поставляемых с ISA-сервером.

Таблица 4-1. Протоколы доступа в Интернет

Имя	Номер порта	Тип протокола	Кто определяет протокол	Описание
FTP	21	TCP	Фильтр FTP access	Протокол FTP, используемый для копирования файлов между узлами
FTP Download only	21	TCP	Фильтр FTP access	Протокол FTP, используемый для копирования файлов между узлами
Gopher	70	TCP	ISA-сервер	Управляется средствами основанного на системе меню интерфейса с другими службам Интернета, в том числе Archie и WAIS (Wide Area Information Server)
HTTP	**80**	TCP	ISA-сервер	HTTP, базовый протокол Web
HTTPS	**443**	TCP	ISA-сервер	Версия HTTP, в которой для шифрования применяется протокол SSL (Secure Sockets Layer)

Определения протоколов, поставляемые в составе ISA-сервера

Определения протоколов, входящие в состав ISA-сервера, перечислены в таблице 4-2.

Таблица 4-2. Предопределенные протоколы ISA-сервера

Протокол	Описание
Any RPC Server	Поддерживает любые интерфейсы удаленного вызова процедур (Remote Procedure Calling, RPC)
AOL Instant Messenger	
Archie	
Chargen (TCP)	Протокол Character generator (генератор символов) (TCP)
Chargen (UDP)	Протокол Character generator (генератор символов) (UDP)
Daytime (TCP)	
Daytime (UDP)	
Discard (TCP)	
Discard (UDP)	
DNS Query	DNS
DNS Query Server	DNS-сервер
DNS Zone Transfer	
DNS Zone Transfer Server	
Echo (TCP)	
Echo (UDP)	
Exchange RPC Server	Поддерживает публикацию сервера Exchange для доступа по протоколу RPC из внешних сетей
Finger	
FTP	Протокол FTP
FTP Download only	FTP, только для чтения
FTP Server	FTP-сервер
Gopher	
H.323	Видеоконференции по протоколу H.323
HTTP	Протокол HTTP
HTTPS	Безопасный протокол HTTP (HTTPS)
HTTPS Server	Сервер протокола HTTPS
ICA	Citrix Intelligent Console Architecture (архитектура интеллектуальной консоли Citrix)
ICQ	Протокол программы обмена сообщениями ICQ (унаследованный)
ICQ 2000	
Ident	
IKE	Internet Key Exchange (обмен ключами через Интернет)
IMAP4	Протокол ШАР (Interactive Mail Access Protocol)

(см. след. стр.)

Таблица 4-2. *(продолжение)*

Протокол	Описание
IMAP4 Server	
IMAPS	Безопасный протокол IMAP (Secure Interactive Mail Access Protocol)
IMAPS Server	
IRC	Протокол IRC (internet Relay Chat)
Kerberos-Adm (TCP)	Администрирование Kerberos (TCP)
Kerberos-Adm (UDP)	Администрирование Kerberos (UDP)
Kerberos-IV	Аутентификация Kerberos IV
Kerberos-Sec (TCP)	Аутентификация Kerberos V (TCP)
Kerberos-Sec (UDP)	Аутентификация Kerberos V (UDP)
LDAP	Протокол LDAP (Lightweight Directory Access Protocol)
LDAP GC (Global Catalog)	
LDAPS	Безопасный протокол LDAP (Secure Light-weight Directory Access Protocol)
LDAPS GC (Global Catalog)	
Microsoft SQL Server	
MMS - Windows Media	
MMS - Windows Media Server	
MSN	Доступ к MSN через Интернет
MSN Messenger	
Net2Phone	
Net2Phone Registration	
NetBIOS Datagram	
NetBIOS Name Service	
NetBIOS Session	
NNTP	Протокол передачи новостей NNTP (Network News Transfer Protocol)
NNTP Server	
NNTPS	Безопасный протокол NNTP (Secure Network News Transfer Protocol)
NNTPS Server	Безопасный протокол NNTP — сервер
NTP (UDP)	Протокол Network Time Protocol (UDP)
PNM (Real Networks) protocol Client	Протокол передачи потоковых мультимедийных данных Real Networks Streaming Media — клиент
PNM (Real Networks) protocol Server	Протокол Real Networks Streaming Media — сервер
POP2	Протокол POP (Post Office Protocol) версии 2
POP3	Протокол POP версии 3

Таблица 4-2. *(окончание)*

Протокол	Описание
POP3 Server	
POP3S	Безопасный протокол POP версии 3
POP3S Server	
Quote (TCP)	Протокол Quote of the day (TCP)
Quote (UDP)	Протокол Quote of the day (UDP)
RADIUS	Протокол RADIUS (Remote Authentication Dial-In User Service)
RADIUS Accounting	
RDP (Terminal Services)	Протокол Remote Desktop Protocol (Terminal Services)
RIP	Протокол RIP (Routing Information Protocol)
Rlogin	Удаленный вход (Remote login)
RTSP	Протокол Real Time Streaming Protocol — клиент
RTSP Server	Протокол Real Time Streaming Protocol — сервер
SMTP	Протокол SMTP (Simple Mail Transfer Protocol)
SMTP Server	
SMTPS	Безопасный протокол SMTP (Secure Simple MailTransfer Protocol)
SMTPS Server	
SNMP	Протокол SNMP (Simple Network Management Protocol, протокол упрощенного управления сетью)
SNMP Trap	Протокол SNMP — уведомления Trap
SSH	SSH — безопасная оболочка
Telnet	
Telnet Server	
TFTP	Протокол Trivial File Transfer Protocol (тривиальный FTP)
Time (TCP)	
Time (UDP)	
Whois	Протокол Nickname/Whois

Практикум. Применение правил протоколов к учетным записям пользователей

Для выполнения этого практикума вам следует создать доменную пользовательскую учетную запись user1 и оставить для нее разрешения по умолчанию. Предполагается, что создано правило протоколов AllowIP (как описано в занятии 1 главы 3), разрешающее прохождение любого IP-трафика в любое время к любым клиентам. Убедитесь, что в Internet Explorer на компьютере Server2 корректно установлены параметры прокси.

При выполнении заданий следует учесть, что Web-сеансы по умолчанию обрабатываются анонимно, то есть в свойствах массива не предусмотрена идентификация пользователей и отсутствуют разрешающие правила, требующие аутентификацию. В таких обстоятельствах на работу пользователей, подключающихся к Интернету через Web-браузеры,

не влияют запрещающие правила, применяемые к учетным записям пользователей Windows 2000. После настройки ISA-сервера на предоставление учетной информации во всех клиентских Web-сеансах вы создадите правило протоколов, запрещающее определенному пользователю доступ в Интернет. И, наконец, вы войдете в систему под учетной записью этого пользователя, чтобы проверить правильность настройки.

Задание 1. Наблюдение за сеансами в консоли ISA Management

Вы просмотрите в консоли ISA Management информацию о сеансе, инициированном клиентом Web-прокси.

▶ **Наблюдение за Web-сеансами в консоли ISA Management**

1. На компьютере Server1 откройте окно оснастки ISA Management.
2. Откройте меню **View** и отметьте команду **Advanced.**
3. В дереве консоли раскройте узел **Monitoring** и выберите папку Sessions.
4. Если в области сведений есть какие-либо сеансы, закройте их, щелкая сеанс правой кнопкой мыши и выбирая в контекстном меню команду **Abort Session.**
5. Войдите в домен DomainOl с компьютера Server2 под учетной записью user1, запустите Internet Explorer и откройте Web-узел *http://www.msn.com.*
6. Во время загрузки Web-узла MSN вернитесь к компьютеру Serverl.
7. На компьютере Serverl в консоли ISA Management по-прежнему открыта папка **Sessions.** Щелкните правой кнопкой мыши область сведений, в контекстном меню выберите команду **Refresh.**

   Вы увидите новый Web-сеанс со следующими параметрами: имя пользователя — Anonymous, имя клиентского компьютера — не указано, IP-адрес клиента — 192.168.0.2 (адрес компьютера Server2).

   По умолчанию Web-сеансы анонимны. Когда Web-сеансы анонимны, на них не действуют запрещающие правила, определенные для отдельных пользователей. Можно назначить идентификацию пользователей при Web-сеансах, создав разрешающее правило, которое требует аутентификацию, или изменив свойства массива так, чтобы при исходящих Web-запросах проводилась идентификация пользователей.

Задание 2. Включение аутентификации при Web-сеансах

Вы запретите анонимный доступ к Web, и пользователям, подключающимся к Интернету через Web-браузеры, придется проходить аутентификацию. В результате правила политики доступа, создаваемые для определенных пользователей и групп пользователей Windows 2000, будут реализованы во всех клиентских Web-сеансах.

▶ **Включение передачи учетной информации Web-сеансами**

1. На компьютере Server1 откройте окно оснастки ISA Management и найдите в дереве консоли узел **MyArray.**
2. Щелкните правой кнопкой мыши узел **MyArray** и выберите в контекстном меню пункт **Properties.** Откроется диалоговое окно **MyArray Properties.**
3. Перейдите на вкладку **Outgoing Web Requests** (исходящие Web-запросы).
4. В области **Connections** установите флажок Ask **unauthenticated users for identification** (требовать идентификацию от пользователей, не прошедших аутентификацию).
5. Убедитесь, что установлен флажок **Resolve Requests Within Array Before Routing** (разрешать запросы внутри массива перед маршрутизацией).
6. Щелкните кнопку **OK.** Откроется диалоговое окно **ISA Server Warning.**

7. Выберите переключатель **Save the changes but don't restart the service(s)** (сохранить изменения, но не перезапускать службы) и щелкните кнопку OK.
8. Остановите и повторно запустите службы брандмауэра и Web-прокси в консоли ISA Management.
9. На компьютере Server2, в систему которого вы в предыдущем задании вошли под учетной записью user1, запустите Web-браузер и загрузите узел *http://www.msn.com*.
10. Во время загрузки Web-страницы вернитесь к компьютеру Server1, выберите в дереве консоли ISA Management папку Sessions, щелкните правой кнопкой мыши область сведений и в контекстном меню выберите **Refresh,**

    В области сведений появится новый Web-сеанс, имя пользователя которого <*имя_домена*>\user1, а адрес клиента — 192.168.0.2.

    Вы настроили передачу учетной информации через Web-браузер и вправе применять правила fSA-сервера к пользователям Windows 2000, подключающимся к Интернету через Web-браузеры.

Задание 3. Определение правила протоколов для определенного пользователя Windows 2000

Вы настроите правило ISA-сервера, запрещающее доступ в Интернет определенному пользователю Windows 2000.

▶ **Создание правила протоколов для пользователя Windows 2000**

1. На компьютере Serverl откройте консоль ISA Management, последовательно раскройте узлы MyArray, **Access Policy** и выберите узел **Protocol Rules**.
2. Щелкните правой кнопкой мыши папку **Protocol Rules** и в контекстном меню последовательно выберите пункты New и **Rule,** Откроется окно мастера **New Protocol Rule.**
3. В поле **Protocol Rule Name** введите имя правила **DenyUserl** и щелкните кнопку Next.
4. На странице **Rule Action** выберите переключатель **Deny** и щелкните кнопку Next.
5. На странице **Protocols** оставьте в поле со списком значение **All IP Traffic** и затем щелкните кнопку Next.
6. На странице **Schedule** оставьте в поле со списком значение **Always** и щелкните кнопку **Next.**
7. На странице **Client Type** установите переключатель в положение **Specific users and groups** и щелкните кнопку Next.
8. На странице **Users and Groups** щелкните кнопку **Add.** Откроется окно выбора пользователей или групп **Select Users or Groups.**
9. В верхней области выберите пользователя user1, щелкните кнопку Add, а затем — кнопку OK, чтобы вернуться на страницу **Users and Groups,** на которой в списке **Account** появится запись **DOMAIN01\user1**.
10. Щелкните кнопку Next. Откроется страница **Completing the New Protocol Rule Wizard.**
11. Щелкните кнопку **Finish,** чтобы вернуться в консоль ISA Management. В области сведений папки **Protocol Rules** появится правило **DenyUserl.**
12. В дереве консоли выберите папку **Services** узла **Monitoring** и перезапустите службы Web-прокси и брандмауэра.
13. Перейдите к компьютеру Server2, в систему которого вы вошли под учетной записью userl. Запустите Internet Explorer (если он еще не открыт), обновите окно браузера.

    Откроется диалоговое окно **Enter Network Password** (Ввод сетевого пароля). Доступ связанной с Web-сеансом учетной записи пользователя userl блокируется, так как действует правило протоколов DenyUserl. Чтобы получить доступ в Web, нужно войти

в систему под другой учетной записью Windows 2000 (не заблокированной правилами), указав ее реквизиты в диалоговом окне ввода сетевого пароля.

14. Щелкните кнопку **Cancel.**

Резюме

Создание правил протоколов позволяет разрешать или запрещать клиентским запросам проходить через ISA-сервер на уровне протокола или их подмножества. Правила протоколов совместно с правилами узлов и содержимого и фильтрами IP-пакетов определяют политику доступа на ISA-сервере.

Когда клиент запрашивает объект, находящийся за брандмауэром, ISA-сервер в первую очередь проверяет правила протоколов. Если нет правила протоколов, явно разрешающего клиенту использование данного протокола, или существует правило прогоколов, запрещающее работу по указанному протоколу, запрос блокируется.

Для удобства настройки правил протоколов в составе ISA-сервера поставляются определения наиболее широко используемых сетевых протоколов и протоколов Интернета. Кроме того, администраторы вправе создать собственные определения протоколов и использовать их в правилах протоколов.

Занятие 4. Настройка правил узлов и содержимого

Правила узлов и содержимого позволяют определить политику доступа в Интернет на уровне адресатов и типов связанного с клиентским запросом информационного наполнения. В отличие от правил протоколов, которые разрешают или блокируют передачу данных по определенным протоколам, правила узлов и содержимого разрешают или управляют доступом к подмножествам Web-узлов, а также к файлам с определенными расширениями или целым группам содержимого, например аудио или видео. Как и правила протоколов, правила узлов и содержимого применяются к любому подмножеству компьютеров, пользователей, IP-адресов и расписаний.

Изучив материал этого занятия, вы сможете:

- ✓ описать, как действуют правила узлов и содержимого ISA-сервера;
- ✓ настраивать правила узлов и содержимого.

Продолжительность занятия — около 40 минут.

Правила узлов и содержимого

Правила узлов и содержимого позволяют разрешать или запрещать доступ в Интернет в зависимости от адресата или типа запрашиваемого содержимого. Правила узлов и содержимого определяют, разрешено ли пользователям или подмножествам адресов клиентов обращаться к определенному содержимому или подмножеству адресатов, и если разрешено, то в какое время.

При запросе объекта клиентом ISA-сервер анализирует правила узлов и содержимого. Если есть правило узлов и содержимого, запрещающее запрос, доступ к объекту запрещается. Кроме того, запрос выполняется только при условии, что существует правило узлов и содержимого, разрешающее клиенту или пользователю доступ к содержимому, и правило протоколов, разрешающее клиенту или пользователю использовать данный протокол. Другими словами, для разрешения доступа в Интернет необходимо выполнить следующее.

1. Создать правило узлов и содержимого, определяющее, какие клиенты обладают доступом к данным подмножествам адресатов.
2. Создать правило протоколов, определяющее протоколы, разрешенные для доступа к данным адресатам.

Порядок выполнения правил

В отличие от правил маршрутизации, правила узлов и содержимого не упорядочиваются по приоритетам, однако запрещающие правила имеют приоритет над разрешающими. Например, если создать два правила, одно из которых разрешает доступ любым запросам, а второе — запрещает доступ пользователям подразделения продаж Sales, Интернет станет недоступным для пользователей указанного подразделения.

Разрешение и запрещение действий

Правила узлов и содержимого либо разрешают, либо запрещают доступ к определенным узлам. При запрещении доступа к объектам HTTP можно перенаправить запрос по альтернативному URL-адресу — обычно это страница внутреннего сервера с объяснением, почему доступ запрещен.

После отклонения попытки доступа ISA-сервер направляет альтернативный URL-адрес клиентскому Web-браузеру, который пытается обратиться по новому адресу.

Предположим, что правило узлов и содержимого запрещает доступ к *http://example.microsoft.com* и перенаправляет Web-запросы на адрес *http://internal.acme.com.* Когда клиент запросит Web-страницу *http://example.microsoft.com/welcome.htm* ISA-сервер заблокирует запрос и передаст браузеру адрес *http://internal.acme.com.* В результате пользователь увидит страницу *http://internal.acme.com/welcorne.htm,* а не *http://example.microsoft.com.*

Внимание! При перенаправлении запроса следует обеспечить доступность указываемого URL-адреса, то есть либо URL-адрес должен указывать на внутренний компьютер, либо необходимо наличие правила, разрешающего доступ по данному адресу.

Подмножества адресатов и обработка путей

При создании правил узлов и содержимого указываются доступные адресаты. Подмножества адресатов содержат IP-адреса определенных компьютеров или имена узлов. В любом случае разрешается включать в подмножество адресов конкретные пути.

ISA-сервер обрабатывает правила узлов и содержимого по-разному — в зависимости от типа запрашивающего объект клиента и типа запрашиваемого содержимого, Например, для определенных клиентов и протоколов ISA-сервер игнорирует указываемые в подмножестве адресатов пути. В таблице 4-3 описан порядок обработки ISA-сервером путей, указанных в подмножестве адресатов.

Таблица 4-3. Обработка путей в зависимости от типа клиентов ISA-сервера

	Клиент Web-прокси	Клиент SecureNAT	Клиент брандмауэра
FTP	Да	Нет	Нет
HTTP	Да	Да	Да
S-HTTP	Нет	Нет	Нет

Если при выполнении правила для запрошенного содержимого обработка путей не поддерживается, ISA-сервер игнорирует всех указанных в правиле адресатов с путями. Другими словами, если правило содержит несколько подмножеств адресатов, то игнорируются только те подмножества, которые не поддерживают пути, но в которых пути указаны. К остальным адресатам правило применяется, как обычно. Например, если правило запрещает доступ к *widgets.microsoft.com* и *example.microsoft.com/example,* то запрос по протоколу NNTP информации по адресу *example.microsoft.com* будет выполнен. Причина в том, что адресат содержит путь, а ISA-сервер не поддерживает обработку путей для NNTP-содержимого и поэтому не применяет к данному адресату запрещающее правило. Однако ISA-сервер проигнорирует запрос NNTP-содержимого с адреса *widgets.microsoft.com,* так как в адресате не указан путь и, следовательно, к нему применяется запрещающее правило.

Запросы по S-HTTP обрабатываются по-другому: если правило запрещает доступ к адресату, для которого указан путь, ISA-сервер запрещает доступ ко всему содержимому компьютера, а не только к тому, что расположен по указанному пути. Например, если правило запрещает доступ по протоколу S-HTTP к *example.microsqft.com/example,* ISA-сервер не разрешит доступ ко всему информационному наполнению на узле *example.microsoft.com.*

Правила узлов и содержимого уровня массива и уровня предприятия

Правила узлов и содержимого создаются как на уровне массива, так и на уровне предприятия. Когда политики массива и предприятия действуют совместно, правилам узлов и содержимого уровня массива разрешено лишь налагать дополнительные ограничения на правила узлов и содержимого уровня предприятия. На уровне массива допускается создание лишь запрещающих правил.

▶ **Создание правила узлов и содержимого**

1. В дереве консоли ISA Management щелкните правой кнопкой мыши узел **Site and Content Rules** и последовательно выберите в контекстном меню пункты New и **Rule.**
2. В мастере создания правила узлов и содержимого New **Site and Content Rule** введите имя правила и щелкните кнопку Next.
3. На странице **Rule Action** укажите тип правила — разрешающее или запрещающее — и щелкните кнопку Next.
4. На странице определения конфигурации правила Rule Configuration выберите вариант применения правила: к определенным узлам **(Deny** access **based on destination),** по расписанию **(Deny access only on certain times),** к конкретным клиентам **(Deny selected clients** access **to all external** sites) или пользовательский вариант (Custom). Щелкните кнопку **Next.**
5. На следующих страницах уточните порядок применения правила.

Примечание Если в массиве действует политика предприятия, можно создавать только запрещающие правила.

Пример правила узлов и содержимого

Чтобы запретить доступ ко всем изображениям в папке *http://example.microsofl.com/stuff,* создайте правило узлов и содержимого со следующими свойствами:

- Rule Action — Deny;
- Rule Configuration — Custom;
- в Destination Set укажите путь *example.microsoft.com/stuff/**;
- Schedule — Always;
- Client Type — Any Requests;
- Content Group — Images.

▶ **Назначение подмножества адресатов для правила узлов и содержимого**

1. В дереве консоли ISA Management щелкните узел **Site and Content Rules.**
2. Откройте меню View и отметьте команду **Advanced.**
3. В области сведений щелкните правой кнопкой мыши нужное правило и в контекстном меню выберите **Properties.**
4. На вкладке **Destinations** выберите одно из значений в поле со списком:
   - **All destinations;**
   - **All external destinations;**
   - **All internal destinations;**
   - **Selected destination set;**
   - **All destinations except selected set.**
5. В случае выбора **Selected destination set или All destinations except selected set** в поле **Name** укажите подмножество адресатов.

Группы содержимого

ISA-сервер поставляется со следующими предустановленными группами содержимого: Application, Application Data Files, Audio, Compressed Files, Documents, HTML Documents, Images, Macro Documents, Text, Video и VRML.

Правила узлов и содержимого применяют к любой из этих групп содержимого, как показано на рис. 4-11.

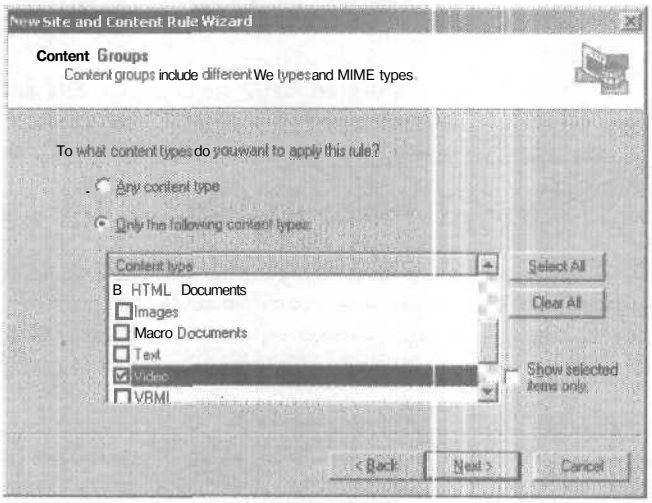


Рис. 4-11. Выбор типов содержимого для правила узлов и содержимого

На Web-серверах различные типы MIME сопоставляются с различными расширениями файлов. В таблице 4-4 показано соотношение между расширениями файлов и типами MIME, определенными по умолчанию на Web-сервере на основе IIS.

Таблица 4-4. Предустановленные типы содержимого ISA-сервера

Расширениефайла	Тип MIME
.hta	application/hta
,isp	application/x-internet-signup
.crd	application/x-mscardfile
.pmc	application/x-perfmon
.spc	application/x-pkcs7-certificates
,sv4crc	application/x-sv4crc
.bin	application/octet-stream
.clp	application/x-msclip
.mny	application/x-msmoney
.p7r	application/x-pkcs7-certreqresp
.evy	**application/envoy**
,p7s	application/pkcs7-signature
.eps	application/postscript
.setreg	application/set-registration-initiation

Таблица 4-4. *(продолжение)*

Расширение файла	Тип MIME
.xlm	application/vnd.ms-excel
.cpio	application/x-cpio
.dvi	application/x-dvi
.p7b	application/x-pkcs7-certificates
.doc	application/msword
.dot	application/msword
.p7c	application/pkcs7-mime
.ps	application/postscript
.wps	application/vnd.ms-works
.csh	application/x-csh
.iii	application/x-iphone
.pmw	application/x-perfmon
.man	application/x-troff-man
.hdf	application/x-hdf
.mvb	application/x-msmediaview
.texi	application/x-texinfo
.setpay	application/set-payment-initiation
.stl	application/vndms-pkistl
.mdb	application/x-msaccess
.oda	application/oda
.hlp	application/winhlp
.nc	application/x-netcdf
.sh	application/x-sh
.shar	application/x-shar
.tcl	application/x-tcl
.ms	application/x-troff-ms
.ods	application/oleobject
.axs	application/olescript
.da	application/vnd.ms-excel
.mpp	application/vnd.ms-project
.dir	application/x-director
.sit	application/x-stuffit
.*	application/octet-stream
.crl	application/pkix-crl
.ai	application/postscript
.xls	application/vnd.ms-excel
.wks	application/vnd.ms-works
.ins	application/x-internet-signup

(см. след. стр.)

Таблица 4-4. (*продолжение*)

Расширение файла	Тип MIME
.pub	application/x-mspublisher
.wri	application/x-mswrite
.spl	application/futu**resplash**
,hqx	application/mac-binhex40
.p10	application/pkcs10
.xlc	application/vnd.ms-excel
.xlt	**applic**ation/vnd.ms-excel
.dxr	application/x-director
.js	application/x-javascript
.m13	application/x-msmediaview
.trm	**applic**ation/x-msterminal
.pml	application/x-perfmon
.me	applic ation/x-troff-**me**
.wcm	application/vnd.ms-works
.latex	**applicat**ion/x-latex
.m14	**application/x-msmediaview**
.wmf	application/x-msmetafile
.cer	application/x-x509-ca-cert
.zip	application/x-zip-compressed
.p12	**applicat** ion/x-pkcs12
.pfx	application/x-pkcs12
.der	application/x-x509-ca-cert
.pdf	application/pdf
.xlw	application/vnd.**ms-excel**
.texinfo	application/x-texinfo
.p7m	application/pkcs7-mime
.pps	application/vnd.ms-powerpoint
.dcr	application/x-director
.gtar	application/x-gtar
.sct	text/scriptlet
.fif	**application/fractals**
.exe	application/octet-stream
.ppt	application/vnd.**ms-powerpoint**
. я	application/vndms-pkicertstore
.pko	application/vndms-pkipko
.scd	application/x-msschedule
.tar	application/x-tar
.roff	application/x-troff

Таблица 4-4. *(продолжение)*

Расширение файла	Тип MIME
.t	application/x-troff
.prf	application/pics-rules
.rtf	application/rtf
.pot	application/vnd.ms-powerpoint
.wdb	application/vnd.ms-works
.bcpio	application/x-bcpio
.dll	application/x-msdownload
.pma	application/x-perfmon
.pmr	application/x-perfmon
.tr	application/x-troff
.src	application/x-wais-source
.acx	application/internet-property-stream
.cat	application/vndms-pkiseccat
.cdf	application/x-cdf
.tgz	application/x-compressed
.sv4cpio	application/x-sv4cpio
.tex	application/x-tex
.ustar	application/x-ustar
.crt	application/x-x509-ca-cert
.ra	audio/x-pn-realaudio
.mid	audio/mid
.au	audio/basic
.snd	audio/basic
.wav	audio/wav
.aifc	audio/aiff
.m3u	audio/x-mpegurl
.ram	audio/x-pn-realaudio
.aiff	audio/aiff
.rmi	audio/mid
.aif	audio/x-aiff
.mp3	audio/mpeg
.gz	application/x-gzip
.z	application/x-compress
.tsv	text/tab-separated-values
.xml	text/xml
.323	text/h323
.htt	text/webviewhtml
.stm	text/html

(см. след. стр.)

Таблица 4-4. (*окончание*)

Расширение файла	Тип MIME
.html	text/html
.xsl	text/xml
.htm	text/html
.cod	image/cis-cod
.ief	image/ief
.pbm	image/x-portable-bitmap
.tiff	image/tiff
.ppm	image/x-portable-pixmap
.rgb	image/x-rgb
.dib	image/bmp
.jpeg	image/jpeg
.cmx	image/x-cmx
.pnm	image/x-portable-anymap
.jpe	image/jpeg
.jfif	image/pjpeg
.tif	image/tiff
.jpg	image/jpeg
.xbm	image/x-xbitmap
.ras	image/x-cmu-raster
.gif	image/gif

Практикум. Создание правила узлов и содержимого

Вы создадите правило узлов и содержимого, блокирующее доступ определенного пользователя ко всем аудио- и видеоданным. Затем вы войдете в систему под двумя разными учетными записями, чтобы проверить правильность настройки правила.

Предполагается, что создана доменная учетная запись пользователя с именем user1 в соответствии с инструкциями занятия 3 этой главы и что ей оставлены разрешения и привилегии по умолчанию. Кроме того, необходимо создать доменную учетную запись пользователя user2 с привилегиями по умолчанию. Предполагается, что существует правило протоколов, разрешающее прохождение любого IP-трафика по любым запросам в любое время, — оно было создано на занятии 1 главы 3. И, наконец, предполагается, что при исходящих Web-запросах требуется идентификация пользователей (в соответствии с инструкциями занятия 3 этой главы). Проверьте правильность настройки прокси в браузере Internet Explorer для всех пользователей компьютера Server2.

Если вы определили правило протоколов DenyUser1 в соответствии с инструкциями занятия 3 этой **главы,** то перед выполнением заданий отключите это правило и перезапустите ISA-сервер.

Задание 1. Запрещение доступа к аудио- и видеоинформации пользователю user1

Данное задание выполняется на компьютере Server1. Вы создадите правило узлов и содержимого, запрещающее пользователю user1 доступ к любому аудио- и видеосодержимому.

▶ **Запрещение пользователю userl доступа к аудио и видео**

1. Войдите в систему сервера Serverl под учетной записью Administrator (Администратор).
2. Откройте консоль ISA Management.
3. Раскройте узел **Access Policy.** Щелкните правой кнопкой мыши папку **Site and Content Rules** и в контекстном меню последовательно выберите команды New **и Rule.** Откроется окно мастера New Site And Content Rule.
4. В поле **Site and content rule name** укажите имя правила — **Deny User1AudioVideo** и щелкните кнопку Next.
5. На странице **Rule Action** оставьте переключатель в положении **Deny** и щелкните кнопку **Next.**
6. На странице **Rule Configuration** установите переключатель в положение **Custom** и щелкните кнопку Next.
7. На странице **Destination** Sets (подмножества адресатов) оставьте в поле со списком значение **All Destinations** (все адресаты) и щелкните Next.
8. На странице **Schedule** оставьте в поле со списком значение **Always** (всегда) и щелкните кнопку Next.
9. На странице **Client Type** установите переключатель в положение **Specific users and groups** (определенные пользователи и группы) и щелкните **Next.**
10. На странице **Users And Groups** щелкните кнопку Add. Откроется окно выбора пользователей или групп **Select Users Or Groups.**
11. В верхней области выберите пользователя userl и шелкните кнопку Add.
12. Щелкните кнопку OK, чтобы вернуться на страницу Users **and Groups.**
13. Убедитесь, что в списке **Accounts** появился **Domain01\user1**, и щелкните кнопку Next.
14. На странице выбора групп содержимого **Content Groups** установите переключатель в положение **Only the following content types.**
15. В поле **Content Type** отметьте флажками элементы **Audio и Video.** Таким образом, вы запретите пользователю userl доступ к аудио- и видеоданным в любое время.
16. Щелкните кнопку **Next.** Откроется страница **Completing the New Site and Content Rule Wizard.**
17. Щелкните кнопку **Finish.** В области сведений папки **Site and Content Rules** появится правило **DenyUser1AudioVideo.** Обратите внимание, что в области сведений также присутствует предустановленное правило **Allow Rule.**

Перед выполнением задания 2 остановите и снова перезапустите средствами консоли ISA Management службы Web-прокси и брандмауэра.

Задание 2. Проверка конфигурации

Вы войдете в систему сервера Server2 под учетной записью user2 и попытаетесь получить доступ к аудиоданным. Затем вы войдете в систему сервера Server2 под учетной записью userl и снова попытаетесь получить доступ к аудиоданным, чтобы увидеть изменения в поведении системы.

▶ **Проверка нового правила узлов и содержимого**

1. Войдите в домен DomainOl с компьютера Server2 под учетной записью user2.
2. Запустите Internet Explorer.

3. В поле **Address** (Адрес) введите **http://www.microsoft.com/seminar.** Откроется страница онлайновых семинаров Microsoft Seminar Online.
4. Щелкните любую из гиперссылок онлайнового семинара. Откроется Web-страница, содержащая звуковые элементы.
5. После завершения загрузки Web-страницы щелкните кнопку со стрелкой для воспроизведения звука. Начнется трансляция лекции.
6. Щелкните в Internet Explorer значок **Stop,** чтобы остановить воспроизведение.
7. Закройте Internet Explorer.
8. На компьютере Server2 завершите работу в домене DomainOl под учетной записью user2 и войдите под учетной записью user1.
9. Повторите операции 1–4.

   Когда загрузка страницы семинара завершится, вы обнаружите, что звуковое содержимое невозможно воспроизвести. Таким образом, доступ пользователя user1 к аудиоданным успешно заблокирован.

Резюме

Правила узлов и содержимого позволяют разрешать или запрещать доступ в Интернет в зависимости от адресата или типа запрашиваемого содержимого. Как и для правил протоколов, ISA-сервер пропускает пакеты только при условии, что существует правило узлов и содержимого, разрешающее клиенту доступ к запрашиваемому типу содержимого и адресату. Правила узлов и содержимого либо разрешают, либо запрещают доступ к определенным узлам и типам содержимого.

При создании правил узлов и содержимого указываются доступные адресаты. Подмножества адресатов обычно состоят из IP-адресов компьютеров, имен компьютеров, путей или Web-адресов.

ISA-сервер поставляется с рядом предустановленных групп содержимого — Application, Application Data Files, Audio, Compressed Files, Documents, HTML Documents, Images, Macro Documents, Text, Video и **VRML.** Эти группы в свою очередь содержат более 100 расширений файлов и типов MIME, каждые разрешается использовать в правилах узлов и содержимого.

Занятие 5. Настройка фильтров IP-пакетов

Фильтры IP-пакетов разрешают или блокируют прохождение пакетов через определенные порты. В простых сетях для обеспечения безопасного доступа клиентских компьютеров в Интернет не обязательно создавать фильтры IP-пакетов, в более сложных средах они нужны для разрешения или блокировки прохождения определенного трафика с внешнего сетевого интерфейса сервера на внутренний интерфейс.

Изучив материал этого занятия, вы сможете:

- ✓ описать по крайней мере три ситуации, когда необходимы фильтры IP-пакетов;
- ✓ создавать и настраивать фильтры IP-пакетов;
- ✓ рассказать, какие параметры фильтрации пакетов следует определять.

Продолжительность занятия — около 45 минут.

Условия, когда необходимо применять фильтры IP-пакетов

Фильтры IP-пакетов открывают и закрывают порты статически, то есть порт остается открытым или закрытым в течение всего периода действия фильтра. Однако в большинстве случаев предпочтительно открывать и закрывать порты динамически, по мере необходимости. Динамическое открытие портов конфигурируется при помощи правил протоколов и правил узлов и содержимого. Поэтому правила политики доступа рекомендуется применять для разрешения внутренним клиентам доступа в Интернет, а правила публикации — для разрешения внешним клиентам доступа к внутренним серверам. Предположим, требуется разрешить всем внутренним пользователям доступ к узлам по протоколу HTTP. В этом случае следует создавать не фильтр IP-пакетов, открывающий порт 80, а разрешающие такой доступ правила — узлов и содержимого, а также протоколов.

Однако в некоторых ситуациях без использования фильтров IP-пакетов не обойтись. Далее перечислены случаи, когда применение фильтров IP-пакетов обязательно:

- публикация серверов, расположенных в *сети периметра* (perimeter network), также называемой *демилитаризованной зоной* (demilitarized zone, DMZ) или *экранированной подсетью* (screened subnet);
- наличие приложений или других служб ISA-сервера, которым требуется доступ в Интернет;
- обеспечение доступа по протоколам, не основанным на UDP или TCP.

Создание фильтров IP-пакетов

Фильтры перехватывают пакеты, адресованные определенным компьютерам корпоративной сети, и пропускают или блокируют их. Таким образом, возможны два типа статических фильтров IP-пакетов: *разрешающие* (allow filter) и *блокирующие* (block filter).

Разрешающие фильтры работают по принципу исключения — блокируются все типы пакетов, за исключением указанных. Если для порта не определен активный фильтр пакетов, службе не удастся прослушивать такой порт, пока тот не откроется динамически. Блокирующие фильтры закрывают указанные в них порты. Блокирующие фильтры создают для более точного определения трафика, которому разрешено проходить через ISA-сервер.

Разрешающие и блокирующие фильтры обычно применяются совместно. Например, создается фильтр, разрешающий трафик TCP по порту 25 между внутренними и внешними узлами (рис. 4-12), то есть передачу данных по протоколу SMTP. А затем доступ огра-

ничивается блокирующим фильтром, запрещающим определенному диапазону внешних IP-адресов (потенциальным злоумышленникам) отправлять на ISA-сервер TCP-пакеты на порт 25.

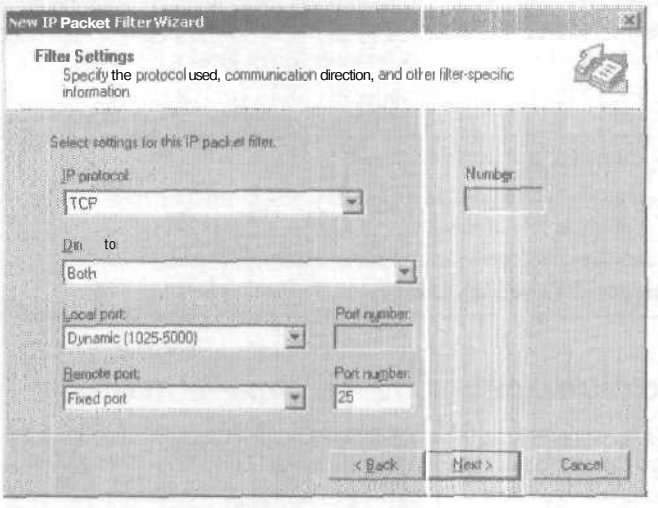


Рис. 4-12. Создание фильтра IP-пакетов, разрешающего передачу данных по протоколу SMTP

При создании фильтров IP-пакетов указываются следующие параметры:

- **серверы** — серверы, с которыми запрещен или разрешен обмен данными;
- **протокол, порт, направление** — фильтр разрешает или блокирует трафик через конкретный порт и протокол в определенном направлении;
- **локальный узел** — имя компьютера внутренней сети, для которого разрешается или блокируется передача данных. Можно указать рад IP-адресов или один IP-адрес;
- **удаленный узел** — имя компьютера в Интернете, которому разрешена или запрещена передача данных.

Примечание Перед созданием фильтров IP-пакетов необходимо включить фильтрацию IP-пакетов. По умолчанию при установке ISA-сервера фильтрация IP-пакетов включается автоматически. Это же можно сделать вручную в диалоговом окне **IP Packet Filters Properties.**

▶ **Создание фильтра IP-пакетов**

1. В консоли ISA Management щелкните правой кнопкой мыши узел **IP Packet Filters** и в контекстном меню последовательно выберите пункты **New** и **Filter.**
2. В окне мастера New IP Packet Filter введите имя нового фильтра и щелкните кнопку **Next.**
3. На странице **Servers** укажите, нужно ли применять фильтр IP-пакетов ко всему массиву ISA-серверов или только к одному из серверов.
4. На странице **Filter Mode** укажите, разрешает или блокирует фильтр прохождение пакетов.
5. На странице **Filter Type** выберите предустановленный фильтр или переместите переключатель в положение **Custom,** чтобы создать новый тип фильтра.
6. В случае выбора **Custom** на странице **Filter Settings** укажите IP-протокол **(IP protocol),** направление **(Direction),** локальный **(Local port)** и удаленный **(Remote port)** порты фильтра IP-пакетов.

7. На странице **Local Computer** укажите компьютер локальной сети, к которому будет применяться фильтр IP-пакетов.
8. На странице **Remote Computers** укажите удаленные компьютеры, к которым будет применяться фильтр IP-пакетов.

Примечание Чтобы внесенные изменения вступили в силу после создания фильтра или изменения конфигурации фильтра IP-пакетов, необходимо перезапустить службы ISA-сервера.

▶ Настройка протокола для фильтра IP-пакетов

1. Откройте меню Mew и отметьте команду **Advanced.**
2. В дереве консоли ISA Management щелкните папку **IP Packet Filters.**
3. В области сведений щелкните правой кнопкой мыши фильтр IP-пакетов, который требуется изменить, и в контекстном меню выберите команду **Properties.**
4. Перейдите на вкладку **Filter Type.**
5. Выполните одно из следующих действий;
   - установите переключатель в положение **Predefined** и выберите фильтр из списка;
   - установите переключатель в положение **Custom и в** поле со списком **IP protocol** выберите одно из значений: **Any, ICMP, TCP, UDP или Custom protocol.**
6. Если выбран переключатель **Custom** и протокол **ICMP,** выполните следующие действия:
   - в поле со списком **Direction** укажите одно из значений: **Inbound, Outbound или Both;**
   - в поле со списком **Type** выберите одно из значений:**All types или Fixed Type.** Если вы выбрали **Fixed type,** введите **type number в** поле **Number;**
   - в поле со списком **Code** щелкните **All Codes или Fixed Code.** Если вы указали **Fixed Code,** введите **code number** в поле **Number.**
7. Если выбраны переключатель **Custom** и элемент Any, в списке **IP Protocol** укажите направление: **Inbound, Outbound или Both.**
8. Если выбран переключатель **Custom** и протокол UDP, выполните следующие действия:
   - в поле со списком **Direction** щелкните **Receive only, Sendonly, Both, Receive send или Send receive;**
   - в поле со списком **Local Port** укажите **All ports, Fixedport или Dynamic.** Если выбран **Fixed port,** укажите номер порта в поле **Port number;**
   - в поле со списком **Remoteport** щелкните **All ports или Fixedport.** Если выбран **Fixed port,** введите порт в поле **Port number.**
9. Если выбран **Custom** и протокол TCP, выполните следующие действия:
   - в поле со списком **Direction** щелкните **Inbound, Outbound или Both;**
   - в поле со списком **Local port** укажите **Allports, Fixed port или Dynamic.** Если выбран **Fixed port,** введите номер порта в поле **Port Number;**
   - в поле со списком **Remote Port** выберите **All Ports или Fixed Port.** Если выбран **Fixed port,** укажите номер порта в поле **Port number.**

▶ Применение фильтра IP-пакетов к серверу

1. Откройте меню View и отметьте команду **Advanced.**
2. В дереве консоли ISA Management щелкните узел **IP Packet Filters.**
3. В области сведений щелкните правой кнопкой мыши фильтр IP-пакетов, который требуется изменить, и в контекстном меню выберите команду **Properties.**
4. На вкладке **General в** разделе **Servers that use this filter** (серверы, использующие этот фильтр) выполните одно из следующих действий:

- установите переключатель в положение **All servers in the array** (все серверы массива);
- установите переключатель в положение **Only this server** (только этот сервер) и затем выберите сервер, к которому будет применяться фильтр.

► **Настройка фильтра IP-пакетов для локального компьютера.**

1. Откройте меню **View** и отметьте команду **Advanced.**
2. В дереве консоли ISA Management щелкните узел **IP Packet Filters.**
3. В области сведений щелкните фильтр IP-пакетов, который требуется изменить, правой кнопкой мыши и в контекстном меню выберите команду **Properties.**
4. На вкладке **Local Computer** выполните следующие действия:
   - чтобы указать, что фильтр IP-пакетов применяется к IP-адресу по умолчанию каждого из внешних интерфейсов локального ISA-сервера, установите переключатель в положение **Default IP address(es) on the external interface(s);**
   - чтобы указать, что фильтр IP-пакетов применяется к определенному IP-адресу локального ISA-сервера, установите переключатель в положение **This ISA server's external IP address;**
   - чтобы выбрать определенный компьютер в сети периметра, установите переключатель в положение This computer (on the **perimeter network) и** введите IP-адрес, не принадлежащий ISA-серверу;
   - чтобы выбрать ряд IP-адресов в сети периметра, установите переключатель в положение These **computers (on the perimeter network)** и в полях **Subnet и Mask** укажите соответствующую информацию.

► **Настройка фильтра IP-пакетов для удаленного компьютера**

1. Откройте меню View и отметьте команду **Advanced.**
2. В дереве консоли ISA Management щелкните узел **IP Packet Filters.**
3. В области сведений щелкните правой кнопкой мыши фильтр IP-пакетов, который требуется изменить, и в контекстном меню выберите команду **Properties.**
4. На вкладке **Remote Computer** укажите компьютер, к которому применяется фильтр IP-пакетов, выполнив одно из следующих действий:
   - если фильтр применяется ковсем внешним компьютерам, установите переключатель в положение **All remote computers;**
   - если фильтр применяется кодному компьютеру, установите переключатель в положение **This remote computer** и укажите IP-адрес внешнего компьютера, к которому применяется фильтр;
   - если фильтр применяется к ряду компьютеров, щелкните переключатель **This range of computers** и введите соответствующую информацию в полях **Subnet и Mask.**

Настройка параметров фильтров пакетов

Вы можете настроить параметры фильтрации пакетов. Щелкните правой кнопкой мыши папку **IP Packet Filters** в консоли ISA Management, выберите в контекстном меню команду **Properties** и перейдите на вкладку **Packet** Filters (рис. 4-13), чтобы настроить следующие параметры:

- фильтрацию IP-фрагментов;
- фильтрацию параметров протокола IP;
- ведение журнала пакетов для разрешающих фильтров.

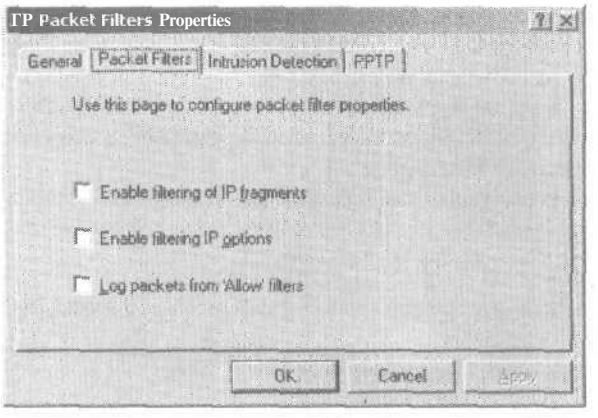


Рис. 4-13. Вкладка Packet Filters диалогового окна свойств IP Packet Filters

Фильтрация IP-фрагментов

При включении флажка **Enable filtering of IP fragments** служба Web-прокси и служба брандмауэра выполняют фильтрацию IP-фрагментов. При включенной фильтрации IP-фрагментов все фрагментированные IP-пакеты блокируются. Известно, что некоторые виды атак со стороны злоумышленников основаны на том, что отправленные в сеть фрагментированные пакеты собираются и причиняют вред системе.

Не включайте фильтрацию IP-фрагментов, если нужно, чтобы через ISA-сервер проходили потоки аудио- или видеоданных.

▶ **Включение фильтрации IP-фрагментов**

1. В дереве консоли ISA Management шелкните правой кнопкой мыши узел **IP Packet Filters** и в контекстном меню выберите команду **Properties.**
2. На вкладке **General** установите флажок **Enable packet filtering,** если он еще не включен.
3. На вкладке **Packet Filters** установите флажок **Enable filtering of IP fragments.**

Фильтрация параметров протокола IP

При включении фильтрации параметров протокола IP ISA-сервер блокирует все пакеты, содержащие слова «IP options» в заголовке.

▶ **Включение фильтрации параметров протокола IP**

1. В дереве консоли ISA Management щелкните правой кнопкой мыши узел **IP Packet Filters** и в контекстном меню выберите **Properties.**
2. На вкладке **General** установите флажок **Enable packet filtering,** если он еще не включен.
3. На вкладке **Packet Filters** включите флажок **Enable filtering IP options.**

Ведение журналов пакетов

Все пакеты, проходящие через ISA-сервер, можно регистрировать в журнале фильтра пакетов. Порядок и принципы регистрации описаны далее:

- по умолчанию после установки ISA-сервера все заблокированные пакеты учитываются в журнале фильтра пакетов. Если отключить фильтрацию пакетов, то прекращается и ведение журнала;

- можно отключить ведение журнала пакетов, не пропущенных всеми блокирующими фильтрами IP-пакетов, выполни» соответствующую настройку в диалоговом окне свойств этого фильтра IP-пакетов:
- иногда ISA-сервер настраивают для ведения журнала всех пропущенных и заблокированных пакетов. Если включено ведение журнала разрешенных пакетов, в журнале учитываются все пакеты, поступающие на ISA-сервер.

Ведение журнала разрешенных и заблокированных пакетов существенно нагружает сервер.

▶ **Включение учета разрешенных пакетов**

1. В дереве консоли ISA Management щелкните правой кнопкой мыши узел **IP Packet Filters** и в контекстном меню выберите **Properties.**
2. На вкладке **Packet Filters** установите флажок **Log packets from 'Allow' filters.**

Практикум. Запуск служб Интернета на ISA-сервере

Если ISA-сервер должен обслуживать доступ к почте, новостям и Web, нужно создать пять фильтров IP-пакетов, разрешающих доступ к портам, используемым службами POP3 (входящая почта), SMTP (исходящая почта), NNTP (новости), DNS (запросы к Web) и HTTP (содержимое Web). Вообще, рекомендуется избегать статического открытия портов путем создания фильтров IP-пакетов на брандмауэре. Чтобы снизить риск, обусловленный статическим открытием портов, создают блокирующие фильтры, запрещающие доступ ко всем IP-адресам, за исключением тех, к которым требуется доступ (например за исключением адресов серверов POP3, SMTP и NNTP). Кроме того, имеется возможность вручную включать и выключать фильтры IP-пакетов, чтобы при необходимости ограничивать использование открытых портов. Не забывайте перезапускать службы ISA-сервера после включения или выключения фильтров IP-пакетов.

Дальнейшие пять заданий следует выполнять на компьютере Server1.

Примечание Если ISA-сервер подключен к Интернету по выделенной линии через сетевой адаптер (а не по телефонной линии через модем), не нужно создавать фильтры IP-пакетов для обеспечения доступа ISA-сервера к Web. Необходимо только настроить Web-браузер на использование IP-адреса внутреннего сетевого адаптера сервера в качестве адреса прокси-сервера. Для использования отличных от Web служб Интернета, таких как почта и новости, по-прежнему потребуется создать фильтры IP-пакетов.

Задание 1. Создание фильтра IP-пакетов для входящей почты (POP3)

Сейчас вы создадите фильтр пакетов, разрешающий прохождение TCP-трафика через порт 110, что позволит ISA-серверу принимать почту по протоколу POP3.

▶ **Создание фильтра IP-пакетов, разрешающего работу по протоколу POP3**

1. Откройте консоль ISA Management.
2. Последовательно раскройте узлы Servers **and Arrays,** MyArray, Access **Policy,** найдите папку **IP Packet Filters.**
3. Щелкните правой кнопкой мыши папку **IP Packet Filters** и в контекстном меню последовательно выберите команды New и **Filter.** Откроется окно мастера New IP Packet Filter.
4. В поле **IP Packet Filter Name** укажите имя нового фильтра **POP3 Filter** и щелкните кнопку **Next.**

5. На странице **Servers** оставьте переключатель в положении **All ISA server computers in the array** (все ISA-серверы массива) и щелкните кнопку Next.
6. На странице **Filter Mode** оставьте переключатель в положении **Allow packet transmission** (разрешить передачу пакетов) и щелкните кнопку **Next.**
7. На странице **Filter Type** установите переключатель в положение **Custom** и щелкните кнопку Next. Откроется страница **Filter Settings.**
8. В поле со списком **IP Protocol** выберите TCP.
9. В поле со списком **Local port** выберите **Dynamic.**
10. В поле со списком **Remote port** выберите **Fixed port** и в поле **Port number** справа от поля со списком **Remote port** введите 110. Щелкните кнопку Next.
11. На странице **Local Computer** оставьте переключатель в положении **Default IP Address(es) for each internal interface on the ISA server computer.**
12. На странице **Remote Computers** оставьте переключатель в положении **All Remote Computers** и щелкните кнопку Next. Откроется страница **Completing the New IP Packet Filter Wizard.**
13. Щелкните кнопку **Finish.**

    В списке фильтров IP-пакетов появится фильтр **POP3 Filter.**

Задание 2. Создание фильтра IP-пакетов для исходящей почты (SMTP)

Вы создадите фильтр I P-пакетов, разрешающий прохождение TCP-трафика через порт 25, что позволит ISA-серверу отправлять почту по протоколу SMTP.

► **Создание фильтра IP-пакетов, разрешающего работу по протоколу SMTP**

1. В консоли ISA Management последовательно раскройте узлы Servers **and Arrays,** MyArray, Access **Policy,** найдите папку **IP Packet Filters.**
2. Щелкните правой кнопкой мыши папку **IP Packet Filters** и в контекстном меню последовательно выберите пункты New и **Filter.** Откроется окно мастера New IP Packet Filter.
3. В поле **IP Packet Filter Name** введите название нового фильтра **SMTP Filter** и щелкните кнопку Next.
4. На странице **Servers** оставьте переключатель в положении **All ISA Server Computers In The Array** и щелкните кнопку Next.
5. На странице **Filter Mode** оставьте переключатель в положении **Allow packet transmission** (разрешить передачу пакетов) и щелкните кнопку Next.
6. На странице **Filter Type** установите переключатель в положение **Custom** и щелкните кнопку Next. Откроется страница **Filter Settings.**
7. В поле со списком **IP protocol** выберите TCP.
8. В поле со списком **Local port** выберите **Dynamic.**
9. В поле со списком **Remote port** выберите **Fixed port и в** поле **Port number** справа от поля со списком **Remote port** введите 25. Щелкните кнопку Next.
10. На странице **Local Computer** оставьте переключатель в положении **Default IP Address(es) for each internal interface on the ISA server computer.** Щелкните кнопку Next.
11. На странице **Remote Computers** оставьте переключатель в положении All **Remote Computers** и щелкните кнопку Next. Откроется страница **Completing the New IP Packet Filter Wizard.**
12. Щелкните кнопку **Finish.**

    В списке фильтров IP-пакетов консоли ISA Management появится фильтр **SMTP Filter.**

Задание 3. Создание фильтра IP-пакетов для протокола NNTP

Вы создадите фильтр пакетов, разрешающий прохождение трафика TCP через порт 119, что позволит ISA-серверу подключаться к серверам NNTP, отправлять и получать сообщения NNTP.

► **Создание фильтра IP-пакетов, разрешающего** NNTP

1. В консоли ISA Management последовательно раскройте узлы **Servers and Arrays, MyArray, Access Policy**, найдите папку **IP Packet Filters.**
2. Щелкните правой кнопкой мыши папку **IP Packet Filters** и в контекстном меню последовательно выберите команды **New** и **Filter**. Откроется окно мастера New IP Packet Filter.
3. В поле **IP Packet Filter Name** укажите имя нового фильтра **NNTP Filter** и щелкните кнопку Next.
4. На странице **Servers** оставьте переключатель в положении **All ISA server computers in the array** (все ISA-серверы массива) и щелкните кнопку Next
5. На странице **Filter Mode** оставьте переключатель в положении **Allow packet transmission** (разрешить передачу пакетов) и щелкните кнопку Next,
6. На странице **Filter Type** установите переключатель в положение **Custom** и щелкните кнопку **Next.** Откроется страница **Filter Settings.**
7. В поле со списком **IP Protocol** выберите TCP.
8. В поле со списком **Local Port** выберите **Dynamic,**
9. В поле со списком **Remote port** выберите **Fixed port** и в поле **Port number** справа от поля со списком **Remote port** введите 119. Щелкните кнопку Next.
10. На странице **Local Computer** оставьте переключатель в положении **Default IP Address(es) for each internal interface on the ISA server computer** и щелкните кнопку **Next.**
11. На странице **Remote Computers** оставьте переключатель в положении **All Remote Computers и** щелкните кнопку Next. Откроется страница **Completing the New IP** Packet **Filter Wizard.**
12. Щелкните кнопку **Finish.**

В списке фильтров IP-пакетов консоли ISA Management появится фильтр **NNTP Filter.**

Задание 4. Создание фильтра IP-пакетов, разрешающего исходящие Web-запросы (DNS-запросы)

Вы создадите фильтр пакетов, разрешающий прохождение трафика UDP через порг 53, что позволит ISA-серверу выполнять DNS- запросы.

► **Создание фильтра IP-пакетов, разрешающего DNS-запросы**

1. Откройте консоль ISA Management.
2. Последовательно раскройте узлы **Servers and Arrays, MyArray,** Access **Policy,** найдите папку **IP Packet Filters.**
3. Щелкните правой кнопкой мыши папку **IP Packet Filters** и в контекстном меню последовательно выберите команды **New** и Filter. Откроется окно мастера New IP Packet Filter.
4. В поле **IP Packet Filter** Name укажите имя нового фильтра **DNS Query и** щелкните кнопку Next.
5. На странице **Servers** оставьте переключатель в положении **All ISA server computers in the array** (все ISA-серверы массива) и щелкните кнопку Next.
6. На странице **Filter Type** установите переключатель в положение **Custom** и щелкните кнопку Next. Откроется страница **Filter Settings.**
7. На странице **Filter Type** установите переключатель в положение **Custom** и щелкните кнопку Next. Откроется страница **Filter Settings.**

8. В поле со списком **IP Protocol** выберите UDP.
9. В поле со списком **Local Port** выберите **Dynamic.**
10. В поле со списком **Remote** port выберите **Fixed port** и в поле **Port number** справа от поля со списком **Remote port** введите 53. Щелкните кнопку **Next.**
11. На странице **Local Computer** оставьте переключатель в положении **Default IP Address(es) for each internal interface on the ISA server computer.**
12. На странице **Remote Computers** оставьте переключатель в положении **All Remote Computers** и щелкните кнопку **Next.** Откроется страница **Completing the New IP Packet Filter Wizard.**
13. Щелкните кнопку **Finish.**

    В списке фильтров IP-пакетов консоли ISA Management появится фильтр пакетов **DNS Query.**

Задание 5. Создание фильтра пакетов для Web-содержимого (HTTP)

Вы создадите фильтр пакетов, разрешающий прохождение трафика TCP через порт 80, что позволит ISA-серверу принимать Web-содержимое.

► **Создание фильтра IP-пакетов, разрешающего пересылку Web-содержимого**

1. Откройте консоль ISA Management.
2. Последовательно раскройте узлы Servers **and Arrays,** MyArray, Access **Policy,** найдите папку **IP Packet Filters.**
3. Щелкните правой кнопкой мыши папку **IP Packet Filters** и в контекстном меню последовательно выберите команды New и **Filter.** Откроется окно мастера New IP Packet Filter.
4. **В поле IP Packet Filter Name** укажите имя нового фильтра **HTTP Client** и щелкните кнопку Next.
5. На странице **Servers** оставьте переключатель в положении **All ISA server computers in the array** (все ISA-серверы массива) и щелкните кнопку Next
6. На странице **Filter Mode** оставьте переключатель в положении **Allow packet** transmission (разрешить передачу пакетов) и щелкните кнопку Next.
7. На странице **Filter Type** установите переключатель в положение **Custom** и щелкните кнопку Next. Откроется страница **Filter** Settings.
8. В поле со списком **IP Protocol** выберите TCP.
9. В поле со списком **Local Port** выберите **Dynamic.**
10. В поле со списком **Remote port выберите Fixed port и в** поле **Port** number справа от поля со списком **Remote port** введите 80. Щелкните кнопку Next.
11. На странице **Local** Computer оставьте переключатель в положении **Default IP Address(es) for each internal interface on** the ISA server **computer.**
12. На странице **Remote Computers** оставьте переключатель в положении **All Remote Computers** и щелкните кнопку Next. Откроется страница **Completing the New IP** Packet **Filter Wizard.**
13. Щелкните кнопку **Finish.**

    В списке фильтров IP-пакетов консоли ISA Management появится фильтр пакетов **HTTP Client.**

    Следует иметь в виду, что этот фильтр пакетов разрешает содержимое протокола HTTP, но не S-HTTP. Если необходимо разрешить просмотр безопасных Web-узлов, следует создать дополнительный разрешающий фильтр пакетов и указать в нем порт 443 протокола TCP.

Резюме

Хотя правила политики доступа и лраиила публикации чаще всего применяют для разрешения и запрещения доступа из Интернета в локальную сеть и из локальной сети в Интернет, иногда вместо них применяют фильтры IP-пакетов. Например, при публикации серверов в сети периметра или если на ISA-сервере выполняются приложения и службы, которым нужно прослушивать Интернет. Кроме того, фильтры IP-пакетов используют, когда необходимы разрешения доступа по протоколам, не основанным на TCP или UDP. Фильтры IP-пакетов бывают разрешающие и блокирующие.

В фильтрах IP-пакетов настраивают три типа параметров: фильтрацию IP-фрагментов, фильтрацию параметров протокола IP и ведение журналов разрешающих фильтров. При включенной фильтрации IP-фрагментов все фрагментированные IP-пакеты блокируются, что позволяет защититься от некоторых видов сетевых атак, но препятствует прохождению через ISA-сервер потоков аудио и видео. При включении фильтрации параметров протокола IP ISA-сервер блокирует все пакеты, содержащие слова «IP options» в заголовке. И, наконец, иногда ISA-сервер настраивают на ведение журналов разрешающих фильтров, когда регистрируются все пакеты — как разрешенные, так и заблокированные. По умолчанию в журналах регистрируются лишь последние.

Занятие 5. Настройка ISA-сервера на обнаружение внешних атак и вторжений

ISA-сервер настраивают на обнаружение стандартных сетевых атак. По умолчанию при включенном механизме обнаружения вторжений ISA-сервер регистрирует сообщение об атаке в журнале событий Windows 2000. Можно также сконфигурировать его для выполнения ответных действий, таких как отправка сообщения по электронной почте, запуск определенной программы, а также запуск или остановка определенных служб.

Изучив материал этого занятия, вы сможете:

- ✓ рассказать о том, какие типы сетевых атак способен обнаружить ISA-сервер;
- ✓ настроить ISA-сервер на обнаружение внешних атак и вторжений.

Продолжительность занятия — около 25 минут.

Типы вторжений и оповещения

ISA-сервер способен обнаруживать атаки на сеть. В этом случае он выполняет ряд заранее определенных действий (или *оповещений*). ISA-сервер способен определять следующие типы вторжений (рис. 4-14):

- *сканирование портов* (port scan и enumerated port scan);
- *IP-атаку без создания подключения* (IP half scan);
- *атаку с обратной адресацией* (land attack);
- *«ping смерти»* (Ping of Death);
- *UDP-бомбу* (UDP-bomb);
- *передачу срочных данных в Windows* (Windows out-of-band attack).

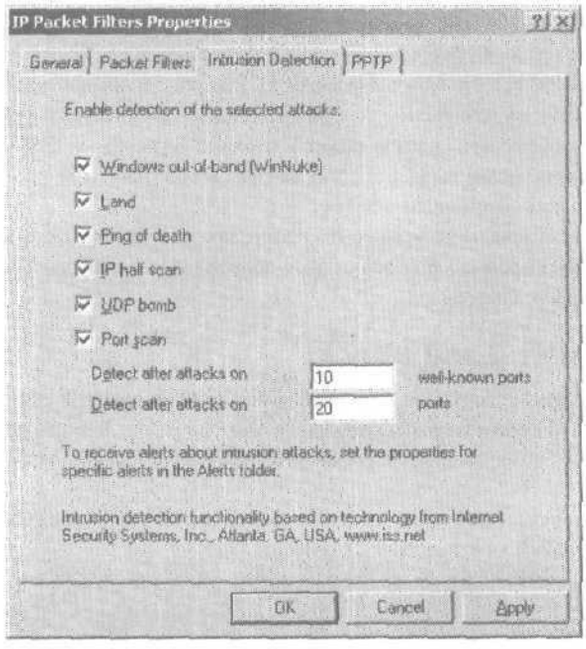


Рис. 4-14. Типы атак, обнаруживаемых ISA-сервером

Сканирование портов

ISA-сервер оповещает о двух типах сканирования портов: All Ports Scan (сканирование всех портов) и Enumerated Port Scan (атака перечисления портов).

Сканирование всех портов (all ports scan)

Оповещение об этой атаке инициируется при попытке извне обратиться к большему количеству портов, чем указано в параметрах ISA-сервера. Максимальное количество доступных портов указывают при настройке ISA-сервера.

Атака перечисления портов (enumerated port scan)

Оповещение об этой атаке инициируется, когда выполняется попытка перечислить все работающие на компьютере службы. Для этого запросы извне направляются на все порты с целью получения ответов.

При оповещении о такой атаке следует определить источник сканирования портов. Сравните его со службами, работающими на компьютере и являющимся целью атаки. Попробуйте выяснить цель сканирования. Проверьте журналы доступа, чтобы выявить признаки неправомочного доступа. Если такие признаки найдены, следует считать систему взломанной и предпринимать соответствующие действия.

IP-атака без создания подключения (IP half scan)

Оповещение об этой атаке инициируется, когда предпринимаются многократные попытки подключения к компьютеру, однако атакующий уклоняется от создания подключения.

Стандартное TCP-подключение осуществляется путем отправки адресату пакета SYN (запрос синхронизации). Если адресат ожидает подключение на данном порту, он отвечает пакетом SYN/ACK (подтверждение синхронизации). Инициатор подключения отправляет пакет ACK, и подключение устанавливается. Если адресат не ожидает подключения на данном порту, он отправляет в ответ пакет RST (сброс).

Многие системы не записывают в журнал информацию о подключении, пока не получат от инициатора подключения пакет ACK. Отправка пакета RST вместо завершающего пакета ACK прерывает процесс создания подключения и, следовательно, не учитывается в журнале. Инициатор в состоянии определить, какой пакет отправил адресат — SYN/ACK или RST. Таким образом, злоумышленник выясняет, какие порты открыты для подключения, а адресат ничего не знает о сканировании портов.

Если система оповестит об этом типе атаки, выясните по журналам адрес, с которого ведется сканирование, и затем настройте правила политики ISA-сервера или фильтры IP-пакетов на блокирование трафика с этого адреса.

Атака с обратной адресацией (Land attack)

При атаках такого типа создается TCP-подключение, в котором ложный IP-адрес и порт источника совпадает с IP-адресом и номером порта атакуемого компьютера. В некоторых реализациях протокола TCP такая атака вызывает зацикливание и аварийный отказ компьютера.

В случае оповещения об этом типе атаки настройте правила политики ISA-сервера или фильтры IP-пакетов на запрещение трафика от источника пакетов.

Атака «ping смерти» (Ping of Death)

Оповещение об этой атаке инициируется, когда к пакету запроса или контроля связи (ping) по протоколу ICMP (Internet Control Message Protocol) добавляются избыточные данные. Успешно выполненное нападение приводит к переполнению буферов ядра при попытке ответить и аварийному отказу компьютера.

В случае оповещения об этом типе атаки создайте правило протоколов, запрещающее входящие эхо-запросы протокола ICMP из Интернета.

Атака «UDP-бомба» (UDP bomb)

Оповещение об этом типе атаки инициируется при попытке отправить атакуемому некорректный UDP-пакет. В некоторых ранних версиях операционных систем получение UDP-пакета с ошибочными значениями в определенных полях вызывает разрушение ОС. Часто достаточно сложно определить причину сбоя.

Атака передачи срочных данных в Windows (Windows out-of-band attack или WinNuke)

Оповещение об этом типе атаки инициируется, когда предпринимается попытка вызвать отказ в обслуживании компьютера, защищенного ISA-сервером, посредством передачи срочных данных в Windows. Успешное нападение вызывает аварийный отказ компьютера или нарушение его подключения к сети.

Примечание Функции обнаружения вторжений ISA-сервер основаны на технологии, полученной по лицензии от компании Internet Security Systems Inc. (ISS), которая расположена в Атланте, штат Джорджия (адрес в Интернете — *http://www.iss.net*).

Настройка обнаружения вторжений

В процессе обнаружения вторжений ISA-сервер сравнивает сетевой трафик и записи журналов с методами известных атак. Если есть основания подозревать вторжение, ISA-сервер выполняет определенные в конфигурации действия — оповещения. Поддерживаются следующие оповещения: завершение подключения, завершение работы службы, сообщение по электронной почте, добавление записи в журнал и запуск определенной программы.

Чтобы ISA-сервер обнаруживал вторжения, установите флажок **Enable Intrusion detection** в диалоговом окне **IP Packet Filters Properties** (рис. 4-15).

В состав ISA-сервера входит предустановленное оповещение о вторжении Intrusion Detected (рис. 4-16).

По умолчанию, если включено обнаружение вторжений, то при выявлении любого типа вторжения это оповещение инициирует запись сообщения в журнал событий Windows 2000. Оповещение Intrusion Detected иногда настраивают на выполнение дополнительных действий при обнаружении вторжений. Кроме того, администраторы создают новые оповещения для выполнения особых ответных действий и параметров обнаружения определенных типов вторжений. Например, при сканировании портов можно указать пороговое количество опрашиваемых портов, вызывающее срабатывание оповещения.

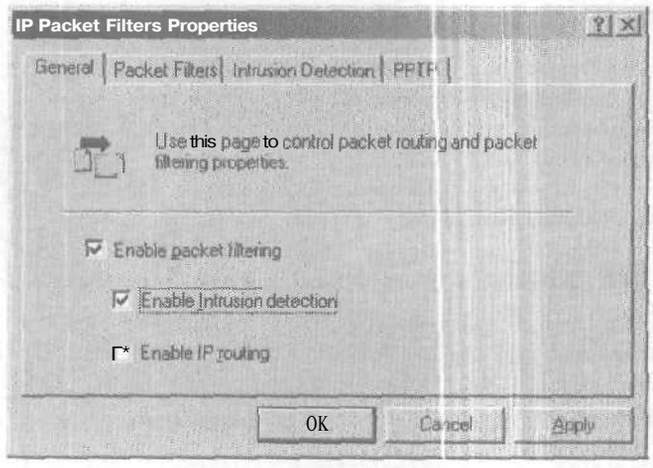


Рис. 4-15. Включение обнаружения вторжений

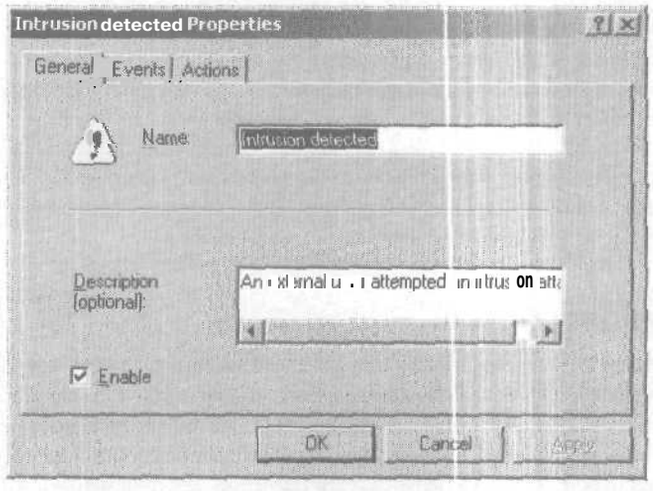


Рис. **4-16. Предустановленное оповещение Intrusion Detected**

▶ Настройка обнаружения вторжений

1. В дереве консоли ISA Management щелкните правой кнопкой мыши узел **IP Packet Filters** и в контекстном меню выберите **Properties.**
2. На вкладке **General** установите флажок Enable **Packet** filtering (если он еще не включен) и флажок **Enable Intrusion detection.**
3. На вкладке **Intrusion Detection** отметьте флажками типы атак, которые требуется обнаруживать:
   - **Windows out-of-band (WinNuke);**
   - **Land;**
   - **Ping of death;**
   - **IP half scan;**
   - **UDP bomb;**
   - **Port scan.**

4. В случае установки флажка **Port Scan** выполните следующие действия:
   - в поле **well-known ports**(общеизвестные порты) укажите пороговое число общеизвестных портов, после сканирования которых инициируется оповещения об атаке;
   - в поле **Ports** укажите пороговое число портов, после сканирования которых инициируется оповещения об атаке.

Примечание К общеизвестным относятся порты из диапазона 0-1023.

Практикум. Настройка обнаружения вторжений на ISA-сервере

Вы включите обнаружение ISA-сервером всех шести типов вторжений.

▶ **Включение обнаружения всех типов вторжений**

1. В консоли ISA Management последовательно раскройте узлы **Servers and Arrays,** MyArray, **Access Policy,** найдите узел **IP Packet** Filters.
2. Щелкните правой кнопкой мыши узел **IP Packet Filters** и в контекстном меню выберите **Properties.** Откроется диалоговое окно **IP Packet Filters Properties.**
3. На вкладке **General** щелкните флажок **Enable Intrusion detection.**
4. Перейдите на вкладку **Intrusion Detection,**
5. Установите флажки **Windows out-of-band (WinNuke), Land, Ping of death, IP half scan, UDP bomb и Port scan.**
6. Два поля **Detect after attacks on** (количество портов, по которым определяется атака) станут доступными для ввода. Оставьте в них значения по умолчанию и щелкните кнопку OK.

Резюме

При включении обнаружения вторжений в диалоговом окне **IP Packet Filters Properties** ISA-сервер можно настроить на обнаружение любого из шести типов известных сетевых атак: сканирование портов (port scan и enumerated port scan), IP-атака без создания подключения (IP half scan), атака с обратной адресацией (land attack), «ping смерти» (Ping of Death), UDP-бомба (UDP-bomb) и атака передачи срочных данных в Windows (Windows out-of-band attack или WinNuke). По умолчанию, если включено обнаружение вторжений, при выявлении любого типа вторжения это оповещение инициирует запись сообщения в журнал событий Windows 2000. Сообщения доступны для просмотра в оснастке Event Viewer (Просмотр событий). Если есть основания подозревать вторжение, ISA-сервер выполняет определенные в конфигурации действия — оповещения. Поддерживаются следующие оповещения: завершение подключения, завершение работы службы, сообщение по электронной почте, добавление записи в журнал и запуск определенной программы.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Ответы для самопроверки — в приложении А «Вопросы и ответы» в конце книги.

1. В каких из перечисленных далее условиях пользователь John получит доступ в Интернет через ISA-сервер? Предполагается, что существует только разрешающее (Allow) правило узлов и содержимого по умолчанию.
   - Вы создали правило протоколов, разрешающее доступ любому IP-трафику по любым запросам, а затем — еще одно правило протоколов, запрещающее пользователю John доступ к любому IP-трафику. Свойства исходящих Web-запросов массива по умолчанию не изменялись. Получит ли John доступ в Интернет через Web-браузер с клиента SecureNAT?
   - Вы создали правило протоколов, разрешающее доступ к любому IP-трафику всем членам группы Domain Users (Пользователи домена). John является членом группы Domain Guests (Гости домена), но не входит в группу Domain Users. Свойства исходящих Web-запросов массива умолчанию не изменялись. Получит ли John доступ в Интернет через Web-браузер с клиента SecureNAT?
   - Вы создали правило протоколов, разрешающее доступ любому IP-трафику по любым запросам, а затем — еще одно правило протоколов, запрещающее доступ к любому IP-трафику членам группы Domain Guests. John входит только в группу Domain Guests. Свойства исходящих Web-запросов массива изменены: требуется идентификация пользователей, не прошедших аутентификацию. Получит ли John доступ в Интернет через Web-брзузер с клиента брандмауэра?
   - Вы создали правило протоколов, разрешающее доступ к любому IP-трафику членам группы Domain Users. John входит в группу Domain Users. Сможет ли он установить подключение к Интернету по протоколу FTP из командной строки с компьютера, на котором нет ПО клиента брандмауэра?
2. Какие защитные меры следует предпринять, если обнаружена атака IP halfscan с определенного сетевого адреса?
3. В каких трех ситуациях для разрешения доступа в Интернет нужно создавать фильтры IP-пакетов вместо правил протоколов и правил узлов и содержимого?
4. Вы создали правило узлов и содержимого, запрещающее доступ к двум адресатам: *ftp://movies.acme.com/clips* и *ftp://radio.acme.com*. Пользователи имеют разрешения на загрузку файлов с FTP-узлов. Смогут ли они загрузить средствами FTP-клиента содержимое с узла *ftp://movies.acme.com?* Смогут ли они загрузить содержимое из папки *ftp://radio.acme.com/songs?*
5. Вы хотите запретить группе пользователей Windows 2000 загрузку любых аудиоданных с 10 до 16 часов по будним дням. Сколько потребуется создать элементов политики?

ГЛАВА 5

Ускорение доступа в Интернет средствами кэширования ISA-сервера

Занятие 1. Создание базовой политики кэширования 154

Занятие 2, Настройка конфигурации кэша ISA-сервера 1G3

Занятие 3. Загрузка содержимого кэша по расписанию 173

Закрепление материала 178

В этой главе

Сервер Microsoft Internet Security and Acceleration Server 2000 (ISA-сервер) позволяет повышать производительность подключения к Интернету посредством кэширования, благодаря чему служба Web-прокси получает запрашиваемые Web-объекты из локального кэша, а не из Интернета. Кэш также используется для хранения информации публикуемой внутренними серверами. Для настройки кэширования в соответствии с требованиями организации создается политика кэширования, которая определяется правилами маршрутизации и свойствами кэша, например *временем жизни* (time-to-live, TTL), Загрузка Web-содержимого по расписанию в соответствии с заданиями также повышает эффективность кэширования.

Прежде всего

Для изучения материалов этой главы необходимо:

- выполнить все задания глав 1–4.

Занятие 1. Создание базовой политики кэширования

Работая в режиме кэширующего сервера и кэшируя часто запрашиваемые Web-объекты, ISA-сервер повышает производительность сети. Создание политики кэширования подразумевает настройку правил маршрутизации, параметров конфигурации кэша и при необходимости политик доступа и правил публикации. На этом занятии вы познакомитесь с основными принципами настройки политик кэширования и с самым важным этапом этого процесса — созданием правил маршрутизации.

Изучив материал этого занятия, вы сможете:

- описать, как ISA-сервер определяет место извлечения запрашиваемого объекта (из кэша или с узла-источника);
- создавать правила маршрутизации, определяющие порядок выполнения ISA-сервером клиентских запросов Web-объектов.

Продолжительность занятия — около 40 минут.

Как работает механизм кэширования

ISA-сервер кэширует объекты, часто запрашиваемые по протоколам HTTP и FTP. Обрабатывая запросы Web- или FTP-информации, ISA-сервер прежде всего обращается к своему кэшу. **Если** запрашиваемых данных в нем нет, ISA-сервер инициирует запрос узлу-адресату. ISA-сервер кэширует информацию Интернета, подученную по запросам клиентов в локальной сети (прямое кэширование), и/или содержимое внутренних серверов для обслуживания запросов (обратное кэширование) пользователей Интернета. Порядок и разрешение на выполнение прямого и/или обратного кэширования определяется конфигурацией правил маршрутизации. Получая ответы целевого Web- или FTP-сервера, ISA-сервер кэширует их и направляет информацию клиенту.

В состав ISA-сервера входит *фильтр-перенаправитель* (redirector filter) HTTP, который предоставляет клиентам брандмауэра и SecureNAT доступ к возможностям кэширования. HTTP-перенаправитель обеспечивает поддержку кэширования по Web-запросам клиентов брандмауэра и SecureNAT.

ISA-сервер, работающий в режиме брандмауэра, кэширование не поддерживает.

Обработка правил кэширования

Решение о том, откуда следует получить запрашиваемый объект — из кэша или с другого сервера, ISA-сервер принимает на основании конфигурации кэша и правил маршрутизации.

Конфигурация кэша

Конфигурация кэша представляют собой набор изменяемых параметров, доступных для настройки в диалоговом окне **Cache Configuration Properties.** Они определяют политики срока хранения (времени жизни) информации в кэше и активного кэширования, максимальный размер кэшируемых объектов, максимальный размер кэшируемых в памяти URL-адресов, а также долю памяти, выделенную для кэширования.

На рис. 5-1 показаны два способа открыть диалоговое окно **Cache** Configuration **Properties:** щелкнуть правой кнопкой узел Cache **Configuration** и в контекстном меню выбрать

команду **Properties** или выбрать узел **Cache Configuration** и щелкнуть значок **Configure Cache Policy** на панели заданий.

Подробнее о свойствах конфигурации кэша — в занятии 2 этой главы.

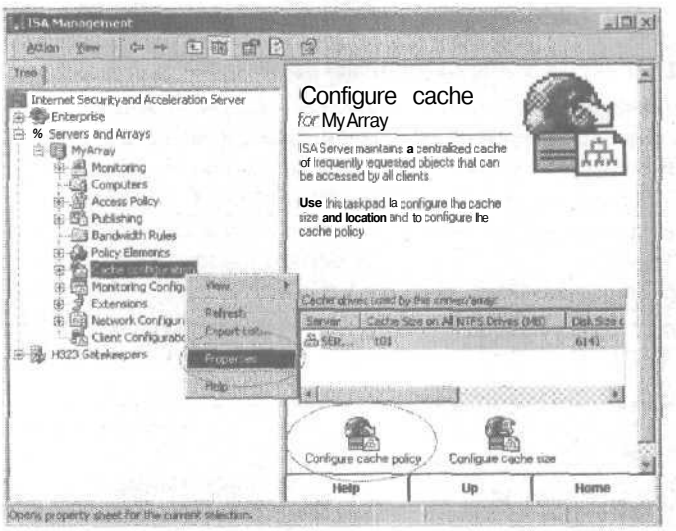


Рис. 5-1. Доступ к конфигурации кэша

Правила маршрутизации

Самым важным этапом создания политики кэширования считается настройка правил маршрутизации, определяющих порядок размещения и извлечения информации из кэша ISA-сервера. Настройка правила маршрутизации выполняется в узле **Network Configuration** оснастки **ISA Management.**

Порядок размещения информации в кэше

Запись загружаемых объектов в кэш выполняется в соответствии с правилами маршрутизации. Создавая новое правило маршрутизации, следует указать, как кэшируется информация: вся без исключения (в том числе динамическое содержимое), только данные (если их заголовки для запросов и ответов указывают на необходимость кэширования) или что она не кэшируется вообще. Правило маршрутизации по умолчанию (его модификация невозможна) ISA-сервера предусматривает кэширование, только когда заголовки для запросов и ответов указывают на такую необходимость. Чтобы ISA-сервер кэшировал все содержимое, следует создать соответствующее новое правило маршрутизации.

Порядок извлечения информации из кэша

Правила маршрутизации также определяют обстоятельства, определяющие, как ISA-сервер отвечает на Web-запрос — извлекая содержимое из кэша или перенаправляя запрос вышестоящему серверу. При создании нового правила маршрутизации вы вправе определить один из нескольких вариантов поведения ISA-сервера: запрашиваемый объект извлекается из кэша только при условии наличия в кэше «свежей» информации и при отсутствии таковой маршрутизирует запрос вышестоящему серверу; запрашиваемые объекты извлекаются из кэша в любом случае, а запрос перенаправляется вышестоящему серверу, только если нужного объекта в кэше нет; запрашиваемые объекты извлекаются из кэша в любом случае, но запрос выше по цепочке никогда не пересылается.

Согласно правилу маршрутизации по умолчанию, ISA-сервер перенаправляет запрос, если в кэше отсутствует «свежая» версия запрашиваемого объекта. Это правило изменить нельзя, поэтому, чтобы определить другой порядок работы с кэшем, необходимо создать новые правила.

Применение правил маршрутизации к определенным адресатам

Правило маршрутизации применяется к запросам, если адресат в запросе совпадает с адресатом, указанном в правиле маршрутизации. Существует несколько вариантов задания правила маршрутизации: для всех адресатов, для всех внутренних адресатов, для всех внешних адресатов, для определенного подмножества адресатов или для всех адресатов за исключением определенного их подмножества. Такая свобода выбора позволяет раздельно управлять «поведением» ISA-сервера при прямом и обратном кэшировании или настраивать его особым образом для отдельных адресатов.

Примечание Обратное кэширование управляется правилами маршрутизации, в которых указываются внутренние адресаты.

▶ **Создание правила маршрутизации**

1. В дереве консоли **ISA Management** щелкните правой кнопкой папку **Routing** (она расположена в папке **Network Configuration)** и в контекстном меню последовательно выберите New и **Rule.**
2. На первой странице мастера создания нового правила маршрутизации **New Routing Rule** введите имя правила и щелкните кнопку **Next.**
3. На странице определения подмножества адресатов **Destination Sets** выберите подмножество адресатов, к которому применяется данное правило, и щелкните **Next.**
4. На странице определения действия по запросу **Request Action** выберите, откуда ISA-сервер должен загружать запрашиваемые клиентом объекты: непосредственно с запрашиваемого узла, с вышестоящего сервера или с внутреннего Web-узла. Кроме того, укажите, используется ли при этом запись удаленного доступа.
5. На странице **Cache Retrieval Configuration** укажите, должен ли ISA-сервер обращаться за запрашиваемым объектом к кэшу.
6. На странице **Cache Content Configuration** укажите, когда объекты должны кэшироваться.

Параметры существующего правила маршрутизации можно изменять на странице свойств правила (рис. 5-2).

▶ **Изменение порядка кэширования для существующего правила маршрутизации**

1. В дереве консоли **ISA Management** выберите папку **Routing.**
2. В области сведений щелкните правей кнопкой правило маршрутизации, свойства которого необходимо изменить, и в контекстном меню щелкните команду **Properties.** (Не пытайтесь изменить свойства правила по умолчанию — это невозможно.)
3. На вкладке **Cache** установите переключатель в области **Search cache for** в одно из следующих положений:
   - A Valid **version of the object; if none** exists, **retrieve the request using the route defined on the Action tab** — если объект должен извлекаться из кэша только тогда, когда его кэшированная копия доступна и *не* просрочена. В противном случае запросы перенаправляются вышестоящему серверу, указанному на вкладке **Action;**
   - **Any version of the object; if none** exists, **retrieve the request using the route defined on the Action tab** — если из кэша должна извлекаться любая доступная версия объекта, а

при ее отсутствии запросы перенаправляются вышестоящему серверу, указанному на вкладке **Action;**

- **Any version of the requested object in the cache,** never **route the request** — если из кэша должна извлекаться любая доступная версия объекта, а при ее отсутствии запросы дальше никуда не перенаправляются.

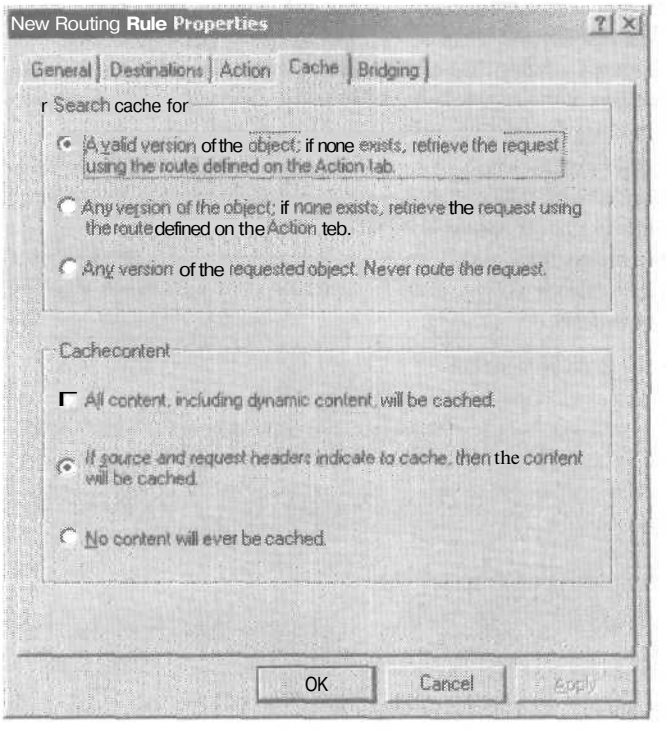


Рис. 5-2. **Настройка порядка кэширования в правиле маршрутизации**

4. На вкладке **Cache** установите переключатель в области **Cache Content** в одно из следующих положений:
   - **All content, including dynamic content, will be cached** — чтобы кэшировать всю информацию, в том числе и динамическое содержимое;
   - **If source and request headers indicate to cache, then the content will be cached** — чтобы кэшировать содержимое, только когда заголовки для запросов и ответов содержат такое указание;
   - **No content will ever be cached** — чтобы запретить какое-либо кэширование.

▶ **Изменение порядка извлечения запрашиваемых объектов**

1. В дереве консоли **ISA Management** выберите папку **Routing.**
2. В области сведений щелкните правой кнопкой правило маршрутизации, свойства которого необходимо изменить, и в контекстном меню выберите команду **Properties.**
3. Установите переключатель на вкладке **Action** в одно из следующих положений:
   - **Retrieving them directly from the** specified **destination** — чтобы получать все запрашиваемые объекты непосредственно из Интернета;
   - **Routing them to a specified upstream server** — если запрос следует перенаправлять на вышестоящий сервер, не забудьте указать основной и резервный маршруты;

- **Redirecting them to a hosted site** — если запрос следует перенаправлять на другой компьютер, укажите узел, порт и порт SSL.

4. *(При необходимости.)* Если запрос перенаправляется определенному компьютеру или вышестоящему серверу и при этом в качестве основного маршрута следует использовать подключение по телефонной линии, установите флажок Use **dial-up** entry **for primary route.** Это обеспечит выполнение автоматического подключения по телефонной линии по запросам клиентов Web-прокси.
5. *(При необходимости.)* Если запрос перенаправляется вышестоящему серверу и в качестве резервного маршрута следует использовать подключение по телефонной линии, установите флажок **Use dial-up entry for backup route.**

Кроме прочего, правила маршрутизации определяют, должны ли кэшироваться результаты запроса, а также динамическое содержимое вместе с нединамическим. ISA-сервер распознает объекты с динамическим содержимым по знаку вопроса (?) в адресе.

Существует несколько вариантов выбора подмножества адресатов: все адресаты, все внутренние адресаты, все внешние адресаты, указанное подмножество адресатов или все направления за исключением указанного.

► **Указание адресатов для правила маршрутизации**

1. В дереве консоли **ISA Management** выберите папку **Routing.**
2. В области сведений щелкните правой кнопкой правило маршрутизации, свойство которого необходимо изменить, и далее в контекстном меню — команду **Properties.**
3. На вкладке адресатов **Destinations** выберите подмножество адресатов, к которому будет применяться правило маршрутизации:
   - **All destinations** — все адресаты;
   - **AH internal destinations** — все внутренние адресаты;
   - **All external destinations** — все внешние адресаты;
   - **Selected destination set** — указанное подмножество адресатов;
   - **All destinations except selected set** — все направления за исключением указанного.
4. Если вы выбрали **Selected destination set или All destination except selected** set, укажите в поле со списком **Name** подмножество адресатов.

Примечание Если необходимого подмножества адресатов нет, создайте его, щелкнув кнопку New, после чего выберите созданное подмножество в поле со списком **Name.**

Чтобы увидеть все правила маршрутизации ISA-сервера, выберите папку **Routing** узла **Network Configuration** оснастки **ISA Management** — в области сведений отображаются имеющиеся правила маршрутизации.

Порядок выполнения правил

Правила маршрутизации выполняются в определенном порядке, при этом правило по умолчанию выполняется последним. ISA-сервер обрабатывает правила маршрутизации по порядку, начиная с первого. Если запрос отвечает указанным в правиле условиям, он маршрутизируется, перенаправляется и кэшируется в соответствии с этим правилом, в противном случае обрабатывается следующее правило. Этот процесс продолжается до тех пор, пока не встретится правило, соответствующее запросу, или не будет применено правило по умолчанию.

► **Изменение порядка выполнения правил маршрутизации**

1. В дереве консоли ISA **Management** выберите папку Routing.
2. В области сведений щелкните правой кнопкой правило, которое следует переместить в общей последовательности правил, и выберите **Move Up,** чтобы переместить правило вверх, или **Move Down** — чтобы переместить его вниз,
3. При необходимости повторите операцию несколько раз, чтобы расположить правила в требуемом порядке.

Примечание Положение правила по умолчанию изменить нельзя.

Правило маршрутизации по умолчанию

Правило маршрутизации по умолчанию создается во время установки ISA-сервера. Согласно этому правилу, на запрос возвращается непросроченная версия запрашиваемого объекта из кэша, если таковая существует. В противном случае запрошенный объект должен загружаться из Интернета. Важно отметить, что, согласно этому правилу, динамическое содержимое не кэшируется.

Правило маршрутизации по умолчанию обрабатывается последним. Удалить правило маршрутизации по умолчанию вам не удастся, но вы вправе изменить его свойства на вкладке **Action** диалогового окна **Default Rule Properties,** а также указать, каким образом перенаправляются исходящие Web-запросы (вкладка **Bridging).**

Процесс кэширования

На рис. 5-3 показана схема процесса кэширования объектов, то есть то, как ISA-сервер анализирует правила маршрутизации, конфигурацию кэша и существующее содержимое кэша, определяя, откуда следует извлекать объект: из кэша или из другого источника.

Если пользователю разрешено запрашивать объекты, ISA-сервер сначала ищет запрашиваемый объект в кэше. Если запрос выполняется массивом ISA-серверов, то, чтобы определить сервер, в кэше которого может быть требуемый объект, используется алгоритм протокола CARP (Cache Array Routing Protocol). Если обнаружить объект в кэше не удалось, ISA-сервер считывает информацию, указанную в разделе Action правила маршрутизации, и определяет, куда следует перенаправить запрос. Если объект в кэше найден, ISA-сервер выполняет процедуру, описанную далее.

1. ISA-сервер проверяет, действителен ли объект. Объект считается недействительным, если выполняется хотя бы одно из следующих условий:
   - истекло определяемое источником время жизни (TTL);
   - истекло TTL, определенное в задании загрузки содержимого кэша по расписанию;
   - истекло TTL, определенное для объекта в диалоговом окне **Cache Configuration Properties.**

   Действительные объекты ISA-сервер извлекает из кэша и возвращает пользователю.
2. Обнаружив недействительный объект, ISA-сервер проверяет соответствующее правило маршрутизации. Если в нем указано, что возвращается любая версия объекта, ISA-сервер извлекает недействительный объект из кэша и возвращает клиенту.
3. Если правило маршрутизации предписывает перенаправить запрос, ISA-сервер определяет, куда его переслать: на вышестоящий сервер или на запрашиваемый Web-сервер.
4. Если, согласно правилу маршрутизации, запрос пересылается на Web-сервер, ISA-сервер проверяет его доступность.

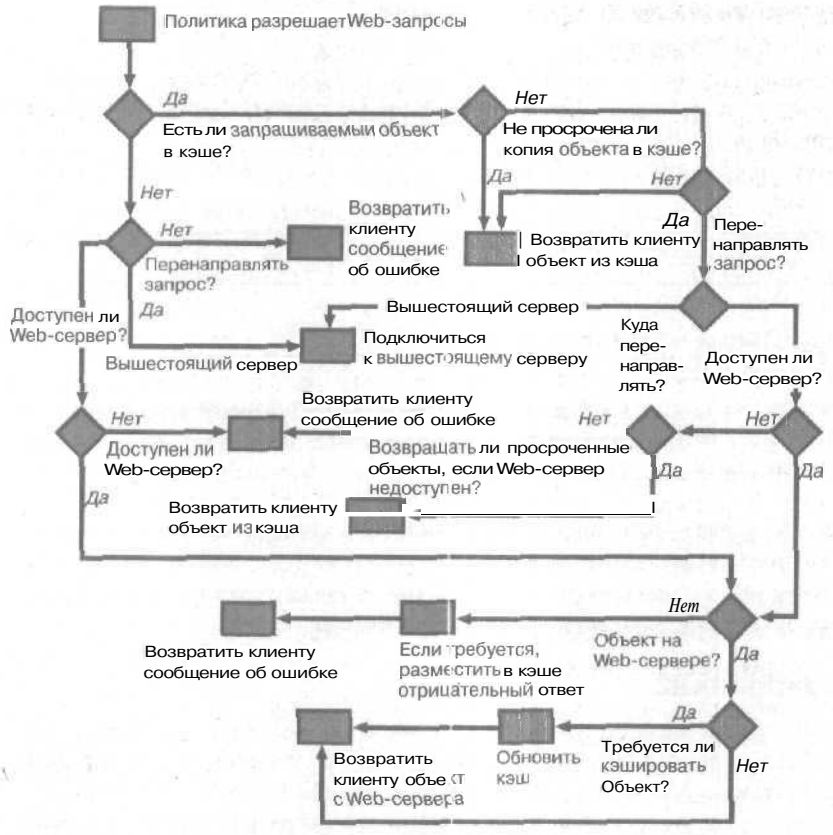


Рис. 5-3. **Процесс кэширования объектов**

5. Если Web-сервер недоступен, ISA-сервер проверяет, допускает ли существующая конфигурация возвращение просроченных объектов. Если да, объект извлекается из кэша и передается клиенту.
6. Если Web-сервер доступен, ISA-сервер определяет, следует ли кэшировать искомый объект. Если это так и в правиле маршрутизации определено, что ответ следует кэшировать, ISA-сервер размещает объект в кэше и возвращает его клиенту.

Фильтрация кэша

Применяя различные правила маршрутизации к разным адресатам, удается настроить ISA-сервер для кэширования содержимого только от заранее определенных адресатов.

Допустим, вы не хотите кэшировать объекты с определенного сервера в Интернете, например example.microsoft.com. Создайте правило маршрутизации со следующими свойствами:

- в окне **Destination Set** укажите адрес example.microsoft.com;
- в окне **Request Action** — подходящий метод маршрутизации;
- параметры кэша установите так, чтобы ответ никогда не кэшировался. Это обеспечит поступление самой свежей информации непосредственно с узла.

Дополнительная политика кэширования

Правила узлов, содержимого и публикации также влияют на порядок кэширования.

При установке ISA-сервера в режиме сервера кэширования правила узлов и содержимого обеспечивают механизмы политики доступа и безопасности. Правила узлов и содержимого регулируют доступ к узлам и MIME-содержанию (Multipurpose Internet Mail Extensions) пользователям Интернета и клиентским компьютерам.

Правила Web-публикации обеспечивают сопоставление (пересылку) запросов клиентов из Интернета с соответствующими Web-серверами в корпоративной сети. Правила Web-публикации влияют на обратное кэширование, определяя подмножества клиентов, которые вправе обращаться к кэшу, и серверы, данные которых разрешено размещать в кэше.

Практикум. Кэширование динамического содержимого

ISA-сервер определяет Web-объекты с динамическим содержимым по знаку вопроса (?) в адресе. Порядок кэширования динамического содержимого настраивается в правилах маршрутизации. Согласно правилу маршрутизации, по умолчанию кэшируются только те объекты, содержимое которых не является динамическим. Ваша задача — включить кэширование динамического содержимого, для чего необходимо создать новое правило маршрутизации.

Задание. Создание правила маршрутизации для кэширования статического и динамического содержимого

Свойства кэширования правила маршрутизации по умолчанию изменить нельзя, поэтому, чтобы изменить тип содержимого, которое кэшируется ISA-сервером, необходимо создать новое правило маршрутизации, согласно которому кэшируется все содержимое. В этом случае результаты станут кэшироваться независимо от типа содержимого.

▶ **Создание правила маршрутизации для кэширования всего содержимого**

1. В оснастке **ISA Management** последовательно раскройте узлы **Servers and Arrays, MyArray, Network Configuration и Routing.**
2. Щелкните правой кнопкой папку **Routing** и в контекстном меню последовательно выберите New и **Rule.** Откроется окно мастера **New Routing Rule.**
3. В текстовом поле **Routing rule name** введите **Cache Dynamic Content.**
4. Щелкните кнопку Next.
5. На странице **Destination Sets** оставьте все без изменений и щелкните кнопку Next.
6. На странице **Request Action** оставьте установленное по умолчанию положение переключателя **Retrieve them directly from specified destination** и щелкните кнопку Next.
7. На странице **Cache Retrieval Configuration** оставьте установленное по умолчанию положение переключателя **A valid version of the object; if none** exists, **retrieve the request using the specified requested action** и щелкните кнопку Next
8. На странице **Cache Content Configuration** установите переключатель в положение **All content, including dynamic content, will be cached** и щелкните кнопку Next.
9. На странице **Completing The New Routing Rule** щелкните кнопку **Finish.**

В области сведений появится правило маршрутизации с именем **Cache Dynamic Content.**

Резюме

Несмотря на то, что полная политики кэширования ISA-сервера подразумевает как конфигурацию кэша, так и политику доступа и правила публикации, порядок кэширования, то есть выбор объектов кэширования и случаев, когда запрашиваемый объект должен извлекаться из кэша, определяется правилами маршрутизации. Это основа всей политики кэширования.

Правила маршрутизации, настраиваемые в узле Network Configuration оснастки ISA Management, определяют способ обработки запроса ISA-сервером. При этом возможны следующие варианты:

- запрос перенаправляется вышестоящему серверу, если ISA-сервер не в состоянии возвратить действительную (не просроченную) версию запрашиваемого объекта из кэша;
- запрос перенаправляется вышестоящему серверу, если ISA-сервер не в состоянии возвратить из кэша хоть какую-нибудь версию (действительную или нет) запрашиваемого объекта;
- из кэша извлекается любая имеющаяся версия запрашиваемого объекта, а запрос никогда не перенаправляется куда-либо далее.

Кроме того, правила маршрутизации определяют, в каких случаях содержимое после выполнения запроса кэшируется: всегда, никогда или только в тех случаях, когда заголовки для запросов и ответов указывают ча необходимость кэширования.

Существует несколько вариантов лрименения правила маршрутизации: ко всем адресатам, ко всем внутренним адресатам, ко всем внешним адресатам, к определенному подмножеству адресатов или ко всем адресатам за исключением определенного их подмножества. Применяя различные правила маршрутизации к разным адресатам, вы можете настроить ISA-сервер для кэширования содержимого только от указанных адресатов.

Правила маршрутизации располагаются и выполняются в определенном порядке, причем правило по умолчанию всегда выполняется последним. Если запрос отвечает указанным в правиле условиям, он маршрутизируется, перенаправляется и кэшируется в соответствии с этим правилом, в противном случае обрабатывается следующее правило. Этот процесс продолжается до тех пор, пока не встретится правило, соответствующее запросу, или не будет применено правило по умолчанию. Правило маршрутизации по умолчанию настроено на перенаправление запросов вверх по иерархии, если в кэше отсутствует свежая версия запрашиваемого объекта. Кроме того, правило маршрутизации по умолчанию предусматривает сохранение объектов в кэше ISA-сервера только в том случае, если заголовки для запросов и ответов указывают на необходимость кэширования данного объекта. Правило маршрутизации по умолчанию изменять нельзя, поэтому для введения новой политики кэширования необходимо создавать новые правила маршрутизации.

Занятие 2, Настройка конфигурации кэша ISA-сервера

Конфигурацией кэша называется совокупность таких его настраиваемых параметров, как размер кэша, его местоположение, порядок кэширования в оперативной памяти, время жизни объектов (TTL), порядок активного кэширования и кэширования отрицательных ответов, ограничения кэширования объектов и общие процедуры кэширования. Эти параметры настраиваются средствами диалогового окна **Properties** узла **Cache Configuration** и диалогового окна **Properties** отдельных серверов в папке **Drives** оснастки ISA Management.

Изучив материал этого занятия, вы сможете:

- ✓ устанавливать размер и местоположение диска кэша средствами оснастки ISA Management;
- ✓ ограничивать размер хранимых в кэше объектов;
- ✓ выделять определенную часть свободной оперативной памяти для кэширования;
- ✓ включать кэширование динамического содержимого;
- ✓ устанавливать политики срока действия кэшированных HTTP и FTP-объектов;
- ✓ определять, когда и в каких случаях ISA-сервер возвращает просроченное содержимое;
- ✓ включать активное кэширование;
- ✓ настраивать кэширование отрицательных ответов.

Продолжительность занятия — около 45 минут.

Конфигурирование дисков кэша

При установке ISA-сервера в режиме сервера кэширования (Cache) или в смешанном (Integrated) режиме установщик предлагает выбрать диски для размещения кэша. На выбранных дисках ISA-сервер резервирует пространство для хранения кэшированных данных.

Вы вправе в любое время изменить конфигурацию дисков кэша, воспользовавшись страницами свойств серверов, значки которых размещены в папке **Drives** узла **Cache Configuration** оснастки ISA Management.

Требования и рекомендации для кэша

Для кэширования используется раздел NTFS локального диска. Как правило, наивысшая производительность достигается, когда кэш размещается на специально выделенном диске, а не на том, где расположены программные файлы ISA-сервера и операционной системы Windows 2000. Выделяемый для кэширования отдельный диск следует предварительно переформатировать.

Настроить кэширование на ISA-сервере можно только при наличии на компьютере по крайней мере одного тома NTFS. Если диск компьютера разбит на разделы с файловой системой FAT, раздел, предназначенный для кэша, следует преобразовать в раздел NTFS при помощи утилиты Convert.exe, входящей в состав Windows 2000 Server. Эта утилита не разрушает хранящиеся на диске данные. Подробнее об ее использовании вы узнаете, выполнив в командной строке команду **convert /?.**

Диски для размещения кэша выбираются во время установки ISA-сервера. Если вы планируете использовать ISA-сервер для кэширования, выделите для кэша как можно больше дискового пространства. Впоследствии размер кэша можно увеличить, добавляя при необходимости дополнительное дисковое пространство.

По умолчанию программа установки находит самый большой раздел NTFS и устанавливает размер кэша равным 100 Мбайт при наличии в этом разделе не менее 150 Мбайт свободного пространства- При установке для кэша требуется назначить один диск и выделить на нем по крайней мере 5 Мбайт. При создании кэша рекомендуется руководствоваться следующим правилом: размер кэша должен быть равен 100 Мбайт плюс 0,5 Мбайт на каждый клиент Web-прокси, полученное значение следует округлить до большего целого значения мегабайт,

Кроме того, для повышения производительности иногда требуется изменить местоположение кэша по умолчанию, указав самый быстрый жесткий диск. Предпочтительнее при этом достаточно большие SCSI-диски.

Windows 2000 позволяет форматировать диски, не назначая им буквенного обозначения, однако следует иметь в виду, что ISA-сервер такие диски не распознает.

Размер и местоположение кэша

Для каждого сервера устанавливается размер и местоположение кэша, используемого службой Web-прокси. При этом желательно выделить для него достаточно места, так как при переполнении хранящиеся в кэше объекты удаляются.

▶ **Настройка размера кэша на сервере**

1. В дереве консоли **ISA Management** раскройте узел **Cache Configuration** и выберите папку **Drives.**
2. В области сведений щелкните правой кнопкой сервер, параметры которого следует изменять, и в контекстном меню выберите команду **Properties.**
3. Укажите нужный диск NTFS.
4. В текстовом поле **Maximum cache size (MB)** введите размер кэша и щелкните кнопку Set, чтобы установить заданное значение.
5. Щелкните **OK.**

Кроме того, вы вправе ограничить размер оперативной памяти, используемой для кэширования, задав в процентном выражении ее часть, которую разрешено занимать под кэшированные объекты.

▶ **Установка ограничения на долю свободной памяти, используемой для кэширования**

1. В дереве консоли **ISA Management** щелкните правой кнопкой узел **Cache Configuration** и в контекстном меню выберите **Properties.**
2. На вкладке **Advanced** в текстовом поле **Percentage of free memory to use for caching** (часть свободной памяти, используемой для кэширования) укажите, сколько процентов памяти разрешено резервировать для кэширования (это число не должно превышать 100 %).
3. Щелкните кнопку **OK.**

Чтобы изменения вступили в силу, следует остановить и перезапустить службу Web-прокси.

Файлы содержимого кэша

После окончания настройки диска для кэширования (рис. 5-4) ISA-сервер создает на нем файл содержимого кэша с расширением .cdat. Этот файл хранится в папке **Urlcache**.

Для каждых 10 Гбайт дискового пространства, выделенных для кэша, создаются отдельные файлы содержимого кэша. Например, если на диске под кэш отведено 12 Гбайт, ISA-сервер создаст два файла размером 10 и 2 Гбайта.

Кэшируемые объекты добавляются о файл содержимого кэша, Если файл содержимого кэша переполнен и новый объект в него не помещается, ISA-сервер удаляет старые

объекты из кэша, выбирая их на основании критериев, учитывающих возраст, частоту обращений к объектам и их размер.

Внимание! Не редактируйте и не удаляйте файлы содержимого кэша.

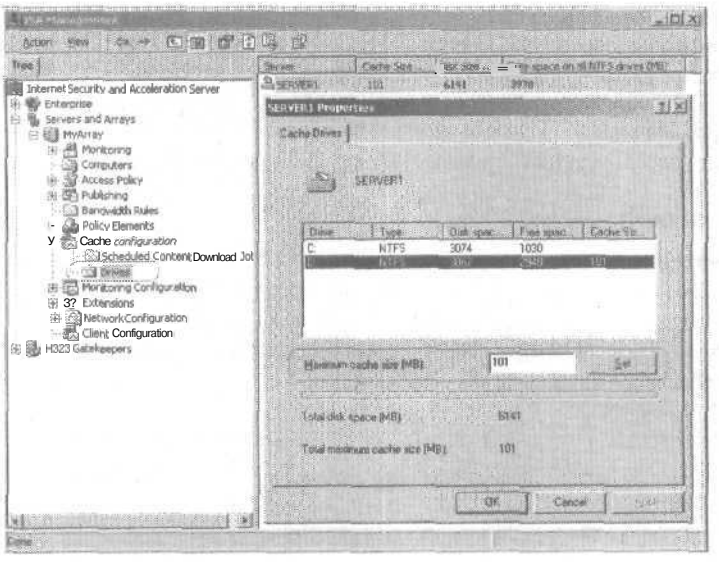


Рис. 5-4. Настройка диска кэша и файла содержимого

Выбор порядка кэширования объектов

Несмотря на то, что правила маршрутизации позволяют управлять кэшированием в зависимости от адресатов и типа содержимого (динамическое или статическое), в диалоговом окне **Cache Configuration Properties** можно выполнить более тонкую настройку кэширования любых объектов.

Кэширование содержимого определенного типа

Для кэширования можно выбирать HTTP-объекты различных типов:

- объекты, размер которых превышает указанное значение;
- объекты, дата последнего изменения которых не указана;
- объекты, не возвращающие ответ 200 (код нормального выполнение запроса);
- объекты со знаками вопроса в URL,

▶ **Настройка кэширования содержимого в зависимости от типа**

1. В дереве консоли **ISA Management** щелкните правой кнопкой узел **Cache Configuration** и в контекстном меню выберите команду **Properties.**
2. На вкладке **Advanced** выполните одно из следующих действий:
   - чтобы ограничить размер кэшируемых объектов, установите флажок **Do not cache objects larger than,** введите максимально допустимый размер и укажите единицы измерения (килобайты, мегабайты или гигабайты);
   - чтобы кэшировать объекты, для которых не указано время последнего изменения, установите флажок **Cache objects that have an unspecified last modification time;**

- чтобы кэшировать динамическое содержимое, установите флажок **Cache dynamic content (objects with question marks in the URL).**

3. Щелкните **OK.**

Примечание Чтобы ограничить максимальный размер объектов, кэшируемых в памяти, укажите в текстовом поле **Maximum size of URL cached in memory (bytes)** максимальный объем памяти в байтах, выделяемый под отдельные объекты.

При SSL-сопряжении ISA-сервер кэширует как HTTP-, так и SSL-объекты. Для управления кэшированием SSL-объектов используется COM-объект FPCWebRequestConfiguration. Подробнее — в ресурсах для разработчиков «ISA Server Software Development Kit».

Кэширование в оперативной памяти

ISA-сервер кэширует объекты в оперативной памяти и на диске. Первые извлекаются быстрее вторых. **По** умолчанию объекты меньше 12800 байт хранятся в оперативной памяти и на диске, а объекты большего размера кэшируются только **на** диске.

Максимальный размер хранящихся в памяти объектов устанавливается на вкладке **Advanced** диалогового окна **Cache Configuration Properties.**

Заголовки для ответов

ISA-сервер не кэширует ответы на запросы, содержащие следующие HTTP-заголовки для ответов:

- cache-control: no-cache;
- cache-control: private;
- pragma: no-cache;
- www-authenticate;
- set-cookie.

Заголовки для запросов

Кроме того, ISA-сервер не кэширует ответы на запросы, содержащие следующие HTTP-заголовки для запросов:

- authorization — кроме случаев, когда исходный сервер однозначно позволяет кэшировать, включая в ответ заголовок «cache-control: public»;
- cache-control: no-store.

Настройка политик, определяющих устаревшие объекты кэша

ISA-сервер позволяет очень гибко управлять политиками, определяющими устаревшие объекты кэша. Для **HTTP-** и FTP-объектов вы вправе выбрать не только эти политики, но и включение/отключение самого кэширования. Кроме того, вы можете определить, в каких случаях в ответ на запрос возвращаются просроченные объекты.

Кэширование HTTP-объектов

ISA-сервер хранит в кэше просроченные объекты и использует их в течение определенного времени, если узел-источник в Интернете становится недоступным. Просроченным называется объект, время жизни (TTL) которого истекло. Политика, определяющая устаревшие объекты, регулирует баланс между необходимостью в обновлении данных и сете-

вой производительностью. В зависимости от требований организации (рис. 5-5), выбирается одна из перечисленных далее политик, определяющих устаревшие HTTP-объекты в кэше:

- **Frequently** — эта политика предусматривает обязательное обновление объектов кэша несмотря на то, что частая их загрузка из Интернета может снизить сетевую производительность;
- **Less frequently** — объекты в кэше обновляются реже, но не в ущерб сетевой производительности;
- **Normally** — сбалансированный подход, устанавливаемый по умолчанию. Объекты обновляются достаточно часто, при этом обеспечивается оптимальная производительность сети;
- **Custom settings** — нестандартная конфигурация, в которой вы вправе установить TTL в любое значение — от нуля до определенного процента от возраста содержимого. Чем выше процент, тем реже обновляется кэш.

▶ **Настройка кэширования HTTP-объектов**

1. В дереве консоли ISA **Management** щелкните правой кнопкой узел **Cache Configuration** и в контекстном меню выберите **Properties.**
2. На вкладке HTTP установите флажок **Enable HTTP caching,** чтобы включить кэширование HTTP.

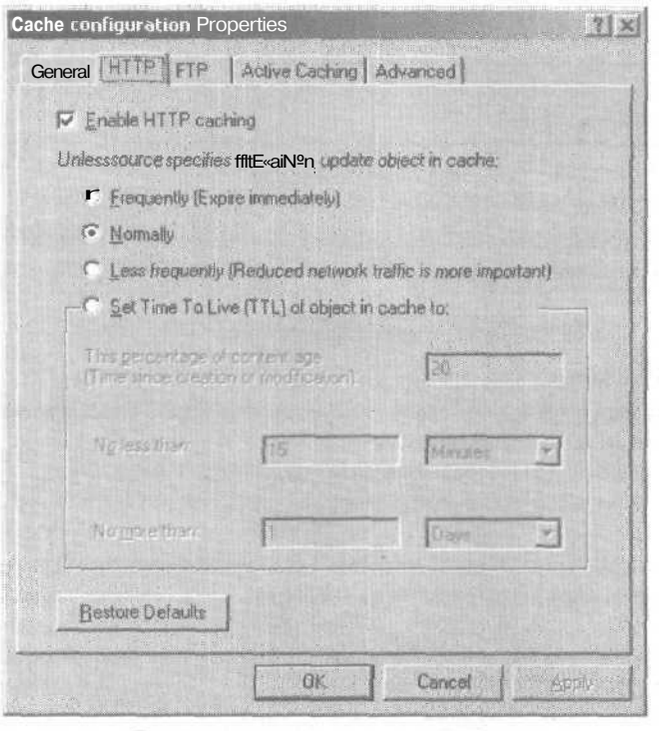


Рис. 5-5. Конфигурация кэширования HTTP-объектов

3. Установите переключатель **Unless source specifies expiration, update object in cache** в одно из следующих положений:
   - **Frequently (Expire immediately)** — если требуется обеспечить наличие самой свежей информации. В этом случае TTL равно нулю;

- **Normally** — если требуется баланс между свежестью информации и нагрузкой на систему;
- **Less frequently (Reduced network traffic is more important)** — если необходимо минимизировать нагрузку на систему. Кроме того, установив этот переключатель, вы удлините время жизни;
- **Set Time To Live (TTL) of object** in cache **to** — если требуется нестандартная политика устаревания HTTP-объектов.

4. Если вы установили переключатель в положение **Set Time To Live (TTL) of object in cache to,** требуется дополнительная настройка:
   - чтобы объекты считались устаревшими по истечении определенного времени, исчисляемого как процент от их возраста, введите необходимое значение в текстовом поле **This percentage of content age (Time since creation or modification);**
   - чтобы указать минимальное и максимальное время, когда HTTP-объекты должны оставаться в кэше:
     - в текстовом поле No **less than** (не менее) введите значение и выберите единицу времени в соответствующем раскрывающемся списке — **Seconds** (секунды), **Minutes** (минуты), **Hours** (часы), **Days** (дни) или **Weeks** (недели);
     - в текстовом поле No **more than** (не более) введите число и выберите единицу времени в соответствующем раскрывающемся списке.
5. Щелкните кнопку **OK.**

Примечание Чтобы восстановить параметры политики устаревания HTTP-объектов по умолчанию, щелкните кнопку **Restore Defaults.**

Кэширование FTP-объектов

ISA-сервер предоставляет механизм управления кэшированием FTP-объектов. Вы вправе по своему выбору включать и отключать кэширование, а также устанавливать время жизни для FTP-объектов (рис. 5-6).

По умолчанию время жизни всех FTP-объектов равно одному дню (1440 минут).

▶ **Настройка кэширования FTP-объектов**

1. В дереве консоли **ISA Management** щелкните правой кнопкой узел **Cache Configuration** и в контекстном меню выберите команду **Properties.**
2. На вкладке FTP установите флажок **Enable FTP caching.**
3. В текстовом поле **Time to Live for all objects** введите значение времени жизни для всех FTP-объектов.
4. В раскрывающемся списке выберите единицу измерения времени: **Seconds** (секунды), **Minutes** (минуты), **Hours** (часы), **Days** (дни) или Weeks (недели).
5. Щелкните кнопку OK.

Примечание Чтобы восстановить параметры политики кэширования FTP по умолчанию, щелкните кнопку **Restore Defaults.**

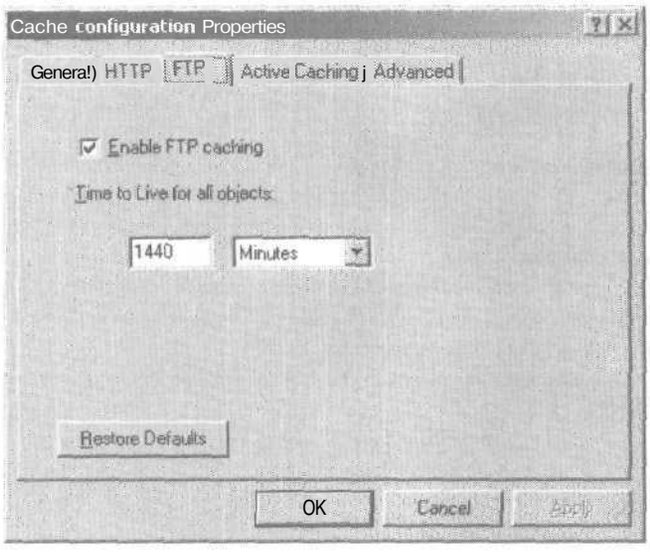


Рис. 5-6. Конфигурация кэширования FTP-объектов

Возвращение просроченных объектов

Для хранимых в кэше объектов устанавливается время жизни (TTL). По истечении TTL объект становится недействительным. Когда клиент запрашивает объект, ISA-сервер проверяет, действительна ли хранящаяся в кэше версия объекта. Если да, объект возвращается клиенту. В противном случае дальнейшее поведение ISA-сервера определяется политиками кэширования — запрашивается объект с указанного Web-сервера или нет.

Если Web-сервер доступен, ISA-сервер извлекает объект и возвращает его клиенту. Если Web-сервер недоступен, вы вправе настроить ISA-сервер на возвращение просроченных копий объектов из кэша.

Возвращение просроченных объектов из кэша включается на вкладке **Advanced** диалогового окна **Cache Configuration Properties** (рис. 5-7).

► **Настройка для возвращения просроченных объектов из кэша**

1. В дереве консоли **ISA Management** щелкните правой кнопкой узел **Cache Configuration** и в контекстном меню выберите команду **Properties.**
2. На вкладке **Advanced** установите переключатель в одно из следующих положений:
   - **Do not return the expired object (return an error page)** — вместо просроченного объекта будет возвращаться сообщение об ошибке;
   - **Return the expired object only if expiration was** — просроченная копия объекта будет возвращаться из кэша ISA-сервера.
3. Если вы выбрали возвращение просроченных объектов, укажите время жизни объекта:
   - в текстовом поле **At less than this percentage of original Time to live** укажите максимальный процент TTL. Если время существования объекта превысит его, объект не возвращается;
   - в текстовом поле **But no more than (minutes)** — укажите верхний предел времени (в минутах), которое должно пройти с момента, когда объект стал недействительным. Если время существования объекта превысит данный предел, объект не возвращается.
4. Щелкните кнопку **OK.**

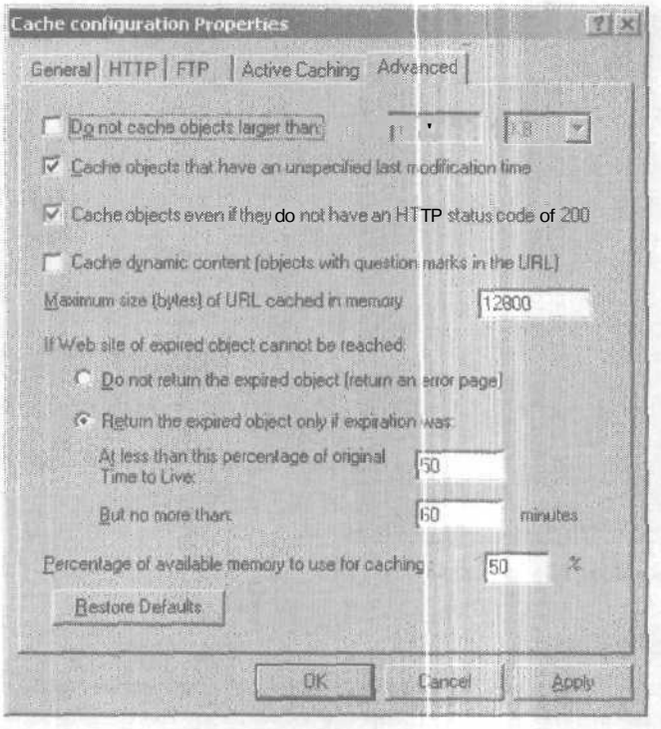


Рис. 5-7. **Вкладка Advanced окна** Cache **Configuration Properties**

Настройка активного кэширования

При включенном активном кэшировании ISA-сервер анализирует объекты в кэше и определяет, какие из них запрашиваются наиболее часто. Если срок действия популярного объекта в кэше подходит к концу, ISA-сервер автоматически обновляет копию в кэше.

Если связь с Интернетом осуществляется по телефонной линии, выполняя активное кэширование, компьютер автоматически соединится с интернет-провайдером для загрузки содержимого.

При настройке политики активного кэширования выберите одну из следующих возможностей:

- **Frequently** — предусматривается обязательное обновление объектов кэша, что обеспечивает постоянную актуальность объектов;
- **Normally** — вариант, устанавливаемый по умолчанию и обеспечивающий сбалансированный подход. Объекты обновляются достаточно часто, при этом обеспечивается достаточная производительность сети;
- **Less Frequently** — в кэш загружаются часть популярных объектов. Несмотря на **то,** что вероятность нахождения свежего объекта в кэше мала, сетевая производительность повышается, так как активное кэширование минимально.

▶ **Настройка активного кэширования**

1. В дереве консоли **ISA Management** щелкните правой кнопкой узел **Cache Configuration** и в контекстном меню выберите команду **Properties.**

2. На вкладке активного кэширования Active Caching установите флажок Enable active caching, чтобы включить активное кэширование.
3. Установите переключатель в одно из следующих положений:
   - Frequently — если ISA-сервер должен обновлять и продлевать действие кэшированных ранее объектов до их устаревания;
   - Normally — если требуется обеспечить баланс между быстрой реакцией и минимизацией сетевой нагрузки;
   - Less Frequently — если необходимо снизить нагрузку на сеть.
4. Щелкните кнопку OK.

Настройка кэширования отрицательных ответов

Существует возможность кэширования отрицательных ответов в тех случаях, когда ISA-серверу не удается загрузить нужные объекты с определенного Web-сервера. Это называется *кэшированием отрицательных ответов* (negative caching). Для настройки отрицательных ответов укажите, какие ответы-ошибки на запросы клиентов следует кэшировать.

Настройка этого типа кэширования заключается в указании ISA-серверу, как кэшировать HTTP-объекты с кодами состояния 203, 300, 301 и 410,

► Настройка кэширования отрицательных ответов

1. В дереве консоли ISA Management щелкните правой кнопкой узел Cache Configuration и в контекстном меню выберите команду **Properties.**
2. На вкладке Advanced установите флажок cache objects even if they do not have an HTTP status code of 200 (кэшировать объекты, даже если их HTTP-код состояния отличается от 200).
3. Щелкните кнопку OK,

Практикум 1. Включение активного кэширования

Активное кэширование позволяет ISA-серверу автоматически инициировать обновления копий в кэше наиболее часто запрашиваемых объектов. При включенном активном кэшировании ISA-сервер анализирует содержащиеся в кэше объекты и определяет, к каким из них чаще всего обращаются клиенты.

Задание. Активизация активного кэширования

В этом задании вы включите активное кэширование с параметрами по умолчанию.

► Включение активного кэширования

1. В дереве консоли ISA Management последовательно раскройте узлы Servers And Arrays, MyArray и Cache Configuration.
2. Щелкните правой кнопкой узел **Cache Configuration** и в контекстном меню выберите команду **Properties.** Откроется диалоговое окно **Cache Configuration Properties.**
3. Перейдите на вкладку Active Caching.
4. Установите флажок Enable active caching. Под надписью Retrieve files (загрузить файлы) активизируется переключатель, установленный в положение Normally.
5. Щелкните кнопку OK.

Практикум 2. Настройка объема оперативной памяти для кэширования

ISA-сервер позволяет зарезервировать для кэширования определенную часть свободной физической памяти. Доступ к файлам в физической памяти выполняется намного быстрее, чем к файлам, хранящимся в дисковом кэше.

Задание. Изменение объема памяти, доступной для кэширования

В этом задании вы измените долю используемой для кэширования свободной оперативной памяти, установленной по умолчанию, — 50 % на 65 %.

▶ **Изменение используемого для кэширования объема доступной памяти**

1. В дереве консоли **ISA Management** последовательно раскройте узлы Servers **And Arrays, MyArray и Cache Configuration.**
2. Щелкните правой кнопкой узел **Cache Configuration** и в контекстном меню выберите команду **Properties.** Откроется диалоговое окно **Cache Configuration Properties.**
3. Перейдите на вкладку **Advanced.**
4. В текстовом поле **Percentage of free memory to use for caching** замените установленное по умолчанию значение 50 на 65.
5. Щелкните кнопку OK. Откроется окно ISA Server Warning с предупреждением и предложением выбрать из двух возможностей: сохранить изменения и перезапустить службы или сохранить изменения без перезапуска служб.
6. Установите переключатель в положение **Save the changes and restart the service(s),** чтобы сохранить изменения и перезапустить службы, и щелкните **OK.**

Резюме

Свойства кэша изменяются в диалоговом окне свойств узла **Cache Configuration** и на страницах свойств отдельных серверов, значки которых размещены в папке **Drives** консоли ISA Management.

Размер и местоположение кэша настраивается при помощи диалогового окна **Properties** отдельных кэширующих серверов.

Посредством диалогового окна **Cache Configuration Properties** настраивается порядок кэширования FTP- и HTTP-объектов, устанавливаются политики устаревания объектов, определяется, в каких случаях ISA-сервер возвращает кэшированные объекты, устанавливается объем доступной для кэширования оперативной памяти, включается активное кэширование и настраивается кэширование отрицательных ответов.

Занятие 3. Загрузка содержимого кэша по расписанию

Служба загрузки содержимого кэша по расписанию ISA-сервера позволяет планировать загрузку Web-содержимого из Интернета в кэш сервера. Загрузка содержимого выполняется фоновыми процессами.

Изучив материал этого занятия, вы сможете:

- ✓ создавать и настраивать задания загрузки содержимого в кэш ISA-сервера по расписанию.

Продолжительность занятия — около 25 минут.

Загрузка содержимого кэша по расписанию

Загрузка содержимого кэша по расписанию позволяет обновлять HTTP-содержимое в расчете на его запрос клиентами Web-прокси. При правильном использовании загрузка содержимого кэша ISA-сервера по расписанию снижает сетевую нагрузку и повышает общую производительность кэширования, не оказывая влияние на пропускную способность сети.

На рис. 5-8 показано, как начать создание нового задания загрузки содержимого по расписанию в оснастке ISA Management.

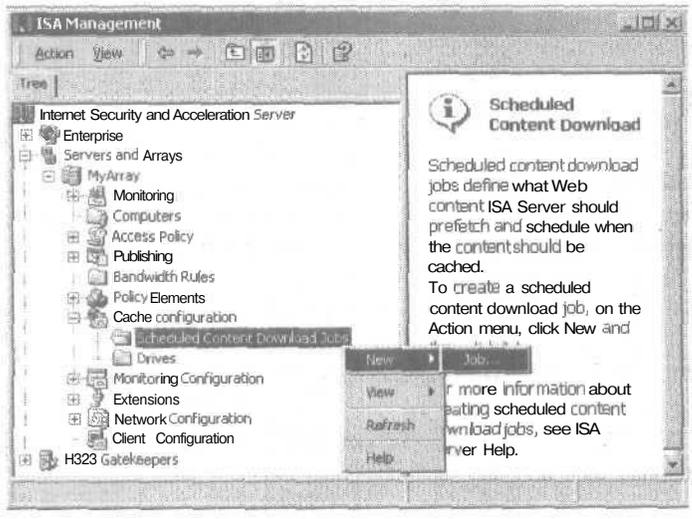


Рис. 5-8. Создание задания загрузки содержимого по расписанию

Автоматическое обновление содержимого кэша

Отслеживая и анализируя обращения клиентов к ресурсам в Интернете, можно определить, какая информация и в какое время им нужна. Механизм загрузки содержимого кэша по расписанию позволяет загружать HTTP-содержимое в кэш ISA-сервера по требованию или по расписанию. Он позволяет обновлять кэш ISA-сервера, загружая содержимое, которое, как предполагается, потребуется клиентам. После загрузки содержимое становится доступно из кэша, поэтому обращаться к узлу в Интернете не придется.

По расписанию разрешается загружать информацию как с одного, так и нескольких узлов, причем не частично, а, если необходимо, целого узла. Создавая задание загрузки содержимого по расписанию, вы вправе задать ограничение. Например, загружать содержимое только из одного домена. Аналогично ограничивается перечень ссылок, по которым выполняется автоматическая загрузка.

• Задания загрузки содержимого по расписанию создаются при помощи соответствующего мастера, его окно показанного на рис. 5-9.

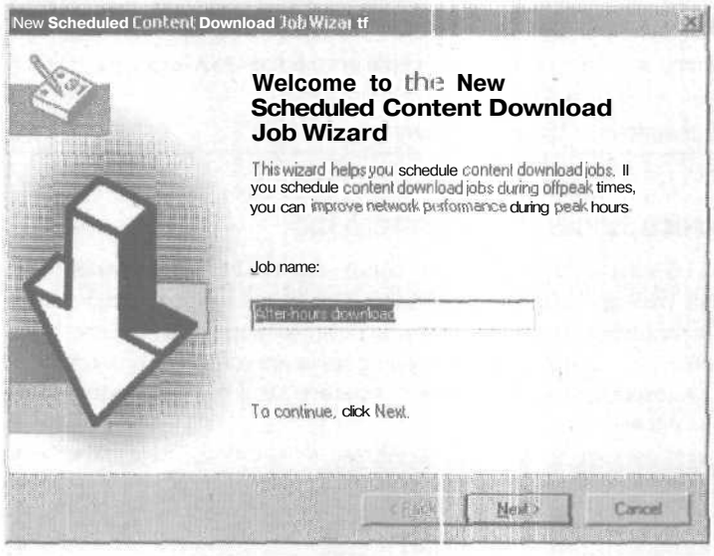


Рис. 5-9. Мастер создания нового задания загрузки содержимого по расписанию

▶ **Задание загрузки содержимого по расписанию**

1. В дереве консоли ISA Management откройте папку Cache Configuration, щелкните правой кнопкой папку **Scheduled Content Download Jobs** (задания загрузки содержимого по расписанию) и в контекстном меню последовательно выберите New и Job.
2. Последовательно выполняйте инструкции мастера.

Настройка свойств существующих заданий загрузки

Вы вправе изменять свойства существующих заданий загрузки. Для этого в консоли **ISA Management** выберите папку **Scheduled Content Download Jobs,** в области сведений щелкните правой кнопкой мыши задание загрузки и в контекстном меню выберите команду **Properties** (рис. 5-10).

▶ **Изменение местоположения, из которого загружается содержимое кэша**

1. В дереве консоли ISA Management выберите папку **Scheduled Content Download Jobs.**
2. В области сведений шелкните правой кнопкой существующее задание загрузки содержимого и в контекстном меню выберите команду **Properties.**
3. На вкладке **Parameters** в текстовом поле **Begin Downloading from URL** введите URL-адрес, с которого следует выполнять загрузку.
4. Чтобы загрузить содержимое только с домена, указанного в текстовом поле **Begin Downloading from URL** (не выполняя загрузку с других URL-адресов), установите флажок **Keep download process inside URL domain only.**

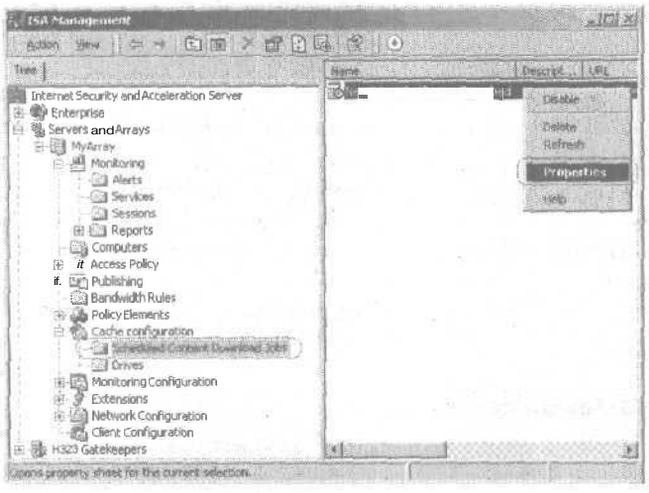


Рис. 5-10. Открытие страницы свойств существующего задания загрузки содержимого по расписанию

5. Чтобы ограничить глубину переходов по ссылкам с одной страницы, установите флажок **Cache up to maximum links depth of и в** соответствующем текстовом поле укажите глубину загрузки.
6. Чтобы ограничить общее число кэшируемых объектов, в текстовом поле **Maximum number of cached objects** введите верхнюю границу числа объектов.
7. Щелкните кнопку OK.

► **Настройка времени жизни загруженного содержимого в кэше**

1. В дереве консоли ISA Management выберите папку **Scheduled Content Download Jobs.**
2. В области сведений щелкните правой кнопкой существующее задание загрузки содержимого, в контекстном меню выберите команду **Properties** и перейдите на вкладку **Parameters.**
3. Чтобы переопределить установленное время жизни объекта, установите флажок **Always override object's TTL.**
4. Чтобы установить время жизни для объектов, у которых оно не определено, пометьте флажок **Override TTL if not defined.**
5. Чтобы задать особое значение времени жизни для загружаемых объектов, введите число минут в текстовом поле **Mark downloaded objects with a new TTL of** *<число>* **minutes.**
6. Щелкните кнопку OK.

Примечание Когда установлен флажок **Always override object's TTL,** время жизни объектов определяется значением TTL, указанным в поле **Downloaded objects with a new TTL of** *<число>* **minutes** или в свойствах конфигурации кэша.

Загрузка динамического содержимого

Создавая задание загрузки содержимого по расписанию, вы вправе включить кэширование динамического содержимого. В этом случае кэшируются даже те объекты, заголовки управления HTTP-кэшированием которых указывают на необязательность их кэширования.

Внимание! Если Web-сервер, с которого загружается объект, требует аутентификации клиента, задание загрузки содержимого по расписанию выполнено не будет.

▶ **Настройка кэширования динамического содержимого для заданий загрузки содержимого по расписанию**

1. В дереве консоли ISA Management выберите папку **Scheduled Content Download Jobs.**
2. В области сведений щелкните правой кнопкой существующее задание загрузки содержимого, в контекстном меню выберите команду **Properties. В** открывшемся диалоговом окне свойств перейдите на вкладку **Parameters.**
3. На вкладке **Parameters** установите флажок **Cache dynamic content.**
4. Щелкните кнопку **OK.**

Настройка расписания задач загрузки содержимого

Загрузка выполняется по заранее определенному расписанию, можно также задать периодичность выполнения задания. Задачи загрузки содержимого по расписанию создаются как для исходящих, так и для входящих Web-запросов.

Для исходящих Web-запросов сначала определяется, какие объекты в Интернете наиболее часто запрашиваются пользователями, а затем планируются задания, которые загружают объекты из Интернета и сохраняют их в кэше.

Для входящих Web-запросов планируются задания, загружающие содержимое с внутренних Web-серверов.

▶ **Настройка расписания задания загрузки содержимого**

1. В дереве консоли ISA Management выберите папку **Scheduled Content Download Jobs.**
2. В области сведений щелкните правей кнопкой существующее задание загрузки содержимого и в контекстном меню выберите команду **Properties.**
3. На вкладке определения периодичности **Frequency** в области **Start downloading в** поле даты **Date** и поле времени **Time** установите дату и время загрузки содержимого.
4. В области **Frequency** установите переключатель в одно из следующих положений:
   - **Once** — чтобы выполнить однократную загрузку содержимого в установленное время;
   - **Daily** — чтобы загружать содержимое ежедневно в установленное время;
   - Weekly on — чтобы загружать содержимое еженедельно в установленное время и в день (или дни), выбираемый установкой соответствующего флажка.
5. Щелкните кнопку OK.

Практикум. Создание задания загрузки содержимого по расписанию

Сейчас вы создадите задание загрузки содержимого по расписанию, которое выполняется каждое воскресенье в 23 часа 59 минут. Еженедельный график выполнения задания выбран в данном случае, так как содержимое не изменяется каждый день.

Задание. Создание задания загрузки онлайновых семинаров Microsoft по расписанию

Сейчас вы создадите задание на загрузку обучающих материалов с Web-узла Microsoft, в том числе и динамического содержимого, причем число объектов не должно превышать 5000.

▶ **Создание задания загрузки содержимого по расписанию**

1. В дереве консоли ISA Management последовательно раскройте узлы Servers **And Arrays, MyArray и Cache Configuration.**
2. Раскройте узел **Cache Configuration.**
3. Щелкните правой кнопкой папку **Scheduled Content Download Jobs**, в контекстном меню последовательно выберите New и Job.
4. На первой странице мастера New Scheduled Content Download Job в текстовом поле имени задания **Job Name** введите **Microsoft Online Seminars** и щелкните кнопку **Next.**
5. На странице **Start Time** оставьте дату неизменной, установите время **23:59:59** и щелкните **Next.**
6. На странице **Frequency** установите переключатель в положение **Weekly on,** пометьте флажок **Sunday** (воскресенье) и щелкните кнопку Next.
7. На странице **Content** в текстовом поле **Download content from this URL** введите **http://www.microsoft.com/seminar/1033/.**
8. Установите флажок **Cache dynamic content.**
9. Щелкните кнопку **Next.**
10. На странице **Links And Downloaded Objects** в текстовом поле **Maximum number of cached objects** (максимальное число кэшированных объектов) введите 5000 и щелкните кнопку Next.
11. На странице **Completing the Scheduled Content Download Job Wizard** щелкните кнопку **Finish.**
12. Щелкните папку **Scheduled Content Download Jobs.**

    В области сведений должно отобразиться задание **Microsoft Online Seminars.**

Резюме

Загрузка содержимого по расписанию позволяет обновлять в кэше ISA-сервера объекты, которые, как полагают, будут запрошены клиентами Web-прокси. Отслеживая и анализируя обращения клиентов к ресурсам в Интернете, можно определить, какая информация и в какое время им нужна. Для настройки заданий загрузки Web-содержимого в кэш ISA-сервера используется мастер New Scheduled Content Download Job. Задания загрузки содержимого выполняются однократно или регулярно по определенному расписанию. Создавая задание загрузки содержимого по расписанию, вы можете настроить ISA-сервер на загрузку как информации с одного, так и с нескольких узлов, причем как частично, так и полностью.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Ответы *для* самопроверки — в приложении А «Вопросы и ответы» в конце книги.

1. Клиент Web-прокси запрашивает Web-объект, ISA-сервер ищет копию этого объекта в своем кэше и обнаруживает, что она просрочена. Согласно правилу маршрутизации, ISA-сервер обращается за объектом к узлу в Интернете, который оказывается недоступным, Каковы дальнейшие действия ISA-сервера?

2. Как ISA-сервер определяет, нужно ли кэшировать полученный из оригинального источника Web-объект?

3. При каких условиях ISA-сервер кэширует динамическое содержимое?

4. Что такое кэширование отрицательных ответов и как оно включается?

5. Как ISA-сервер выполняет загрузку содержимого по расписанию, если сервер-источник требует выполнять аутентификацию клиента?

ГЛАВА 6

Безопасная публикация серверов

Занятие 1. Особенности безопасной публикации серверов 180
Занятие 2. Безопасная публикация Web-серверов 187
Занятие 3. Публикация почтового сервера 196
Закрепление материала 202

В этой главе

Если в сети есть серверы, публикующие информацию в Интернете, такие как Web- и FTP-серверы или серверы базы данных, необходимо предоставлять доступ к ним внешним клиентам, не ставя под угрозу безопасность сети. ISA-сервер обеспечивает безопасную публикацию таких серверов — он обрабатывает запросы извне от имени серверов внутренней сети. Полученные запросы ISA-сервер по мере необходимости безопасно переправляет на соответствующие серверы. Запросы, пересылка которых не разрешена явно, ISA-сервер по умолчанию отбрасывает.

Прежде всего

Для изучения материалов этой главы необходимо выполнить все упражнения в главах 1–5.

Занятие 1. Особенности безопасной публикации серверов

При обработке входящих запросов на серверы внутренней сети на ISA-сервере применяется механизм *публикации серверов*. Запросы пересылаются на сервер, который расположен во внутренней сети, защищенной ISA-сервером.

Публикация серверов осуществляется путем определения правил публикации серверов, которые создаются с помощью мастера New Server Publishing Rule в оснастке ISA Management. Существующее правило публикации сервера изменяется в диалоговом окне свойств правил в оснастке ISA Management.

Изучив материал этого занятия, вы сможете:

- ✓ публиковать серверы внутренней сети, защищенной ISA-сервером;
- ✓ безопасно публиковать серверы на компьютере ISA-сервера;
- ✓ безопасно публиковать серверы, расположенные в сети периметра.

Продолжительность занятия — около 35 минут.

Правила политики публикации

Для управления публикацией на ISA-сервере определяются политики публикации, которые состоят из правил публикации серверов и правил Web-публикации. Правила публикации серверов применяются для фильтрации всех входящих запросов и дальнейшего их перенаправления на соответствующие серверы, защищенные службами ISA-сервера. Для перенаправления Web-запросов извне на серверы внутренней сети применяются правила Web-публикации.

ISA-сервер устанавливается в одном из трех возможных режимов: брандмауэра (Firewall), сервера кэширования (Cache) или смешанном (Integrated). От выбранного режима зависит перечень доступных правил политики публикации, как показано в таблице 6-1.

Таблица 6-1. Доступность правил политик публикации в зависимости от режима ISA-сервера

Тип правила	Брандмауэр	Сервер кэширования	Смешанный
Правила Web-публикации	Нет	Да	Да
Правила публикации серверов	Да	Нет	Да

Правила публикации серверов

Теперь можно безопасно публиковать в Интернете компьютеры, расположенные во внутренней сети. Безопасность не нарушается, так как все входящие запросы и исходящие ответы проходят через ISA-сервер. В качестве внешнего IP-адреса внутреннего сервера публикуется внешний адрес ISA-сервера. Удаленные пользователи взаимодействуют с ISA-сервером и обращаются по его IP-адресу. Получив запрос, ISA-сервер пересылает его от имени пользователя на соответствующий опубликованный сервер во внутренней сети. Другими словами, связь внешних пользователей с безопасно опубликованными серверами выполняется через ISA-сервер.

По существу, правила публикации серверов фильтруют все запросы, проходящие через ISA-сервер, и пересылают их на соответствующие серверы за ISA-сервером. Правила предоставляют пользователям Интернета доступ к соответствующему публикующему серверу динамически (только при необходимости).

Опубликованный сервер — это клиент протокола *безопасного преобразования сетевых адресов* (SecureNAT); устанавливать и запускать на нем клиент брандмауэра не требуется. По этой же причине после создания правила публикации на ISA-сервере не нужно дополнительно конфигурировать публикующий сервер. Тем не менее следует иметь в виду, что в качестве основного шлюза на опубликованном сервере следует указать IP-адрес, назначенный интерфейсу адаптера ISA-сервера, подключенному ко внутренней сети.

Механизм публикации серверов

ISA-сервер обрабатывает запросы, направленные на опубликованные серверы, в определенной последовательности.

1. Клиентский компьютер в Интернете запрашивает объект, расположенный по IP-адресу публикующего сервера. Этот IP-адрес фактически относится к ISA-серверу — это адрес его внешнего интерфейса.
2. ISA-сервер обрабатывает запрос, пересылая его по IP-адресу внутреннего сервера от имени внешнего клиента.
3. Внутренний сервер возвращает нужный объект ISA-серверу, который в свою очередь пересылает его клиенту.

▶ Создание правила публикации сервера

1. В дереве консоли ISA Management раскройте узел **Publishing,** щелкните правой кнопкой мыши папку Server **Publishing Rules,** выберите команду New, а затем щелкните **Rule.**
2. На первой странице мастера **New Server Publishing Rule** введите имя правила публикации сервера и нажмите кнопку Next.
3. На странице **Address Mapping** (рис. 6-1) введите IP-адрес публикуемого внутреннего сервера, а также внешний IP-адрес ISA-сервера.

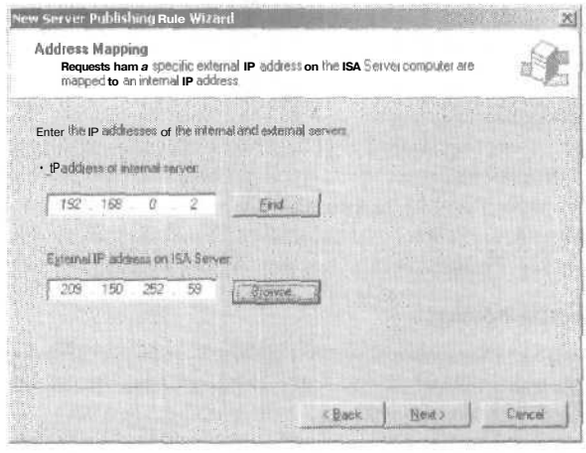


Рис. 6-1. Сопоставление адресов для публикации сервера

4. На странице **Protocol Settings** (рис. 6-2) выберите протокол сервера, к которому относится правило.

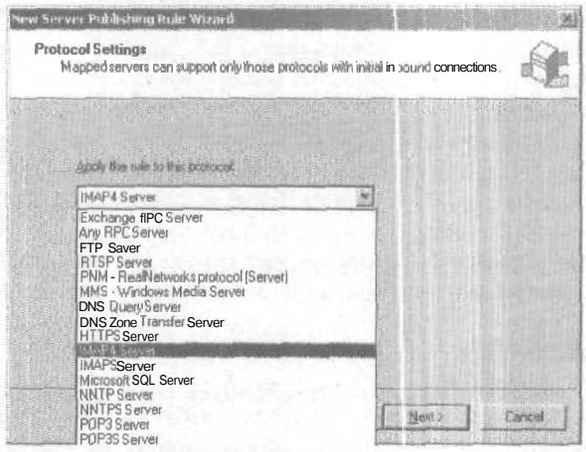


Рис. 6-2. Выбор протокола для публикации сервера

5. На странице **Client Type** определите, к каким клиентам применяется правило — ко всем или только к определенному подмножеству.

Примечание В массивах, в которых политика предприятия запрещает публикацию серверов, нельзя создать правило публикации.

Действия для правил публикации серверов

Действие для правила — это процедура, применяемая по отношению к запросу, который соответствует критериям этого правила. Действие для нового правила публикации серверов обычно конфигурируются на страницах **Address Mapping и Protocol Setting** мастера New Server Publishing Rule. Модификация действий для существующего правила выполняется в оснастке ISA Management на вкладке **Action** страницы свойств соответствующего правила. Но в любом случае вы должны указать ряд параметров действия:

- **IP-адрес ISA-сервера** — адрес, по которому опубликованный сервер доступен внешним клиентам;
- **IP-адрес опубликованного сервера** — IP-адрес, на который ISA-сервер пересылает все запросы, адресованные опубликованному серверу;
- **протокол, сопоставленный серверу** — состав данных, пересылаемых на внутренний сервер, определяется протоколом, который выбирается из перечня всех определений протоколов, настроенных на ISA-сервере, причем нужно определить протоколы хотя бы для входящих (Inbound) подключений. Перечень определений протоколов доступен для просмотра и редактирования в папке **Protocol Definitions** узла **Policy Elements**.

Пример определения действия для правила

Допустим, внешним клиентам требуется предоставить доступ к **SMTP-серверу,** IP-адрес и порт прослушивания которого — соответственно И 1.111.111.111 и 25. Для этого нужно создать правило публикации сервера и указать следующее:

- внутренний IP-адрес сервера — 111.111.111.111;
- внешний адрес ISA-сервера — IP-адрес внешнего интерфейса адаптера на компьютере ISA-сервера;
- набор протоколов, сопоставленных SMTP-серверу.

▶ **Редактирование действия для существующего правила публикации сервера**

1. В дереве консоли ISA Management откройте узел **Publishing** и щелкните папку **Server Publishing Rules.**
2. В меню View отметьте команду **Advanced.**
3. В области сведений щелкните правой кнопкой мыши нужное правило публикации сервера и в контекстном меню выберите команду **Properties.**
4. На вкладке **Action,** в текстовом поле **IP address of internal server** введите адрес внутреннего сервера, доступ к которому следует предоставить внешним пользователям.
5. В текстовом поле **External IP Address on ISA Server** введите IP-адрес одного из внешних интерфейсов сетевого адаптера ISA-сервера, через который планируется предоставлять доступ внешним клиентам.

Примечание **В** поле со списком **Mapped server protocol** выберите определение протокола, который будет использоваться внешними клиентами для доступа к опубликованному компьютеру.

Подмножества адресов клиентов

В процессе конфигурирования правила публикации сервера администратор может определить, что правило применяется лишь к определенному подмножеству клиентских компьютеров. Последние задаются не на публикуемом сервере, а в узле **Policy Elements** оснастки ISA Management.

▶ **Определение подмножества клиентов для существующего правила публикации сервера**

1. В дереве консоли ISA Management разверните узел **Publishing** и щелкните папку **Server Publishing Rules.**
2. В меню View выберите команду **Advanced.**
3. В области сведений щелкните правой кнопкой мыши нужное правило и выберите в контекстном меню команду **Properties.**
4. На вкладке **Applies To** определите подмножество клиентов, к которым планируется применять правило:
   - установите переключатель в положение **Any request,** чтобы применять правило ко всем запросам;
   - установите переключатель в положение **Client addresssets specified below,** чтобы применить правило к определенному подмножеству клиентов.
5. В последнем случае следует выполнить следующие операции:
   - чтобы добавить клиент к списку **Applies to requests coming from** (применяется к запросам от...), щелкните соответствующую кнопку Add;
   - чтобы добавить клиент к списку исключений **Exceptions,** щелкните соответствующую кнопку Add.

Примечание В правилах публикации серверов в качестве клиентских адресов обычно используются адреса компьютеров в Интернете.

Правила публикации серверов и фильтры IP-пакетов

Как правила публикации серверов, так и фильтры IP-пакетов открывают определенные порты для связи между локальной сетью и Интернетом. В большинстве случаев правила публикации серверов позволяют предоставить доступ внешним пользователям к серверам внутренней сети.

Однако в некоторых случаях следует применять фильтры IP-пакетов, а не правила публикации серверов:

- при публикации серверов, расположенных в сети периметра;
- при публикации служб, расположенных на самом ISA-сервере.

Публикация серверов в сети периметра

Для публикации серверов, расположенных в локальной сети, и предоставления доступа к ним внешних клиентов применяются правила публикации серверов. Например, для публикации внутреннего FTP-сервера. Б этом случае следует просто создать правило публикации сервера следующим образом:

- в качестве IP-адреса внутреннего сервера указать IP-адрес FTP-сервера;
- в качестве внешнего адреса ISA-сервера указать IP-адрес внешнего интерфейса адаптера на компьютере ISA-сервера;
- выбрать для правила протокол FTP;
- при выборе подмножества клиентов предоставить доступ к FTP-серверу всем клиентам, установив переключатель в положение **Any request.**

Однако, если публикуемый сервер расположен в сети периметра, а не в локальной сети, для открытия порта на сервере придется воспользоваться фильтрами IP-пакетов. Допустим, вы хотите опубликовать FTP-сервер, расположенный в сети периметра. Воспользуйтесь мастером New IP Packet Filter для создания нового фильтра IP-пакетов и настройте его следующим образом:

- на странице **Servers** укажите, что фильтр устанавливается для всех ISA-серверов массива **(All ISA Servers computers in the array);**
- на странице **Filter Mode** отметьте разрешающий фильтр **Allow packet transmission;**
- на странице **Filter Type** выберите пользовательский фильтр **Custom;**
- на странице **Filter Settings** присвойте параметрам следующие значения:
  - **IP Protocol — TCP;**
  - **Direction** (направление) — **Both** (двустороннее);
  - **Local Port Fixed** (фиксированный локальный порт) — 21;
  - **Remote Port** (удаленный порт) — **All Ports** (все порты);
- на странице **Local Computer** установите переключатель в положение **This computer (on the perimeter network),** чтобы определить компьютер в сети периметра, и в текстовом поле введите IP-адрес FTP-сервера;
- на странице **Remote Computers** установите переключатель в положение **All remote computers.**

Публикация сервера, расположенного на ISA-сервере

Для открытия порта и публикации сервера, который расположен на самом ISA-сервере, применяются фильтры IP-пакетов, а не правила публикации. В частности, на ISA-сервере предусмотрен стандартный фильтр IP-пакетов DNS Filter, который применяется, когда запросы DNS разрешаются на самом ISA-сервере.

Практикум. **Публикация** внугреннего **сервера**

Вы опубликуете службу FTP на сервере Server2. Для предоставления доступа внешним пользователям к службе FTP на Server2 на ISA-сервере следует создать правило, разрешающее пересылку запросов FTP-сервера.

Внимание! Это занятие предполагает наличие активного подключения к Интернету по телефонной линии, кроме того, все три следующих задания необходимо выполнять в течение одного сеанса связи.

До выполнения заданий следует остановить службу FTP на сервере Server1. Для этого в оснастке Internet Services Manager щелкните правой кнопкой мыши значок **Default FTP Site** (FTP-узел по умолчанию) и выберите команду **Stop** (Остановить).

Задание 1. Создание правила публикации на сервере Server1

Вы создадите правило публикации, которое разрешает пересылку всех FTP-запросов через ISA-сервер на сервер Server2. Выполните задание на сервере Server1.

1. Убедитесь, что Server1 подключен к Интернету через модем. Если подключение к Интернету не установлено, создайте его.
2. Откройте консоль ISA Management.
3. В дереве консоли разверните узел **MyArray** и перейдите к узлу **Publishing.**
4. Разверните узел **Publishing.**
5. Щелкните правой кнопкой мыши папку **Server Publishing Rules,** в контекстном меню перейдите к пункту New и затем выберите команду **Rule.** Откроется окно мастера New Server Publishing Rule.
6. В текстовом поле **Server Publishing Rule Name** введите **FTP Server** и щелкните кнопку Next.
7. На странице **Address Mapping** в текстовом поле **IP address of internal server** введите **192.168.0.2.**
8. Щелкните кнопку **Browse.** Откроется информационное окно, где указаны внешние адреса ISA-сервера.
9. Выберите внешний IP-адрес и щелкните кнопку OK. Этот внешний IP-адрес компьютера появится в текстовом поле **External IP address on ISA Server.** Следует иметь в виду, что это правило действует лишь на протяжении текущего сеанса связи через Интернет, так как IP-адрес, как правило, изменяется при каждом подключении к интернет-провайдеру.
10. Запишите или запомните внешний I P-адрес — он понадобится в следующих заданиях. Щелкните кнопку Next.
11. На странице **Protocol Settings** в поле со списком **Apply the rule to this protocol** выберите **FTP Server** и щелкните кнопку Next.
12. На странице **Client Type** оставьте без изменений установленное по умолчанию положение **Any Request** переключателя и щелкните кнопку **Next.**
13. На странице **Complete The New Server Publishing Rule** щелкните кнопку **Finish.**
14. Прежде чем перейти к заданию 2, перезапустите службу ISA-сервера средствами оснастки ISA Management.

Задание 2. Проверка публикации FTP-сервера

Вы подключитесь по протоколу FTP к JSA-серверу по его внешнему IP-адресу. Хотя опубликованный FTP-сервер установлен на внутреннем сервере Server2, а не на самом ISA-сервере, благодаря новому правилу публикации сервера, созданному в задании 1, для внешних пользователей FTP-сервер выглядит как размещенный на Serverl.

1. Войдите в систему сервера Serverl под учетной записью Administrator (Администратор).
2. В меню **Start** (Пуск) выберите команду Run (Выполнить). Откроется диалоговое окно Run (Выполнить).

3. В поле **Open** (Открыть) введите **cmd** и щелкните кнопку OK. Откроется окно командной строки.
4. В командной строке введите:

   ftp *<внешний_IP-адрес>*

   где *<внешний IP-адрес>* — это внешний IP-адрес ISA-сервера, назначенный интернет-провайдером, для которого вы определили правило публикации в задании 1. Вы записали его, выполняя операцию 10 задания 1 настоящего практикума.
5. Нажмите Enter. В окне консоли вы увидите сообщение, информирующее о подключении к FTP-серверу и предлагающее ввести имя пользователя. Наличие этого сообщения подтверждает, что новое правило публикации позволило подключиться из Интернета к службе FTP на сервере Server2.
6. В качестве имени пользователя укажите **anonymous**. Следующее сообщение проинформирует о возможности анонимного доступа и предложит ввести пароль.
7. Введите пустой пароль, просто нажав клавишу Enter. Откроется строка приглашения FTP.
8. В приглашении FTP введите команду **quit.** Система вернет вас в окно командной строки.
9. Закройте окно командной строки.

Резюме

Правила публикации серверов позволяют ISA-серверу обрабатывать входящие запросы, адресованные серверам во внутренней сети, таким как SMTP- и FTP-серверы и серверы баз данных. Вы можете опубликовать в Интернете практически любой компьютер внутренней сети. Безопасность не нарушается, так как все входящие запросы и исходящие ответы проходят через ISA-сервер. Подобно правилам узлов и информации, правила публикации серверов открывают TCP-порты для запросов служб динамически, то есть по мере необходимости.

При публикации ISA-сервером в качестве внешнего IP-адреса внутреннего сервера публикуется внешний адрес ISA-сервере. Удаленные пользователи взаимодействуют с ISA-сервером и обращаются по его IP-адресу, Получив запрос, ISA-сервер пересылает его от имени внешнего пользователя на соответствующий опубликованный сервер во внутренней сети. Для создания новых правил публикации серверов применяется мастер New Server Publishing Rule. Параметры существующих правил публикации серверов можно корректировать в диалоговых окнах свойств соответствующих правил в оснастке ISA Management.

Для публикации серверов, расположенных в сети периметра, или служб, размещенных на самом ISA-сервере, применяются фильтры IP-пакетов, а не правила публикации серверов.

Замятие 2, Безопасная публикация Web-серверов

ISA-сервер принимает запросы извне от имени опубликованных внутренних Web-серверов. Когда клиент Интернета запрашивает объект на опубликованном Web-сервере, запрос на самом деле направляется по внешнему адресу ISA-сервера. Перенаправление запросов на внутренний Web-сервер осуществляется на основании сконфигурированных на ISA-сервере правил публикации. Опубликованный Web-сервер не нуждается ни в никакой дополнительной настройке.

Для создания нового правила публикации Web-сервера применяется мастер New Web Publishing Rule. Существующие правила публикации Web-серверов можно корректировать в диалоговом окне свойств правил в оснастке ISA Management.

Изучив материал этого занятия, вы сможете:

- ✓ публиковать Web-серверы внутренней сети, защищенной ISA-сервером;
- ✓ безопасно публиковать Web-серверы на компьютере ISA-сервера.

Продолжительность занятия — около 45 минут.

Правила Web-публикации

Правила Web-публикации на ISA-сервере применяются для укрепления безопасности и предотвращения компрометации внутренней защиты сети при публикации информации в Интернете. Правила Web-публикации определяют, каким образом ISA-сервер обрабатывает входящие HTTP-запросы, адресованные внутреннему Web-серверу, и отвечает на них от имени Web-сервера. Правило определяет, какие запросы отбрасываются, а какие пересылаются далее на внутренний Web-сервер, расположенный в защищенной ISA-сервером сети. По возможности запросы выполняются с использованием информации из кэша ISA-сервера.

Внимание! Для укрепления защиты не разрешайте просмотр каталогов на опубликованном Web-сервере. По этой же причине не настраивайте Web-сервер на базовую аутентификацию или аутентификацию на основе хешей, В случае использования этих методов у внешних пользователей появляется возможность узнать внутреннее имя и/или IP-адрес Web-сервера.

Подмножества адресатов и клиентов

В процессе конфигурирования правил Web-публикации, например с помощью мастера New Web Publishing Rule (рис. 6-3), вам предлагается определить подмножество адресатов (серверов во внутренней сети), на которое распространяется правило. В правилах Web-публикации подмножества адресатов обычно состоят из доменных имен, которые сопоставляются IP-адресу ISA-сервера. В подмножестве адресатов разрешается также указывать полный или частичный путь, в этом случае правило управляет запросами на уровне отдельных каталогов или файлов. (Например, запросы по адресу *http://www.microsoft.com/example* могут перенаправляться на один внутренний сервер, а запросы *http://www.microsofl.com/marketing* — на другой.) Подмножества клиентов — это, как правило, адреса клиентов Интернета, а не клиентов внутренней корпоративной сети. Указанная группировка клиентов облегчает администрирование, так как доступ к опубликованному Web-серверу предоставляется или запрещается целым группам.

Подмножества адресатов и клиентов создаются и управляются в папках узла Policy Elements.

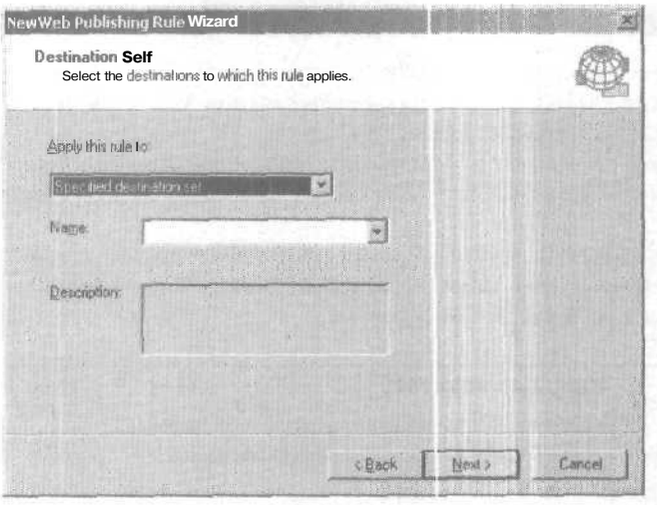


Рис. 6-3. Публикация подмножества внутренних адресатов

► **Создание правила Web-публикации**

1. В дереве консоли ISA Management раскройте узел **Publishing,** щелкните правой кнопкой мыши папку **Web Publishing Rules**, в контекстном меню перейдите к команде **New** и выберите **Rule.**
2. На первой странице мастера New **Web Publishing Rule** введите имя правила и щелкните кнопку Next.
3. На странице **Destination Sets** создайте подмножество адресатов, содержащее **IP-адрес** публикуемого сервера, и щелкните кнопку Next.
4. На странице **Client Type** определите, к каким клиентам применяется правило — ко всем пользователям или лишь к определенным подмножествам адресатов или клиентов, и щелкните кнопку **Next.**
5. На странице **Rule Action** определите порядок переадресации запросов.

Примечание В массивах, где политика предприятия запрещает публикацию серверов, нельзя создать правило публикации.

Действия для правил Web-публикации

Действия для правил Web-публикации настраиваются на странице **Rule Action** мастера New Web Publishing Rule (рис. 6-4). Правила предусматривают либо отбрасывание HTTP-запросов, адресованных определенным подмножествам адресатов, либо перенаправление запросов на другие узлы, например на Web-сервер в корпоративной сети.

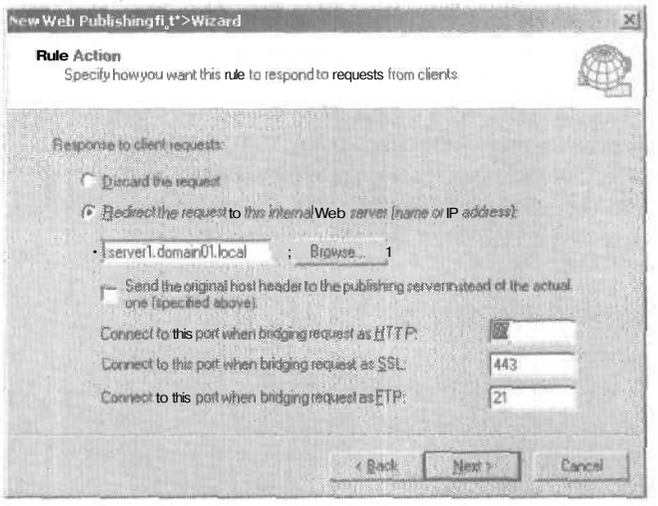


Рис. 6-4. Перенаправление **Web-запросов на внутренний сервер**

▶ **Настройка действия для существующего правила Web-публикации**

1. В дереве консоли ISA Management щелкните папку **Web Publishing Rules.**
2. В меню **View** отметьте команду **Advanced.**
3. В области сведений щелкните правой кнопкой мыши нужное правило публикации и выберите команду **Properties.**
4. На вкладке **Action** выполните одно из следующих действий:
   - чтобы отбрасывать запросы, установите переключатель в положение **Discard the request;**
   - чтобы перенаправлять запросы насервер(ы), публикуемые в Интернете,установите переключатель в положение **Redirect the requests to this internal Web** server **(name or IP address).**
5. В последнем случае выполните следующие операции:
   - введите IP-адрес или доменное имя, по которому следует перенаправлять запросы;
   - в текстовом поле **Connect to this port when bridging request as HTTP** введите номер порта для обслуживания запросов по HTTP. По умолчанию протокол HTTP сконфигурирован на порт 80;
   - в поле **Connect to this port when bridging request** as SSL введите номер порта для обслуживания запросов по *безопасному HTTP* (Secure Hypertext Transfer Protocol, S-HTTP). По умолчанию S-HTTP конфигурируется на порт 443;
   - в поле **Connect to this port when bridging request as FTP** введите номер портадля обслуживания запросов по FTP. По умолчанию FTP конфигурируется на порт 21.

SSL- и HTTP-сопряжение

На вкладке **Bridging** страницы свойств правила Web-публикации (рис. 6-5} настраивается порядок преобразования и переадресации HTTP-запросов — в виде обычных HTTP-запросов, по протоколу SSL (Secure Sockets Layer) или по протоколу FTP. Если запрос переадресуется в качестве SSL-запроса, пакеты шифруются.

Вы также вправе переадресовывать SSL-подключения. Другими словами, если в исходном подключении используется SSL, то после ISA-сервера на внутренний Web-сервер запрос можно переадресовать в виде HTTP, SSL или FTP. Такой механизм называется

сопряжением (bridging). При переадресации по SSL перед отправкой на Web-сервер ISA-сервер заново шифрует пакеты, то есть для связи с Web-сервером создается новый безопасный SSL-канал.

При перенаправлении HTTP- или SSL-запросов в виде FTP ISA-сервер пересылает их запросы на внутренний Web-сервер ло стандартному протоколу FTP, причем вам предоставляется возможность определить, какой порт следует использовать для пересылки.

Наконец, если внутренний Web-сервер требует предъявлять клиентский сертификат, ISA-сервер обычно настраивается на аутентификацию с применением определенного сертификата клиента.

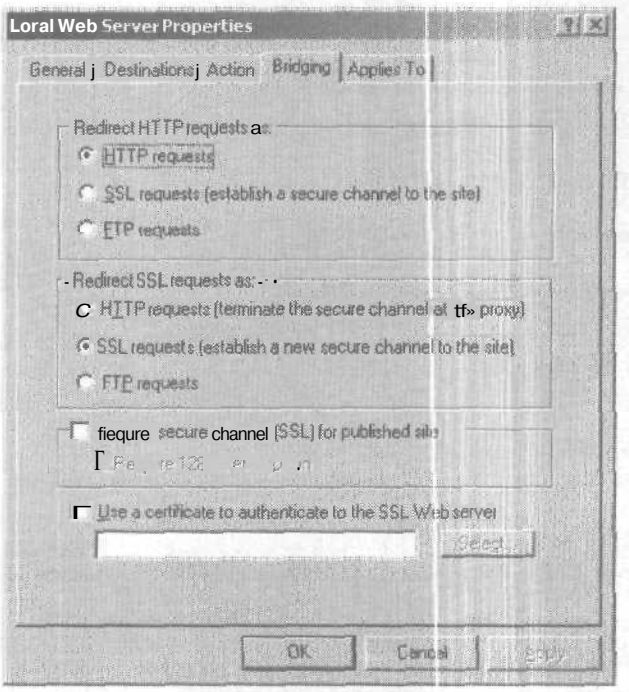


Рис. 6-5. Конфигурирование свойств сопряжения для правила Web-публикации

Порядок выполнения правил

Входящие Web-запросы обрабатываются правилами Web-публикации в определенном порядке. Если существует правило, которому соответствует запрос, он перенаправляется и кэшируется в соответствии с правилом.

Если правила, связанного с запросом, нет, ISA-сервер применяет правило по умолчанию, которое отбрасывает запрос. Последовательность, в которой выполняются два и более правил Web-публикации, определяется администратором.

Правило Web-публикации по умолчанию

В процессе установки ISA-сервера автоматически конфигурируются правила Web-публикации по умолчанию, которые настроены на отбрасывание всех запросов. Правило Web-публикации по умолчанию выполняется последним в перечне других правил, кроме того его нельзя изменить.

▶ **Изменение порядка следования правил Web-публикации**

1. В дереве консоли ISA Management щелкните папку **Web Publishing Rules.**
2. В меню **View** выберите команду **Advanced.**
3. В области сведений щелкните правой кнопкой мыши правило, порядок выполнения которого нужно изменить, и в контекстном меню выберите команду **Move Up** (чтобы переместить правило вверх) или **Move Down** (чтобы переместить правило вниз).
4. При необходимости повторите операцию 3 несколько раз, чтобы добиться нужного порядка правил.

Примечание Положение правила по умолчанию изменить нельзя.

Пример создания правила Web-публикации

Допустим, в домене example.microsoft.com нужно опубликовать два внутренних Web-сервера — Dev и Mktg. IP-адрес домена example.microsoft.com соответствует внешнему интерфейсу ISA-сервера, однако клиентские запросы по адресу example.microsoft.com/Marketing должны перенаправляться на внутренний сервер Mktg, а запросы по адресу example.microsoft.com/Development — на внутренний сервер Dev.

Для решения поставленной задачи создайте два подмножества адресатов: первый назовите Marketing, включите в него компьютер с доменным именем example.microsoft.com и определите путь /Marketing/*, а второй назовите Development, включите в него компьютер example.microsoft.com и определите путь /Development/*.

Далее создайте два правила Web-публикации, которые переадресуют запросы на соответствующие внутренние Web-серверы. Определите параметры первого правила Web-публикации следующим образом:

- в **Destination Set** укажите подмножество **Marketing;**
- установите переключатель в положение **Any request;**
- настраивая действия, в **Redirect request to this internal Web server (name or IP address)** определите **Mktg** в качестве узла для перенаправления.

Когда клиент запросит объект, расположенный по адресу example.microsoft.com/Marketing, ISA-сервер перешлет запрос на Mktg/Marketing.

Определите параметры второго правила Web-публикации следующим образом:

- **в Destination Set** задайте подмножество **Development;**
- установите переключатель в положение **Any request;**
- настраивая действия, в **Redirect request to this internal Web server (name or IP address)** определите Dev в качестве узла для перенаправления.

Когда клиент запросит объект, расположенный по адресу example.microsoft.com/Development, ISA-сервер перешлет запрос на Dev/Development.

Публикация Web-сервера, расположенного в локальной сети

▶ **Публикация внутреннего Web-сервера, расположенного ь сети, защищенной ISA-сервером**

1. Убедитесь, что на сервере DNS выбранное полное доменное имя сопоставлено внешнему IP-адресу ISA-сервера. При запросе информации клиенты Интернета используют доменное имя.
2. Настройте на ISA-сервере параметры обработки входящих Web-запросов. В качестве IP-адреса следует определить адрес внешнего интерфейса.

3. Создайте подмножество адресатов с именем Marketing, которое содержит компьютер example.microsoft.com и путь \Marketing*.
4. Создайте подмножество адресатов с именем Development, которое содержит компьютер example.microsoft.com и путь \Development*.
5. Создайте правило Web-публикации, определив следующие параметры:
   - в **Destination** Set задайте подмножество **Marketing;**
   - установите переключатель в положение **Any request;**
   - настраивая действия, в **Redirect request to this internalWeb server (name or IP address)** определите **Mktg** в качестве узла для перенаправления.
6. Создайте второе правило Web-публикации, определив следующие параметры:
   - в **Destination Set** задайте подмножество **Development;**
   - установите переключатель в положение Any request;
   - настраивая действия, в **Redirect request to thisinternal Web server (name or IP address)** определите Dev в качестве узла для перенаправления.

Публикация Web-сервера, расположенного на ISA-сервере

По умолчанию Web-серверы, так же как и ISA-сервер, в ожидании входящих запросов прослушивают порт 80. Это означает, что, если не изменить порт HTTP по умолчанию, возникнет конфликт между Web-сервером и расположенным на том же компьютере ISA-сервером. Для предотвращения этого следует сконфигурировать Web-сервер на прослушивание другого порта, после чего изменить правило Web-публикации на ISA-сервере на пересылку запросов на порт Web-сервера.

Например, Web-сервер можно сконфигурировать на прослушивание порта 9999 и создать правило Web-публикации со следующими параметрами:

- в **Destination Set** задать подмножество, содержащее IP-адрес ISA-сервера;
- при настройке действия установить **Redirect request to this internal Web server (name or IP** address) и указать имя компьютера Web-сервера и порт 9999.

Использование фильтров IP-пакетов для публикации Web-сервера, совмещенного с ISA-сервером

Другой способ публикации Web-сервера, расположенного на компьютере ISA-сервера, заключается в конфигурировании фильтров пакетов. В этом случае Web-сервер получает возможность использовать порт 80 для прослушивания входящих Web-запросов.

В данной ситуации конфликт при обработке исходящих запросов не возникает, так как ISA-сервер прослушивает порт 8080, а Web-сервер ожидает запросы от внутренних клиентов на порту 80. Однако при публикации Web-сервера на компьютере ISA-сервера следует проверить, не включена ли функция автоматического обнаружения ISA-серверов, которая прослушивает на порту 80; эта функция может конфликтовать с запросами от внутренних клиентов. Кроме того, так как порт 80 используется службой IIS, не следует в этом случае создавать правила Web-публикации.

▶ **Публикация Web-сервера, расположенного на компьютере ISA-сервера, с применением фильтра IP-пакетов**

1. Разрешите фильтрацию IP-пакетов, если она еще не включена.
2. Создавая фильтр IP-пакетов с помощью мастера, сконфигурируйте параметры следующим образом:
   - на странице **Servers** установите переключатель в положение **Only this server и** выберите локальный компьютер;

- на странице **Filter Mode** установите переключатель в положение **Allow packet transmission;**
- на странице **Filter Type** установите переключатель в положение Custom;
- на странице **Filter Settings** в поле со списком **IP Protocol** выберите TCP:
  - определите входящий трафик, выбрав **Inbound** в поле со списком **Direction;**
  - в области **Local Port** выберите **Fixed** и введите номер порта — 80;
  - в **Remote Port** (удаленный порт) щелкните **All ports;**
- на странице **Local Computer** выберите **This ISA server's external IP address;**
- на странице **Remote Computers** установите переключатель в положение **All remote computers.**

3. Отключите автоматическое обнаружение, если оно было включено, или перенастройте его на порт, отличный от 80. Указанные действия выполняются на вкладке **Auto Discovery** страниц свойств массива.

Практикум. Публикация Web-сервера, расположенного на компьютере ISA-сервера

Сейчас вы настроите Web-сервер, расположенный компьютере ISA-сервера. Для выполнения заданий требуется подключить сервер Server1 к интернет-провайдеру с помощью модема. Все задания выполняются в течении одного сеанса связи.

Задание 1. Настройка параметров обработки входящих Web-запросов

Вы настроите ISA-сервер на прослушивание входящих Web-запросов на порту 80.

1. Войдите в систему сервера Server1 под учетной записью Administrator (Администратор).
2. Подключитесь через модем к интернет-провайдеру, используя подключение, назначенное ISA-серверу.
3. Откройте оснастку ISA Management.
4. Щелкните правой кнопкой мыши узел **MyArray** и в контекстном меню выберите команду **Properties,** Откроется диалоговое окно свойств массива.
5. Перейдите на вкладку **Incoming Web Requests.**
6. В области **Identification** установите переключатель в положение **Use the same listener configuration for all IP addresses.**
7. Убедитесь, что в текстовом поле **Port TCP** установлено значение 80, и щелкните кнопку OK. Откроется информационное окно **ISA Server Warning.**
8. Установите переключатель в положение **Save the changes but don't restart the service(s)** и щелкните OK.

Задание 2. Создание подмножества адресатов для Web-сервера

Вы создадите подмножество адресатов и сопоставите его IP-адресу внешнего интерфейса сервера Server1. Это задание выполняется на Server1.

1. В оснастке ISA Management разверните узел **Policy Elements.**
2. Щелкните правой кнопкой мыши папку **Destination** Sets и в контекстном меню последовательно выберите команды New и Set. Откроется диалоговое окно определения нового подмножества адресатов **New Destination Set.**
3. В текстовом поле **Name** введите **External Interface.**
4. Щелкните кнопку Add. Откроется диалоговое окно **Add/Edit Destination.**

5. Выберите переключатель **IP Addresses.**
6. В текстовом поле **From** введите IP-адрес, назначенный интернет-провайдером для внешнего интерфейса на Server1. Если вы не знаете текущего IP-адреса, откройте окно командной строки и введите команду **ipconfig** — эта утилита предоставит адрес внешнего интерфейса. Следует иметь в виду, что создаваемое подмножество адресатов действительно лишь на протяжении текущего сеанса связи по телефонной линии.
7. Щелкните кнопку **OK,** чтобы завершить ввод IP-адрес адресата. Адрес отобразится в поле **Include these destinations** диалогового окна New **Destination Set.**
8. Щелкните кнопку **OK.**

Задание 3. Подготовка Web-узла

В этом задании вы создадите Web-узел на компьютере ISA-сервера и сконфигурируете его на прослушивание для Web-залросов на порту 9999.

1. Продолжая работу в системе Server 1 под учетной записью Administrator (Администратор), скопируйте файл\Exercises\Chapter6\default.htm *с* компакт-диска с материалами курса в папку C:\Inetpub\wwwroot на компьютере Server1.
2. В меню **Start** (Пуск) перейдите к **Administrative Tools** (Администрирование), а затем — к **Internet Services Manager.** Откроется окно оснастки **Internet Information Services.**
3. В дереве консоли **Internet Information Services** щелкните правой кнопкой мыши значок **Default Web Site** (Веб-узел по умолчанию) и в контекстном меню выберите команду **Stop** (Остановить). (Если, конечно, Web-узел по умолчанию уже не остановлен.)
4. Щелкните правой кнопкой мыши значок **Default Web Site** и в контекстном меню выберите команду **Properties** (Свойства), Откроется диалоговое окно **Default Web Site (Stopped) Properties** [Свойства: Веб-узел по умолчанию (Останов)]. Перейдите на вкладку **Web Site** (Веб-узел).
5. В текстовом поле **IP Address** (IP-адрес) введите **192.168.0.1.**
6. В текстовом поле **TCP Port** (TCP-порт) удалите 80 и введите **9999.**
7. Щелкните кнопку OK.
8. Щелкните правой кнопкой мыши значок **Default Web Site** и в контекстном меню выберите команду **Start** (Пуск).

Задание 4. Создание правила Web-публикации

В этом задании вы создадите правило Web-публикации, в соответствии с которым Web-запросы внешнего интерфейса на ISA-сервере пересылаются на внутренний Web-сервер на том же компьютере.

1. Продолжая работу в системе Serverl под учетной записью Administrator (Администратор), откройте окно оснастки **ISA Management.**
2. В дереве консоли разверните узел **Publishing.**
3. Щелкните правой кнопкой мыши папку **Web Publishing Rules** и в контекстном меню последовательно выберите команды New и **Rule,** Откроется окно мастера создания нового правила New Web Publishing Rule.
4. В текстовом поле **Web Publishing Rule Name** введите **Local Web Server** и щелкните кнопку Next.
5. На странице **Destination Sets в** поле со списком **Apply this rule to** выберите **Specified destination set.** На странице отобразится поле со списком **Name.**
6. В поле со списком **Name** выберите **External Interface** и щелкните кнопку Next.
7. На странице **Client Type** щелкните кнопку Next.

8. На странице установите переключатель в положение **Redirect the request to this internal Web** server **(name or IP address).**
9. В относящемся к выбранному переключателю текстовом поле введите **192.168.0.1.**
10. Очистите поле **Connect to this port when bridging request as HTTP** и введите в нем **9999.**
11. Щелкните кнопку Next.
12. На странице **Completing the New Web Publishing Rule Wizard** щелкните кнопку **Finish.**
13. Прежде чем перейти к следующему заданию, остановите и перезапустите службы Web-прокси и брандмауэра в оснастке ISA Management.

Задание 5. Проверка конфигурации

Вы проверите конфигурацию публикации, подключившись с браузера на компьютере Server2 ко внешнему IP-адресу компьютера Server1.

1. Войдите в систему сервера Server2 под учетной записью Administrator (Администратор).
2. Откройте Internet Explorer.
3. В текстовом поле **Address** (Адрес) введите внешний IP-адрес, назначенный интернет-провайдером серверу Server1, и нажмите Enter.

Вы должны увидеть стандартную Web-страницу с приветствием сервера, появление которой свидетельствует о том, что вы подключились к внутреннему Web-серверу через внешний IP-адрес брандмауэра ISA-сервера, то есть публикация Web-узла по умолчанию выполнена успешно.

Резюме

Правила Web-публикации позволяют ISA-серверу отвечать на клиентские запросы от имени опубликованных Web-серверов. Web-запросы, направляемые клиентами Интернета на внешний IP-адрес ISA-сервера, пересылаются на опубликованный Web-сервер, указанный в соответствующем правиле Web-публикации. Таким образом, правила Web-публикации определяют порядок перехвата и обработки входящих Web-запросов ISA-сервером.

Подмножества адресатов в правилах Web-публикации обычно содержат доменное имя (соответствующий IP-адрес относится к компьютеру ISA-сервера) и путь. Подмножества клиентских адресов обычно включают IP-адреса клиентов Интернета. Действия для правил Web-публикации обычно предусматривают отбрасывание HTTP-запросов, направленных определенным подмножествам адресатов, или их перенаправление на другие узлы, например на Web-сервер в корпоративной сети. В процессе создания правила Web-публикации вы также вправе сконфигурировать порядок пересылки и преобразования входящих HTTP- и SSL-запросов в формат других протоколов, в том числе HTTP, SSL и FTP. Этот процесс называется *сопряжением* (bridging).

При публикации Web-сервера, расположенного на одном компьютере с ISA-сервером, его следует сконфигурировать на прослушивание порта, отличного от 80, после чего изменить на ISA-сервере правило Web-публикации так, чтобы запросы пересылались на соответствующий порт Web-сервера.

Занятие 3. Публикация почтового сервера

Почтовые серверы обычно работают по нескольким протоколам, поэтому, публикуя защищенный брандмауэром почтовый сервер, обычно требуется разрешить доступ по всем необходимым протоколам. Имеющийся в составе ISA-сервера мастер Mail Server Security упрощает процесс публикации почтовых серверов.

Мастеру достаточно указать необходимые службы, местоположение почтового сервера и внешний адрес ISA-сервера — все нужные правила и/или фильтры IP-пакетов создаются автоматически.

Изучив материал этого занятия, вы сможете:

- ✓ с помощью мастера Mail Server Security опубликовать почтовый сервер на компьютере, расположенном во внутренней сети;
- ✓ с помощью мастера Mail Server Security опубликовать почтовый сервер, расположенный на одном компьютере с ISA-сервером.

Продолжительность занятия — около 30 минут.

Мастер Mail Server Security

В составе ISA-сервера поставляется мастер Mail Server Security, который применяется для безопасной публикации почтового сервера, расположенного в сети, защищенной ISA-сервером. Мастер самостоятельно конфигурирует правила ISA-сервера, которые обеспечивают безопасную публикацию внутренних почтовых служб для доступа внешних пользователей.

Чтобы запустить мастер Mail Server Security, щелкните правой кнопкой папку **Server Publishing Rules** в оснастке ISA Management и в контекстном меню выберите команду **Secure Mail** Server. Для изменения параметров существующего правила публикации почтового сервера воспользуйтесь окном свойств правила в папке Server **Publishing Rules.**

▶ **Запуск мастера Mail Server Security**

1. В дереве консоли ISA Management щелкните правой кнопкой папку **Server Publishing Rules** и в контекстном меню выберите команду **Secure Mail Server.**
2. Последовательно выполняйте инструкции мастера.

Параметры, настраиваемые с помощью мастера Mail Server Security

Мастера Mail Server Security позволяет настроить ряд параметров:

- протокол для выбранной почтовой службы;
- публикуемый IP-адрес почтового сервера, который является внешним IP-адресом ISA-сервера;
- внутренний IP-адрес почтового сервера.

Мастер Mail Server Security также создает разрешающее пересылку почтового трафика правило протоколов со следующими параметрами:

- протокол — SMTP (клиент);
- подмножество клиентов содержит внутренний **IP-адрес** компьютера почтового сервера.

Состав создаваемых правил определяется параметрами, определяемыми в процессе работы мастера. ISA-сервер отмечает создаваемые мастером правила, добавляя к их именам приставку «Mail Wizard Rule». Например, если средствами мастера Mail Server Security конфигурируется публикация исходящей почты по протоколу SMTP, ISA-сервер создаст

правило протокола по имени «Mail Wizard Rule—SMTP (client). Internal IP: <*IP-адрес*>», где <*IP-адрес*>— это внутренний IP-адрес, заданный в процессе работы мастера. Имена правил отображаются в области сведений при выборе в дереве консоли папки Server Publishing Rules.

Если почтовый сервер расположен на одном компьютере с ISA-сервером, то. чтобы разрешить трафик по протоколу SMTP, мастер Mail Server Security создаст фильтр IP-пакетов, а не правило протоколов.

Фильтрация информационного наполнения Интернета

Если на ISA-сервере установлен и работает фильтр SMTP, вы вправе включить фильтрацию информационного наполнения Интернета для всей входящей почты. Для это достаточно не забыть установить в мастере флажок Apply content filtering. Фильтрация информационного наполнения Интернета выполняется в соответствии с конфигурацией фильтра SMTP.

Обратите внимание, что, если SMTP-фильтр уже работает, отключить его средствами мастера Mail Server Security не удастся.

Конфигурирование сервера Exchange в локальной сети

Мастер Mail Server Security позволяет конфигурировать внутренний сервер Microsoft Exchange Server, предоставляя доступ к нему клиентов по одному или нескольким из перечисленных протоколов:

- MAPI (Messaging Application Programming interface);
- POP3 (Post Office Protocol 3);
- IMAP4 (Internet Messaging Access Protocol 4);
- NNTP (Network News Transfer Protocol);
- безопасный NNTP (Secure NNTP).

Мастер создает один или несколько правил публикации — в соответствии с перечнем защищаемых ISA-сервером служб. В создаваемых мастером правилах публикации серверов указаны следующие параметры;

- внутренний адрес почтового сервера;
- внешний адрес, являющийся адресом ISA-сервера;
- протокол для избранной почтовой службы.

Имена создаваемых мастером правил получают приставку «Mail Wizard Rule».

Сервер Exchange, совмещенный с ISA-сервером

Мастер Mail Server Security применяется для публикации сервера Exchange, расположенного на одном компьютере с ISA-сервером. В такой ситуации мастер создает фильтр IP-пакетов для каждой публикуемой почтовой службы. Допустим, требуется средствами мастера Mail Server Security сконфигурировать ISA-сервер, разрешив исходящую почту по протоколу SMTP и обеспечив доступ клиентов по протоколу POP3. У клиентов Microsoft Outlook не будет доступа к серверу Exchange извне локальной сети. Чтобы предоставить уполномоченным клиентам доступ к серверу SMTP как извне, так и изнутри локальной сети, следует создать следующие четыре фильтра IP-пакетов:

- фильтр IP-пакетов, разрешающий входящие TCP-подключения (Inbound TCP) на локальном порту 25 с любых удаленных портов (чтобы разрешить прохождение входящих SMTP-пакетов);
- фильтр IP-пакетов, разрешающий исходящие TCP-подключения (Outbound TCP) на любые удаленные порты с локального порта 25 (чтобы разрешить прохождение исходящих SMTP-пакетов);

- фильтр IP-пакетов, разрешающий входящие TCP-подключения **(Inbound TCP)** на локальном порту 110 с любых удаленных портов (чтобы разрешить прохождение входящих POP3-пакетов);
- фильтр IP-пакетов, разрешающий исходящие TCP-подключения **(Outbound TCP)** на любые удаленные порты с локального порта **110** (чтобы разрешить прохождение исходящих POP3-пакетов).

Практикум. Публикация службы SMTP

Вы сконфигурируете службу **SMTP** на компьютере Server2, а затем воспользуетесь мастером Mail Server Security для опубликования службы SMTP в Интернете. Затем вы проверите корректность конфигурирования, направив сообщение электронной почты по опубликованному адресу внутреннего сервера **SMTP.**

Этот практикум предполагает наличие активного подключения к Интернету по телефонной линии, кроме того, все четыре задания должны выполняться в течение одного сеанса связи. Перед выполнением заданий подключитесь к своему интернет-провайдеру.

До выполнения заданий следует остановить на Server1 сдужбу **SMTP.** Для этого в оснастке Internet Services Manager щелкните правой кнопкой мыши значок **Default SMTP Virtual Server** (Виртуальный SMTP-сервер по умолчанию) и в контекстном меню выберите команду **Stop** (Остановить).

В этом практикуме также предполагается, что вы создали и включили фильтр IP-пакетов, разрешающий пересылку трафика по протоколу SMTP, как описано в занятии 5 главы 4.

Задание 1. Конфигурирование службы SMTP

Вы сконфигурируете службу **SMTP** на Server2. Основная задача службы SMTP заключается в отправке почты; ее работа зависит от других служб, таких как служба POP3, обеспечивающих доставку почты в почтовые ящики пользователей. Хотя в Windows 2000 и не предусмотрена встроенная служба **POP3,** служба SMTP и сама успешно сохраняет всю отправленную почту в локальном доменном каталоге Drop. Размещенные в каталоге Drop сообщения можно открывать и читать вручную или обрабатывать и пересылать с помощью сценариев.

1. Войдите в домен DomainOl с компьютера Server2 под учетной записью Administrator (Администратор).
2. В меню **Start** (Пуск) перейдите к **Administrative Tools** (Администрирование), а затем — к **Internet Services Manager.** Откроется окно оснастки **Internet Information Services.**
3. В дереве консоли Internet Information Services разверните узел * **server2.**
4. Щелкните правой кнопкой мыши узел **Default SMTP Virtual Server** (Виртуальный SMTP-сервер по умолчанию) и в контекстном меню выберите команду **Properties** (Свойства). Откроется окно свойств виртуального SMTP-сервера.
5. В поле со списком **IP Address** (IP-адрес) выберите **192.168.0.2.**
6. Щелкните кнопку OK.

Задание 2. Создание правила для почты

Вы воспользуетесь мастером Mail Server Security, чтобы создать правило, сопоставляющее внешнему IP-адресу ISA-сервера внутренний почтовый сервер на компьютере Server2.

1. Войдите в систему сервера Serverl под учетной записью Administrator (Администратор).
2. Откройте оснастку ISA Management.

3. Разверните узел **Publishing.**
4. Щелкните правой кнопкой мыши папку **Server Publishing Rules** и в контекстном меню выберите команду **Secure Mail Server,** чтобы открыть окно мастера Secure Mail Server.
5. Щелкните кнопку **Next.**
6. На странице **Mail Services Selection** в столбце **Default Authentication** установите флажки **Incoming SMTP и Outgoing SMTP** и щелкните кнопку **Next.**
7. На странице **ISA Server's External IP Address** щелкните кнопку **Browse** и в открывшемся окне **Browse for external IP Addresses** выберите внешний IP-адрес, назначенный интернет-провайдером компьютеру Server1,
8. Щелкните кнопку OK. Внешний IP-адрес отобразится в текстовом поле **External IP address.**
9. Щелкните кнопку Next, чтобы перейти на страницу **Internal Mail Server.**
10. На странице **Internal Mail Server** установите переключатель в положение **At this IP address** и в текстовом поле введите **192.168.0.2.**
11. Щелкните кнопку Next, чтобы перейти на страницу **Completing the Mail Server Security Wizard.**
12. Щелкните кнопку **Finish.**
13. Прежде чем перейти к следующему заданию, средствами оснастки ISA Management перезапустите службы Web-прокси и брандмауэра.

Задание 3. Конфигурирование Outlook Express

В этом задании вы сконфигурируете программу Outlook Express для отправки почты через SMTP-сервер, размещенный на компьютере Server2. В качестве IP-адреса сервера SMTP вы укажете опубликованный адрес, соответствующий внешнему IP-адресу Server1,

1. Войдите в систему сервера Server1 под учетной записью Administrator (Администратор).
2. В меню **Start** (Пуск) перейдите к **Programs** (Программы) и щелкните значок **Outlook Express.** Откроется **Outlook Express** и окно **Your Name** (Введите имя) мастера Internet Connection wizard (Мастер подключения к Интернету).
3. В текстовом поле **Display name** (Введите имя) введите **Test User.**
4. Щелкните кнопку Next (Далее), чтобы перейти на страницу **Internet E-mail Address** (Адрес электронной почты Интернета).
5. В текстовом поле **E-mail address** (Адрес электронной почты) введите **testuser.**
6. Щелкните кнопку **Next.** Откроется информационное окно с сообщением, что введенная строка не является действительным адресом электронной почты.
7. Щелкните кнопку Yes (Да), чтобы проигнорировать предупреждение и перейти на страницу **E-mail Server Names** (Серверы электронной почты).
8. В текстовом поле **Incoming mail (POP3, IMAP or HTTP) server** [Сервер входящих сообщений (POP3, ШАР или HTTP)] введите **example.microsoft.com.** (Это имя используется в качестве метки-заполнителя и не является реальным сервером — вы вправе ввести имя любого действительного сервера POP3, используемого для электронной почты.)
9. В текстовом поле **Outgoing mail (SMTP) server** [Сервер исходящих сообщений (SMTP)] введите внешний IP-адрес, назначенный интернет-провайдером компьютеру Server1. Он должен совпадать с IP-адресом, назначенным при создании правила средствами мастера Mail Server Security в задании 2.
10. Щелкните кнопку Next, чтобы перейти на страницу **Internet Mail** Logon (Вход в почту Интернета).
11. Щелкните кнопку **Next,** чтобы перейти на страницу **Congratulations** (Поздравляем).
12. Щелкните кнопку **Finish** (Готово), чтобы вернуться в окно **Outlook Express.**

13. В меню **Tools** (Сервис) выберите команду Accounts (Учетные записи). Откроется диалоговое окно **Internet Accounts** (Учетные записи в Интернете).
14. Перейдите на вкладку **Mail** (Почта), выберите учетную запись **example.microsoft.com** и щелкните кнопку **Properties** (Свойства). Откроется диалоговое окно свойств записи Example.microsoft.com.
15. Перейдите на вкладку **Servers** (Серверы).
16. В области **Outgoing Mail Server** (Сервер исходящей почты) установите флажок **My server** requires **authentication** (Проверка подлинности пользователя).
17. Щелкните кнопку Settings (Настройка). Откроется диалоговое окно **Outgoing Mail Server** (Сервер исходящей почты).
18. Установите переключатель в положение Log **on** using (Использовать).
19. В текстовом поле **Account name** (учетную запись) введите **Administrator.**
20. В текстовом поле **Password** (пароль) введите пароль, назначенный учетной записи Administrator на компьютере Server2.
21. Щелкните кнопку **OK**, чтобы вернуться в окно свойств учетной записи **Example.microsoft.com**.
22. Щелкните кнопку OK.
23. В диалоговом окне **Internet Accounts** щелкните кнопку **Close** (Закрыть).

Задание 4. Проверка настройки

В этом задании вы проверите корректность выполненной настройки, отправив сообщение электронной почты с помощью опубликованного SMTP-сервера, а затем проверите успешность пересылки сообщения SMTP-сервером в папку Drop на компьютере Server2.

1. Не выходя из системы сервера Server1 и не закрывая **Outlook Express,** щелкните значок New **Mail** (Создать сообщение) на панели инструментов, чтобы открыть диалоговое окно New **Mail** (Новое сообщение) создания нового сообщения электронной почты.
2. В текстовом поле To (Кому) введите **<*ваше_имя*>@server2.domain01.local**, где в качестве **<*ваше_имя*>** укажите свое имя. Имя не обязательно должно быть действительной учетной записью пользователя.
3. В текстовом поле **Subject** (Тема) введите **SMTP test mail.**
4. В теле сообщения введите короткое сообщение, например **This is a test** (Это тест).
5. Щелкните значок **Send** (Отправить) на панели инструментов.
6. Войдите в домен DomainOIc сервера Server2 под учетной записью Administrator (Администратор) и откройте папку C:\Inetpub\mailroot\Drop.
7. В меню Tools (Сервис) выберите команду **Folder Options** (Свойства папки).
8. Перейдите на вкладку **View** (Вид).
9. Сбросьте флажок **Hide file extensions for known file types** (Скрывать расширения для зарегистрированных типов файлов).
10. Щелкните кнопку OK. Теперь в папке должен отображаться файл сообщения Outlook Express с расширением .eml и длинным алфавитно-цифровым именем.
11. Щелкните правой кнопкой мыши файл и в контекстном меню выберите команду **Open** (Открыть). Откроется окно мастера подключения к Интернету.
12. Щелкните кнопку **Cancel** (Отмена). Откроется информационное окно с сообщением, что на компьютере не создана почтовая учетная запись.
13. Щелкните кнопку Yes (Да), чтобы закрыть информационное окно. Откроется другое информационное окно с предупреждением о том, что на компьютере нет заданного по умолчанию почтового клиента.

14. Щелкните кнопку **OK,** чтобы закрыть информационное окно. Вы должны увидеть сообщение, которое только что отправили с компьютера Server1. Поскольку в почтовом клиенте мы определили внешний IP-адрес сервера SMTP, наличие указанного сообщения свидетельствует об успешной публикации SMTP-сервера.
15. Закройте диалоговое окно **SMTP Test Mail.**

Резюме

Мастер Mail Server Security облегчает публикацию почтовых серверов, размещенных в локальной сети. В процессе публикации почтового сервера мастер Mail Server Security создает правила публикации серверов, определяющие публикуемый (соответствующий внешнему IP-адресу ISA-сервера) и внутренний IP-адреса почтового сервера. К именам новых созданных мастером правил добавляется приставка «Mail Wizard Rule». Мастер Mail Server Security также создает правила протоколов, чтобы разрешить исходящий почтовый трафик. Если почтовый сервер расположен на одном компьютере с ISA-сервером, то, чтобы разрешить трафик по протоколу SMTP, мастер Mail Server Security создает фильтр IP-пакетов, а не правило протоколов.

Для запуска мастера Mail Server Security нужно в дереве консоли ISA Management щелкнуть правой кнопкой мыши папку **Server Publishing Rules** и в контекстном меню выбрать команду **Secure Mail Server.**

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Ответы для самопроверки — в приложении А «Вопросы и ответы» в конце книги.

1. Какие типы правил публикации доступны в режимах брандмауэра (Firewall) и сервера кэширования (Cache)?

2. Как вы порекомендуете опубликовать SMTP-сервер, расположенный в сети периметра, если сеть защищена ISA-сервером?

3. ISA-сервер получил HTTP-запрос. Какие протоколы ISA-сервер может использовать для пересылки запроса адресатам внутренней сети?

4. На каком порту служба Web-сервера IIS по умолчанию прослушивает запросы? На каком порту прослушивает запросы механизм автоматического обнаружения серверов? На каких портах ISA-сервер по умолчанию прослушивает внутренние и внешние запросы?

5. Почтовый сервер совмещен на одном компьютере с ISA-сервером. Какие четыре фильтра IP-пакетов следует создать, чтобы предоставить внутренним и внешним клиентам доступ к службам протоколов SMTP и POP3?

ГЛАВА 7

Обеспечение безопасности сети предприятия средствами ISA-сервера

Занятие 1. Применение политики предприятия 204

Занятие 2, Настройка массивов ISA-серверов 213

Занятие 3. Обеспечение безопасности виртуальных частных сетей средствами ISA-сервера 224

Закрепление материала 232

В этой главе

В сетях крупных предприятий часто требуются многоуровневые, надежные и гибкие структуры для обеспечения безопасной работы в Интернете. Политики предприятия и возможности конфигурирования ISA-сервера позволяют реализовать политики в многоуровневых структурах, обеспечивая возможность безопасного доступа в Интернет как на уровне предприятия, так и массивов, причем эти два механизма могут применяться и совместно, и по отдельности. Многосерверные массивы ISA-сервера способны обеспечить надежную защиту для достаточно крупных предприятий. И, наконец, ISA-сервер предоставляет достаточно гибкую систему безопасности для работы в Интернете в сетях, охватывающих множество местоположений и содержащих мобильных пользователей.

Прежде всего

Для изучения материалов этой главы необходимо:

- выполнить процедуры установки, описанные в разделе «Об этой книге»;
- выполнить все упражнения глав 1–4.

Занятие 1. Применение политики предприятия

Политики предприятия на ISA-сервере конфигурируются на уровне штаб-квартиры организации и могут применяться как к отдельным массивам, так и ко всем массивам без исключения. Политики массивов **конфигурируются** на уровне подразделения и обычно наследуют политику предприятия. Существует несколько вариантов применения политик в отдельных массивах ISA-серверов: только политики предприятия, только политики массива или совместно и те и другие.

Изучив материал этого занятия, вы сможете:

- ✓ конфигурировать политику предприятия на ISA-сервере;
- ✓ применять политику предприятия к массиву;
- ✓ создавать политику предприятия по умолчанию, которая наследуется массивами.

Продолжительность занятия — около 40 минут.

Политики предприятия и массивы

За конфигурирование и применение политик предприятия к массивам ISA-серверов отвечают администраторы предприятия. В каждом конкретном массиве ISA-серверов политики предприятия определяют, разрешены ли в массиве политики массивов и в каком объеме (то есть какие правила разрешены в политиках массивов).

Порядок применения политик предприятия

В процессе установки ISA-сервера, выполняемом после инициализации предприятия, вы вправе установить ISA-сервер как член массива. Если присоединить ISA-сервер к существующему массиву, то ISA-сервер унаследует политики предприятия массива. В процессе создания нового массива мастер установки ISA-сервера выполняет поиск доступных политик предприятия, которые можно применить к новому массиву. Если установку ISA-сервера выполняет член группы Enterprise Admins (Администраторы предприятия), ему предоставляется право определить порядок наследования политик и их перечень: наследует ли новый массив политику предприятия (политику по умолчанию, существующую политику, новую политику) или игнорирует политики предприятия и использует лишь политику массива. При установке ISA-сервера не членом группы Enterprise Admins новый ISA-сервер автоматически унаследует политики предприятия по умолчанию, определенные администратором предприятия.

Примечание Если массив настроен на использование исключительно политики массива (а не предприятия), его нельзя перенастроить на использование политики предприятия. Аналогичным образом массив, использующий политику предприятия, не удастся перенастроить на игнорирование политик предприятия и использование лишь политик массива.

Создание политики предприятия

В политику предприятия входят правила узлов и содержимого и правила протоколов; ее разрешается применять к любому доступному массиву, тогда как политики массива лишь создают дополнительные ограничения (если на то есть разрешения). Допускается также создавать элементы политики на уровне предприятия, которые используются правилами на уровне предприятия или массива.

Хотя по умолчанию разрешения на конфигурирование политики предприятия предоставлены только членам группы Enterprise Admins, свойства любой политики предприятия можно изменить и предоставить такое разрешение другим пользователям. То есть, будучи администратором предприятия, вы вправе предоставить любому пользователю или группе разрешения на изменение отдельных или всех политик предприятия.

▶ **Создание политики предприятия**

1. В дереве консоли ISA Management раскройте узел **Enterprise**.
2. Щелкните правой кнопкой узел **Policies** и в контекстном меню последовательно выберите команды **New** и **Policy.**
3. В мастере New Enterprise Policy последовательно выполняйте инструкции.

▶ **Конфигурирование политики предприятия для массива**

1. В дереве консоли ISA Management щелкните правой кнопкой мыши массив, к которому следует применить политику, и в контекстном меню выберите команду **Properties.**
2. На вкладке **Policies** установите переключатель в положение Use **custom enterprise policy settings** (использовать настраиваемые параметры политики предприятия).
3. Установите переключатель Use **this enterprise policy** (использовать данную политику предприятия) и в поле со списком выберите политику предприятия, которую предполагается применить к массиву.

Имейте в виду, что:

- для создания новой политики предприятия следует войти в систему под учетной записью члена группы Enterprise Admins;
- создание новой политики предприятия возможно только при условии, что ISA-сервер установлен как член массива или при администрировании на уровне предприятия.

Настройка параметров политики предприятия

Параметры политики предприятия определяются порядком наследования, который указывает, как политика предприятия применяется на уровне массива. Администратор предприятия вправе изменить это поведение, щелкнув правой кнопкой мыши узел Enterprise в оснастке ISA Management и выбрав в контекстном меню команду **Set Defaults.** Порядок наследования также определяется в процессе установки или изменения свойств массива администратором предприятия.

На рис. 7-1 показано окно параметров политики предприятия в диалоговом окне Set **Defaults.** Чтобы открыть это окно, щелкните правой кнопкой мыши узел **Enterprise** в оснастке ISA Management и выберите команду **Set Defaults.** Настраиваемые в этом окне параметры политики предприятия по умолчанию применяются ко всем массивам, исключение составляют массивы, свойства которых особо определены администратором предприятия.

На рис. 7-2 показаны параметры политики предприятия на вкладке **Policies** страницы свойств массива. Если переключатель установлен в положение **Use default enterprise policy settings** (использовать параметры политики предприятия по умолчанию), к массиву применяются параметры, заданные в диалоговом окне Set **Defaults.** Если же переключатель установлен в положение **Use custom enterprise policy settings,** новые параметры переопределят политику предприятия по умолчанию. Разрешениями на изменение параметров политики предприятия в массиве обладают только администраторы предприятия. Если установка ISA-сервера или создание массива выполняется пользователем, не обладающим такими полномочиями, к новому массиву применяются параметры политики предприятия по умолчанию.

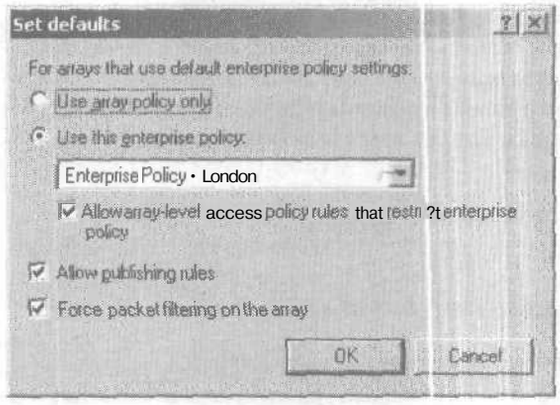


Рис. 7-1. Параметры политики предприятия по умолчанию

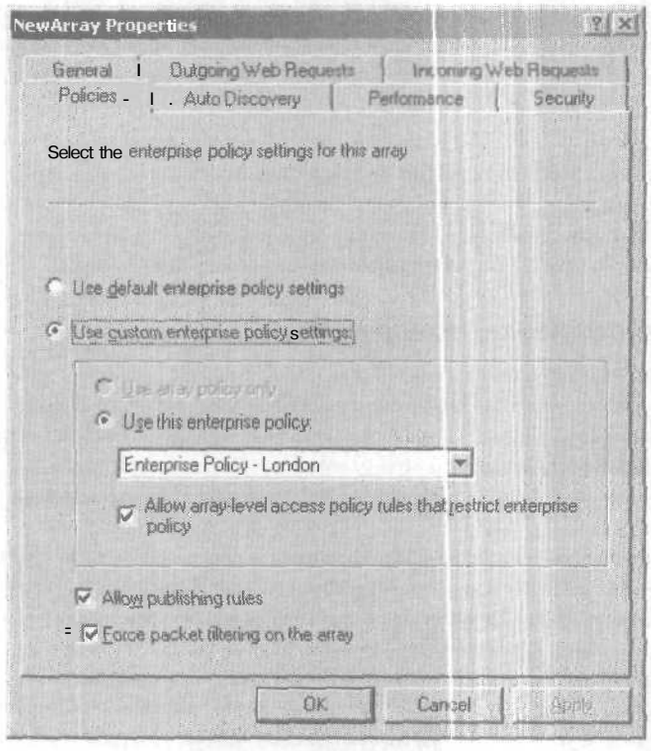


Рис. 7-2. Параметры политики предприятия для массива

Разработано несколько вариантов применения политики предприятия.

- **Только политика предприятия.** Чтобы выбрать этот вариант, установите переключатель **Use this enterprise policy** и в поле со списком выберите нужную политику. Применение только данной политики предприятия диктуется на уровне предприятия — на уровне массива новые правила протокола или Web-узла и содержимого добавить нельзя.
- **Сочетание политик предприятия и массива.** Чтобы выбрать этот вариант, установите флажок **Allow array-level access policy rules that restrict enterprise policy** (разрешить прави-

ла политики доступа уровня массива, ограничивающие политику предприятия) и переключатель Use **this enterprise policy.** В этом варианте разрешается устанавливать правила узлов и содержимого и правила протокола на уровне массива, однако допустимы лишь правила, которые дополнительно ограничивают доступ. Другими словами, правила протоколов и правила узлов и содержимого в массиве могут лишь добавлять дополнительные ограничения к уже определенным правилами уровня предприятия.

- **Только политика массива.** Чтобы выбрать этот вариант, выберите переключатель **Use array policy only** (использовать только политику массива). В этом случае никакая политика предприятия не задается — администратор массива вправе создавать любые правила: как разрешающие, так и ограничивающие доступ. В этом варианте назначить в массиве политику предприятия не удастся.

Примечание На рис. 7-2 переключатель Use **array policy only** недоступен.

- **Разрешить правила публикации.** Задается установкой флажка **Allow publishing rules** и разрешает (или запрещает) создание правил публикации для массива. Обратите внимание, что сами правила публикации на уровне предприятия создать нельзя.
- **Принудительная фильтрация пакетов массива.** Чтобы выбрать этот вариант, установите **Force packet filtering on the array.** Определяет, осуществляется ли фильтрация пакетов массива в обязательном порядке или этим занимается администратор уровня массива. Обратите внимание, что сами фильтры IP-пакетов на уровне предприятия создавать нельзя, а также их невозможно запретить политикой предприятия.

Стандартную (по умолчанию) политику предприятия, которая используется хотя бы одним массивом предприятия, изменить нельзя. Если какой-то массив применяет стандартный вариант политики, член группы Enterprise Admins вправе изменить параметры предприятия, используемые массивом, установив переключатель **Use custom enterprise policy settings** в свойствах массива на вкладке **Policy.** Администратор предприятия имеет возможность определить, будет ли данный массив игнорировать все параметры политики предприятия, наследовать конкретную политику предприятия (в неизменном виде) или наследовать политику предприятия и далее ограничивать ее на уровне массива.

► **Настройка политики предприятия по умолчанию**

1. В дереве консоли ISA Management щелкните правой кнопкой мыши узел **Enterprise.**
2. В контекстном меню выберите команду **Set Defaults.**
3. В диалоговом окне **Set Defaults** установите переключатель в одно из положений:
   - **Use array policy only** — если к массиву нужно применять только политику массива;
   - **Use this enterprise policy** — если к массиву нужно применить определенную политикупредприятия.
4. Если вы установили переключатель Use **this enterprise policy,** следует выполнить хотя бы одно из перечисленных далее действий:
   - в поле со списком выберите политику предприятия, применяемую к массиву;
   - *(Не обязательно.)* чтобы разрешить правилам политики уровня массива налагать дополнительные ограничения кроме тех, которые определены в выбранной политике предприятия, установите флажок **Allow array-level access policy rules that restrict enterprise policy.**

Следует иметь в виду, что:

- изменять порядок применения политик предприятия разрешается только при администрировании ISA-сервера с компьютера — члена массива;
- если настроить массив на применение исключительно политики массивов, в дальнейшем его не удастся перенастроить на использование политики предприятия.

Внимание! В момент применения политики предприятия к массиву все ранее определенные правила узлов и содержимого и правила протоколов уровня массива удаляются.

Архивирование и восстановление конфигурации предприятия

Можно архивировать все параметры конфигурации предприятия в локальном файле — в любом каталоге и под определенным пользователем именем. В процессе архивирования сохраняется вся информация, касающаяся предприятия, в том числе все политики предприятия и их элементы. Также сохраняется информация о массивах и используемых ими политиках предприятия. Нельзя лишь сохранить информацию, относящуюся к самим массивам.

Ранее сохраненная в файле конфигурация предприятия полностью восстанавливается и возвращает систему в состояние на момент выполнения архивирования.

Внимание! Восстановление конфигурации предприятия может повлиять на политики массивов, использующие политики предприятия, поэтому после архивирования предприятия следует выполнить архивирование всех массивов предприятия. Восстановление выполняется также в два этапа: после восстановления конфигурации предприятия следует восстановить конфигурации всех массивов.

► Архивирование конфигурации предприятия

1. В дереве консоли ISA Management щелкните правой кнопкой узел **Enterprise** и выберите в контекстном меню **Back Up.** Откроется диалоговое окно **Backup Enterprise Configuration** (архивирование конфигурации предприятия).
2. В текстовом поле **Store backup information in this location** введите имя и путь *к* файлу, в который планируется выполняться архивирование. По умолчанию архивный файл имеет расширение .bef.
3. *(Не обязательно.)* В поле **Comment** введите любую информацию, которую сочтете полезной.
4. Щелкните **OK.**

   Через некоторое время откроется информационное окно **Backup Enterprise Configuration,** сообщающее об успешном завершении архивирования.

► Восстановление конфигурации предприятия

1. В дереве консоли **ISA Management** щелкните правой кнопкой узел **Enterprise,** затем щелкните **Restore.** Откроется информационное окно ISA-сервера, информирующее о том, что существующая конфигурация будет заменена.
2. Если вы действительно решили заменить существующую конфигурацию предприятия копией из архива, щелкните кнопку Yes.
3. Откроется диалоговое окно **Restore Enterprise Configuration** (восстановление конфигурации предприятия).
4. В текстовом поле **Restore Configuration From The Following Backup** введите путь к папке с архивными копиями и имя файла.
5. Щелкните **OK.** Снова откроется диалоговое окно **Restore Enterprise Configuration.**
6. Щелкните OK.

   Через некоторое время откроется информационное окно **Restore Enterprise Configuration** с сообщением об успешном выполнении восстановления конфигурации.

Практикум. Создание и применение политики предприятия

На этом практическом занятии вы создадите политику предприятия. Затем вы установите ISA-сервер на Server2, примените созданную политику предприятия и просмотрите результаты.

Задание 1. Создание политики предприятия

Сейчас вы настроите параметры политики предприятия на сервере Server1.

▶ **Создание политики предприятия на Server1**

1. Войдите в систему Server1 под учетной записью Administrator (Администратор).
2. В дереве консоли ISA Management последовательно раскройте узлы **Enterprise и Policies.**
3. Щелкните правой кнопкой мыши узел **Enterprise Policy 1** и выберите команду **Properties.** Откроется диалоговое окно **Enterprise Policy 1 Properties,**
4. Переименуйте **Enterprise Policy 1.** Для этого введите **Test Enterprise Policy** в текстовом поле **Name.**
5. Щелкните кнопку **OK.**
6. Раскройте узел **Test** Enterprise **Policy.**
7. Щелкните правой кнопкой палку **Protocol Rules и** последовательно выберите в контекстном меню команды New и **Rule.** Откроется окно мастера **New Protocol Rule.**
8. В текстовом поле **Protocol Rule** Name введите **Deny Archie Protocol** (запрет протокола Archie) и щелкните кнопку Next.
9. На странице **Rule Action** установите переключатель в положение **Deny** и щелкните кнопку Next.
10. На странице **Protocols** в поле со списком **Apply this rule** to (применять данное правило к...) выберите **Selected Protocols.** Откроется список **Protocols (Enterprise Level).**
11. В списке **Protocols (Enterprise** Level) пометьте вариант **Archie** и щелкните кнопку Next.
12. На странице Schedule оставьте в поле со списком **Use this schedule** значение Always и щелкните кнопку Next.
13. На странице **Client Type** оставьте переключатель в положении **Any request** и щелкните кнопку Next.
14. На странице **Completing the New Protocol Rule Wizard** щелкните кнопку **Finish.**
15. В дереве консоли щелкните правой кнопкой узел **Enterprise** и выберите команду **Set Defaults.** Откроется диалоговое окно **Set Defaults.**
16. Убедитесь, что выбран переключатель Use **this enterprise policy. В** поле со списком должен быть выбран элемент **Test Enterprise Policy.**
17. Убедитесь, что установлен флажок **Allow array-level access policy rules that restrict enterprise policy.**
18. Щелкните **OK.**

Таким образом, вы создали политику предприятия, которая полностью блокирует использование протокола Archie для всех запросов. Поскольку массив MyArray настроен на использование только политики массива, новую политику предприятия применить к нему не удастся. Однако ничто не мешает вам создать новый массив и применить к нему политику Test Enterprise Policy. Эту процедуру вы выполните в задании 2.

Задание 2. Создание нового массива, наследующего политику предприятия по умолчанию

Сейчас вы установите ISA-сервер на Server2 в качестве члена нового массива. Вы войдете в систему под учетной записью члена группы Domain Admins (Администраторы домена), но не группы Enterprise Admins (Администраторы предприятия). Поскольку Test Enterprise Policy является политикой предприятия по умолчанию и у вас нет разрешений группы Enterprise Admins, новый массив автоматически унаследует параметры Test Enterprise Policy. После установки нового массива вы не получите разрешения на выбор политики предприятия, применяемой к новому массиву, — в этом случае автоматически применяется политика предприятия по умолчанию.

▶ **Создание массива, который наследует политику предприятия**

1. Создайте в домене Domain01 учетную запись нового пользователя с именем ArrayAdmin (администратор массива). Включите ArrayAdmin только в члены группы Domain Admins (Администраторы домена). Оставьте его членом группы Domain Users (Пользователи домена).
2. Войдите в домен DomainOl с сервера Server2 под учетной записью ArrayAdmin.
3. Установите ISA-сервер, как описано в практикуме занятия 2 в главе 2. Инициализировать предприятие не нужно, поскольку эта операция была выполнена при установке ISA-сервера на Server1.
4. Для установки выберите полный вариант и установите сервер как член массива.

   В начале процесса установки откроется диалоговое окно **Microsoft ISA Server Setup,** в котором следует указать, присоединить сервер *к* массиву MyArray или же создать новый массив.
5. Щелкните New для создания нового массива. Откроется диалоговое окно New **Array.**
6. В текстовом поле **Array Name** замените имя по умолчанию **Server2** на **NewArray.**
7. Щелкните кнопку OK.

   Откроется диалоговое окно **Microsoft ISA Server Setup,** в котором выбран переключатель **Integrated Mode.** Оставьте переключатель в таком положении.
8. Щелкните кнопку **Continue.**
9. Закончите установку ISA-сервера, приняв параметры кэша ISA-сервера по умолчанию и построив *таблицу локальных адресов* (Local Address Table, LAT) на основе внутреннего диапазона IP-адресов 192.168,0.0-192.168.0.255.

Задание 3. Проверка созданной конфигурации

В этом задании вы проверите, как политики Test Enterprise Policy влияют на политику уровня массива, определенную для NewArray.

▶ **Проверка конфигурации**

1. Войдите в домен DomainOl с сервера Server2 под учетной записью ArrayAdmin.
2. Откройте консоль ISA Management.
3. В дереве консоли последовательно раскройте узлы **Enterprise и Policies.**
4. Откройте подузел **Test Enterprise Policy** узла. **Policies** и выберите папку **Protocol Rules** (правила протоколов). Убедитесь, что в области сведений есть правило **Deny Archie Protocol.**
5. В дереве консоли последовательно раскройте узлы **Servers And Arrays и NewArray.**
6. Раскройте узел Access **Policy** (политика доступа) и выберите папку **Protocol Rules.** Найдите в области сведений правило **Deny Archie Protocol.** Политика доступа массива NewArray унаследовала параметры Test Enterprise Policy. При установке ISA-сервера вы

вошли в систему как член группы Domain Admins, а не Enterprise Admins, поэтому новый массив унаследовал параметры политики предприятия по умолчанию.

7. В меню **View** отметьте команду **Advanced.**
8. В области сведений щелкните правой кнопкой мыши правило **Deny Archie Protocol** и в контекстном меню выберите команду **Delete.** Откроется диалоговое окно **Confirm Delete.**
9. Щелкните кнопку Yes, чтобы подтвердить удаление правила.

   Откроется окно **ISA Error,** информирующие об отсутствии разрешения на выполнение этого действия.

   Для корректной работы политики на всем предприятии следует планировать сеть так, чтобы администраторы массивов уровня подразделений не входили в группу Enterprise Admins. При этом им необходимо предоставить привилегии группы Domain Admins.
10. Щелкните кнопку **Continue.**
11. При повторном появлении окна с сообщением еще раз щелкните **Continue,** чтобы закрыть его.
12. В дереве консоли щелкните правой кнопкой папку **Protocol Rules,** расположенную под узлом Access **Policy,** и в контекстном меню последовательно выберите New и **Rule.**

    Откроется окно мастера New **Protocol Rule.**
13. В текстовом поле **Protocol Rule Name** введите **Array-Level Protocol Rule,** затем щелкните кнопку **Next.**

    Откроется окно **Rule Action.** Обратите внимание, что переключатель **Allow** недоступен. Это означает, что при действующей политике уровня предприятия разрешается создавать только запрещающие правила, то есть типа **Deny.** Это же верно в отношении правил узлов и содержимого.
14. Щелкните кнопку **Cancel,** чтобы выйти из мастера,
15. В дереве консоли ISA Management щелкните правой кнопкой папку **IP Packet Filters,** в контекстном меню выберите New и затем — **Filter.**

    Откроется окно мастера New **IP Packet Filter.**
16. В поле **IP Packet Filter Name** введите **Open All** и щелкните кнопку **Next,** чтобы перейти на страницу **Servers.**
17. Щелкните кнопку Next, чтобы перейти на страницу **Filter Mode.**
18. Щелкните Next, чтобы перейти на страницу **Filter Type.**
19. Установите переключатель в положение **Custom и** щелкните кнопку **Next.**

    Откроется окно **Filter Settings.** Обратите внимание, что в поле со списком **IP protocol** выбрано значение Any (любой), а в поле **Direction** — значение **Both** (в обоих направлениях).
20. Щелкните кнопку **Next,** чтобы перейти на страницу **Local Computer.**
21. Щелкните кнопку **Next,** чтобы перейти на страницу **Remote Computers.**
22. Щелкните Next, чтобы перейти на страницу **Completing the** New **IP Packet Filter Wizard.**
23. Щелкните кнопку **Finish.**
24. В дереве консоли щелкните папку **IP Packet Filters.** В области сведений в списке фильтров пакетов указан фильтр **Open All.** Политика предприятия не ограничивает использование фильтров IP-пакетов.
25. Выйдите из системы Server2, завершив работу под учетной записью ArrayAdmin, и снова войдите под учетной записью Administrator.
26. Снова запустите ISA Server Setup и удалите все компоненты ISA-сервера. Когда появится диалоговое окно с запросом на удаление всех журналов и архивных копий конфигурации ISA-сервера, щелкните кнопку Yes.

Резюме

Члены группы Enterprise Admins имеют право создавать любое количество политик предприятия, применяемых к группам массивов ISA-серверов. В политики предприятия входят правила узлов и содержимого и правила протоколов, а также иногда предусматриваются элементы политик, действующие как на уровне предприятия, так и на уровне массива.

Изменять параметры политики предприятия вправе только члены группы Enterprise Admins. В политиках предприятия определены параметры по умолчанию для всех массивов и параметры уровня предприятия, применяемые к конкретным массивам. Для каждого отдельно взятого массива эти параметры определяют вариант действия политик: только политика предприятия, только политика массива или их сочетание, а также допустимо ли использование правил публикации или фильтрации пакетов на уровне массива. При комбинировании политик предприятия и массива последняя задает дополнительные ограничения помимо назначенных политикой предприятия. Если массив настроен на использование только политики массива, его нельзя переконфигурировать на наследование политики предприятия. Аналогично, если существующий массив использует только политику предприятия, вам не удастся настроить его на игнорирование параметров политики предприятия и использование политики массива.

В массиве, созданном пользователем, который не обладает разрешениями администратора предприятия, автоматически применяется политика предприятия по умолчанию.

Все параметры конфигурации предприятия можно архивировать и сохранять в локальном файле. При архивировании сохраняется вся относящаяся к предприятию информация, в том числе все политики предприятия и их элементы. Заархивированные параметры конфигурации предприятия легко восстанавливаются из архивного файла.

Занятие 2. Настройка массивов ISA-серверов

Компьютеры со службой ISA-сервер часто объединяются в массивы, в которых группы ISA-серверов рассматриваются и управляются как единая логическая сущность. Кроме того, в массивах клиентские запросы распределяются между несколькими ISA-серверами, что позволяет повысить производительность и надежность серверов за счет снижения времени отклика и повышения отказоустойчивости.

Изучив материал этого занятия, вы сможете:

- ✓ создавать массивы из нескольких ISA-серверов;
- ✓ выдвигать изолированные серверы в члены массива;
- ✓ удалять отдельные серверы из массива;
- ✓ архивировать и восстанавливать конфигурацию массива.

Продолжительность занятия — около 50 минут.

Создание массивов ISA-серверов

При установке ISA-сервера вы можете выбрать, будет ли он изолированным сервером или членом массива (рис. 7-3). В любом случае в оснастке ISA Management ISA-сервер отображается как член массива.

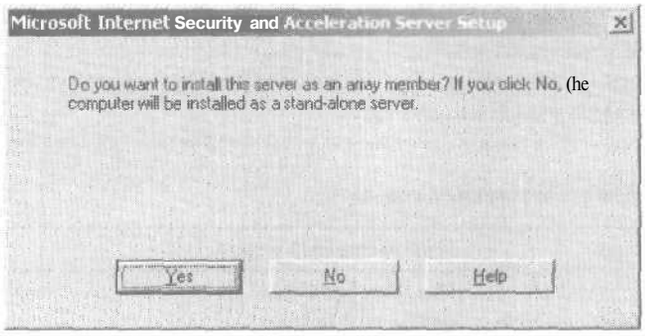


Рис. 7-3. Установка ISA-сервера в качестве изолированного сервера или члена массива

Примечание Перед установкой ISA-сервера в качестве члена массива не забудьте внести в схему службы каталогов Active Directory схему ISA-сервера. Этот процесс называется *инициализацией предприятия* (enterprise initialization). Для выполнения инициализации предприятия необходимы полномочия администратора локального компьютера и члена группы Enterprise Admins (Администраторы предприятия).

Чтобы создать первый массив в сети, установите ISA-сервер как член массива. Не обнаружив существующих массивов, установщик ISA-сервера создаст новый массив. При установке всех последующих ISA-серверов в качестве члена массива установщик предложит присоединиться к массиву из списка (рис. 7-4). Сервер, присоединенный к существующему массиву, наследует все параметры политики массива, поэтому все серверы одного массива обладают *общей конфигурацией*.

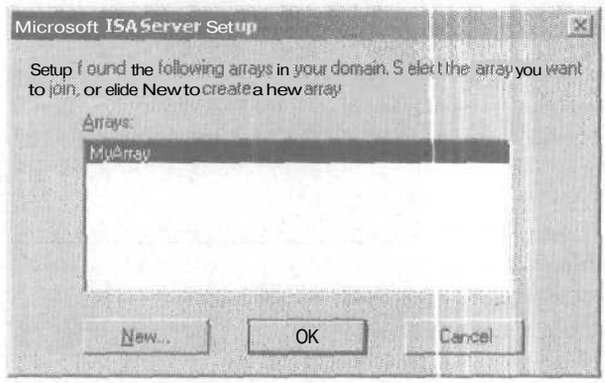


Рис. 7-4. Присоединение сервера к существующему массиву

Требования к членам массивов

Все члены массива должны относиться к одному домену и сайту. Сайт — это группа компьютеров, расположенных в одной TCP/IP-подсети с высокоскоростными соединениями. Домен — определенная администратором группа компьютеров, имеющая общую базу данных каталогов.

Массивы и изолированные серверы

ISA-сервер, устанавливаемый как изолированный сервер, не обязательно входит в домен Microsoft Windows 2000. В процессе установки изолированному ISA-серверу присваивается имя компьютера, на котором он устанавливается.

В таблице 7-1 сравниваются характеристики членов массива и изолированных серверов.

Таблица 7-1. Сравнение массивов и изолированных серверов

Характеристика	Член массива	Изолированный сервер
Масштабируемость	Массивы состоят из одного и более членов	Работает лишь на одном компьютере
Необходимость службы каталогов Active Directory	Необходима. Массивы устанавливаются лишь в домене Windows 2000 со службой каталогов Active Directory	Не обязательна. Информация о конфигурации хранится в реестре ISA-сервера. Разршается устанавливать в доменах Windows NT 4.0
Возможность применения политики предприятия	Да. Одну политику можно применять ко всем массивам предприятия	Нет

Выдвижение изолированных серверов в члены массива

ISA-сервер, установленный как изолированный, нельзя присоединить к массиву, однако его можно *выдвинуть* (promote) в члены массива — в этом случае создается новый массив, членом которого и становится выдвигаемый ISA-сервер.

Если операцию выдвижения выполняет пользователь, не обладающий привилегиями администратора предприятия, в новом массиве применяется политика предприятия по умолчанию. Если политика предприятия разрешает публикацию, все определенные в массиве правила публикации сохраняются.

Обратите внимание, что стандартная (по умолчанию) политика предприятия может переопределять (а значит, удалять) существующие правила политики массива. Например, если политика предприятия запрещает массивам иметь свою политику, все правила политики массива уничтожаются. Если стандартная политика предприятия требует применения политики предприятия и при этом разрешает массивам налагать свои дополнительные ограничения, то все запрещающие правила останутся, а все разрешающие будут удалены.

Право изменять параметры политики предприятия предоставлено группе Enterprise Admins. При настройке параметров политики предприятия для массива вы вправе выбрать стандартную или специальную (настраиваемую) политику предприятия.

▶ **Выдвижение изолированного сервера в члены массива**

1. В меню View выберите **Advanced.**
2. В дереве консоли **ISA Management** щелкните правой кнопкой нужный массив и в контекстном меню выберите команду **Promote.** Откроется информационное окно ISA-сервера, извещающее о готовности начать выдвижение сервера в члены массива.
3. Щелкните кнопку Yes. Откроется диалоговое окно **Enterprise Policy Settings.**
4. Установите переключатель в одно из положений:
   - **Use default enterprise policy settings** (использовать политику предприятия по умолчанию);
   - **Use custom enterprise policy settings** (использовать специальную политику).
5. Если выбран переключатель Use **custom enterprise policy settings,** щелкните один из следующих переключателей:
   - Use array **policy only** — чтобы разрешить только политику массива;
   - **Use this enterprise policy** — чтобы выбрать определенную политику предприятия.
6. Если выбран переключатель **Use this enterprise policy,** выполните одну из операций:
   - выберите в поле со списком политику предприятия, которую следует применить к массиву;
   - *(Не обязательно.)* установите флажок **Also allow array policy** (разрешить также и политику массива).
7. *(Не обязательно.)* Если выбран переключатель **Use custom enterprise policy settings,** установите хотя бы один из флажков:
   - **Allow publishing rules to be created on the array** — чтобы разрешить определять правила публикации на уровне массива;
   - **Force packet filtering on the array** — чтобы включить фильтрацию пакетов.
8. Щелкните кнопку **OK.** Откроется информационное окно **Promoting Server,** сообщающее о завершении процесса выдвижения.

При выдвижении изолированных серверов следует иметь в виду, что:

- выдвигать разрешается только изолированные серверы, входящие в домены Windows 2000;
- перед началом выдвижения ISA-сервера необходимо инициализировать предприятие.

Параметры членов массива

Далее описан порядок настройки параметров и характеристик членов массива.

- **Режимы установки.** При установке ISA-сервера в существующий массив мастер установки автоматически выбирает тот же режим, что и для других членов массива: сервер кэширования (Cache), брандмауэр (Firewall) или смешанный (Integrated). Например,

если все серверы массива установлены в режиме брандмауэра, для нового члена массива также выбирается режим брандмауэра.

- Конфигурация **политики.** Политика массива ISA-серверов — правила доступа, публикации, использования пропускной способности — определяется один раз на уровне массива и затем автоматически применяется ко всем серверам. Кэш также настраивается централизованно на уровне массива. Задания загрузки содержимого по расписанию идентичны для всех серверов.
- **Расширения.** К ним относятся Web-фильтры и фильтры приложений. Установка расширения на один из серверов массива не означает автоматическую установку на все остальные серверы массива — администратор должен установить расширение на каждый из серверов массива.
- **Настройка оповещений.** Оповещения настраиваются индивидуально для каждого из серверов массива или для всех серверов массива сразу.
- Отчеты. Они предоставляют информацию о работе компьютеров массива ISA-серверов. Данные отчета хранятся в базе данных компьютера и в указанной администратором папке — по умолчанию они размещаются на ISA-сервере, ответственном за генерацию отчетов.
- Кэш. Пространство, отводимое под кэш ISA-сервера на каждом из компьютеров, соответствует значению, задаваемому при установке JSA-сервера или при перенастройке кэша. Однако все параметры кэша являются общими для всех серверов массива. Это верно в отношении параметров кэширования протоколов HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protoco) и CARP (Cache Array Routing Protocol). Задания по загрузке содержимого в кэш по расписанию являются общими для всех серверов массива.

Хранение конфигурации массива

Информация о конфигурации изолированных серверов хранится в реестре, а конфигурационные данные массивов размещаются в базе данных Active Directory. При выдвижении изолированного сервера в массив информация о его конфигурации переносится в базу данных службы Active Directory.

При изменении свойств любого из членов массива изменения применяются ко всем членам массива. У всех членов массива конфигурации идентичны, что гарантирует отказоустойчивость системы.

Для серверов можно задавать индивидуальные параметры конфигурации. В часгности, фильтры IP-пакетов, Web-фильтры и фильтры приложений определяются на уровне сервера. Содержимое кэша и журналы хранятся локально. Отчеты создаются на основании информации о работе всех серверов массива, но хранятся на одном сервере. Особенности конфигурации отдельных серверов при архивировании массива не сохраняются.

Поскольку каждый член массива немедленно получает самую свежую информацию обо всех остальных членах, клиенту достаточно взаимодействовать лишь с одним из членов массива. Это обеспечивает дополнительную отказоустойчивость и прозрачность доступа для клиентов.

Управление членством в массиве

В массиве разрешено добавление и удаление, а также самостоятельный выход серверов из массива. Чтобы удалить ISA-сервер из массива, нужно удалить с компьютера программное обеспечение ISA-сервера, запустив мастер установки и выбрав вариант удаления всех компонентов ISA-сервера. Чтобы перенести компьютер в другой массив, достаточно уда-

лить с него ISA-сервер, а затем переустановить и в процессе переустановки присоединить к другому массиву. Любой пользователь вправе получить информацию о составе массива, но только члены группы Administrators (Администраторы) могут изменять состав массива.

При добавлении или удалении сервера из массива происходят изменения в конфигурации предприятия, которые отражаются в базе данных службы Active Directory. Изменения сначала сохраняются на ближайшем контроллере домена Windows 2000, а затем служба Active Directory автоматически реплицирует их на остальные контроллеры доменов.

После внесения любых изменений состава массива следует выполнять архивирование конфигурации массива. При восстановлении массива ISA-серверов восстанавливается состав членов, существовавший на момент архивирования.

Архивирование и восстановление конфигурации массива

ISA-сервер позволяет сохранять и восстанавливать большую часть информации о конфигурации массива. Архивирование выполняется в локальный файл в указанной пользователем папке и под заданным именем. Для обеспечения максимальной безопасности рекомендуется сохранять архивные файлы на разделах с файловой системой NTFS.

Информация о конфигурации ISA-сервера, состоящего в составе массива, хранится в базе данных Active Directory, а на изолированном ISA-сервере параметры конфигурации хранятся в локальном реестре.

Архивирование конфигурации

ISA-сервер позволяет сохранять всю информацию общего назначения о конфигурации массива: правила политики доступа, правила публикации, элементы политики, параметры оповещений, конфигурацию кэша и свойства массива.

Информация, относящаяся к отдельным серверам, не архивируется, в том числе содержимое кэша, журналы, отчеты и действующая политика предприятия.

Рекомендуется архивировать конфигурацию массива после каждого существенного изменения, в том числе после:

- изменения параметров политики предприятия;
- изменения режима массива;
- добавления, удаления и переименования серверов — членов массива;
- изменения размера или местоположения кэша;
- добавления или удаления Web-фильтров.

Рекомендуется также периодически архивировать индивидуальные конфигурации серверов. Для архивирования информации ISA-сервера обычно применяют программу архивирования Windows (Ntbackup), которая кроме прочего позволяет сохранить пароли, параметры локального реестра, конфигурацию кэша, конфигурацию привратника Gatekeeper H.323, отчеты, локальные параметры фильтров приложений, параметры оптимизации производительности, содержимое кэша и журналы. Программа архивирования Windows также применяется для сохранения индивидуальной конфигурации сервера. Ее нельзя использовать для архивирования конфигурации массива, если только ISA-сервер одновременно не является контроллером домена. Это объясняется тем, что информация о конфигурации массива размещена в базе данных Active Directory, которая хранится лишь на контроллерах домена. Перед использованием программы архивирования Windows рекомендуется заархивировать конфигурацию массива. Кроме того, восстанавливать конфигурацию массива рекомендуется сразу же после восстановления средствами программы архивирования Windows.

▶ **Архивирование конфигурации массива**

1. В дереве консоли **ISA Management** щелкните правой кнопкой массив и в контекстном меню выберите команду **Back Up.** Откроется диалоговое окно **Backup Array.**
2. В текстовое поле **Store backup configuration in this location** введите путь и имя архивного файла. По умолчанию архивные файлы получают расширение .bif.
3. (*Необязательно.*) В поле **Comment** введите комментарий к архивному файлу.
4. Щелкните OK.

   Через некоторое время откроется информационное окно **Backup Array**, сообщающее об удачном завершении архивирования.
5. Щелкните кнопку OK.

Примечание **Файл** архива разрешается создавать на любом диске локального компьютера или на сетевом диске — достаточно ввести путь в формате UNC или имя подключенного сетевого диска.

Архивирование конфигурации изолированного сервера

Можно архивировать конфигурацию изолированного сервера. Последующее восстановление конфигурации необходимо выполнять на тот же изолированный сервер.

Восстановление конфигурации

В процессе восстановления происходит восстановление большинства параметров, относящихся к массиву.

▶ **Восстановление конфигурации массива**

1. В дереве консоли **ISA Management** щелкните правой кнопкой мыши нужный массив и в контекстном меню выберите команду **Restore.** Откроется информационное окно ISA-сервера с предупреждением о том, что в процессе восстановления переопределяется существующая конфигурация.
2. Щелкните кнопку **Yes.**
3. В текстовом поле **Restore array configuration from the following backup (.BIF) file** введите путь и имя файла с архивной копией конфигурации.
4. Щелкните OK. Откроется диалоговое окно **Restore Array** с информацией об архиве, из которого предполагается восстановить конфигурацию.
5. Щелкните OK.

   Через некоторое время откроется информационное окно **Restore Array,** сообщающее об успешном завершении процесса восстановления.

При восстановлении конфигурации массива следует иметь в виду, что:

- нельзя заархивировать конфигурацию массива, а затем восстанавливать из полученного архива конфигурацию другого массива или изолированного сервера;
- для восстановления конфигурации массива нельзя использовать файл конфигурации предприятия (.bef);
- нельзя восстанавливать конфигурацию в массиве, в котором действует политика предприятия, отличная от той, что действовала на момент создания архива.

Обеспечение отказоустойчивости в массивах

Отказоустойчивость является важным параметром массивов кэшируюших ISA-серверов. Для гарантированного обслуживания запроса клиента подходящим ISA-сервером используется алгоритм CARP (Cache Array Routing Protocol). В массивах даже при выходе из строя отдельных серверов массива обслуживание запросов клиента продолжают остальные члены массива.

Однако отказоустойчивость службы брандмауэра ISA-сервера зависит от клиента и типа установки. Например, сам по себе ISA-сервер без использования дополнительных программ не в состоянии обеспечить отказоустойчивость и правильное распределение нагрузки:

- для клиентов SecureNAT, которые не поддерживают идентификацию ISA-сервера по имени массива;
- для изолированных серверов, которые не поддерживают объединение в массивы.

В указанных случаях для создания отказоустойчивой, сбалансированной сети применяется сочетание ISA-сервера и других служб операционной системы. Подробнее о настройке DNS-сервера и *службы балансировки сетевой нагрузки* (Network Load Balancing) в Microsoft Windows 2000 Advanced Server для достижения этой цели мы расскажем чуть позже в этой главе.

Отказоустойчивость для клиентов брандмауэра

Отказоустойчивости для клиентов брандмауэра достигается совместным использованием двух и более ISA-серверов и DNS-сервера.

Всем ISA-серверам присваивается одно и то же DNS-имя. Все обращения клиентов к ISA-серверу по его DNS-имени обслуживаются DNS-сервером по механизму циклического обслуживания DNS.

Примечание *Циклическое обслуживание* (round robin) DNS — механизм, используемый DNS-серверами для совместного использования сетевых ресурсов и балансирования их нагрузки. В ответ на запрос сервер DNS возвращает IP-адрес, соответствующий IP-адресу одного из ISA-серверов. Подробно о DNS и циклическом обслуживании — в справочной системе Windows 2000 Server и в комплекте ресурсов «Windows 2000 Server Resource Kit».

► **Настройка DNS-сервера для массива ISA-серверов**

1. В меню **Start** последовательно выберите **Programs** (Программы), **Administrative Tools** (Администрирование) и DNS.
2. В дереве консоли раскройте узел **Forward Lookup Zone**.
3. Щелкните правой кнопкой домен, в который входит массив ISA-серверов, и в контекстном меню щелкните команду New **Host.** Откроется диалоговое окно **New Host**.
4. В текстовом поле **Name** введите DNS-имя ISA-сервера или массива.
5. В текстовом поле **IP address** введите IP-адрес нового узла.
6. Щелкните кнопку **Add Host,** чтобы добавить в зону запись о новом узле.

Выполните пункты 3 и 5 для каждого ISA-сервера. Всем серверам следует присвоить одно и то же имя.

Отказоустойчивость для клиентов SecureNAT

Отказоустойчивость для SecureNAT-клиентов службы брандмауэра достигается установкой двух и более ISA-серверов под управлением *службы балансировки сетевой нагрузки* (Network Load Balancing, NLB) в Windows 2000 Advanced Server. Служба Network Load Balancing — это

один из механизмов организации кластеров в Windows 2000. Сочетая в едином кластере ресурсы нескольких компьютеров под управлением Windows 2000 Advanced Server, эта служба обеспечивает надежность и производительность, необходимую Web-серверам и другим критически важным серверам.

Кластеры NLB объединяют несколько компьютеров-серверов, работающих по протоколу TCP/IP. Доступ ко всем компьютерам кластера осуществляется по единому IP-адресу, а на уровне кластера у каждого из них есть свой уникальный IP-адрес. Служба Network Load Balancing распределяет запросы, поступающие от клиентов по протоколу TCP/IP, между компьютерами кластера.

Внимание! Служба Network Load Balancing поставляется лишь в составе Windows 2000 Advanced Server и Windows 2000 Datacerter Server.

Для работы службы Network Load Balancing требуется назначить всем ISA-серверам кластера уникальные IP-адреса. Кроме того, следует определить IP-адрес, который используется кластером NLB в целом. Подробнее о службе Network Load Balancing *и* кластерах — в разделе «Network Load Balancing» справочной системы Windows 2000 Advanced Server.

► **Настройка ISA-серверов для работы под управлением службы Network Load Balancing**

1. Убедитесь, что ISA-серверы установлены в одинаковом режиме.
2. Для внутреннего сетевого адаптера каждого из ISA-серверов измените свойства Network Load Balancing следующим образом:
   - назначьте основным IP-адресом (Primary IP) IP-адрес кластера Network Load Balancing. Этот адрес используется для IP-адресации кластера в целом, должен быть одинаковым на всех серверах и совпадать с IP-адресом полного имени кластера в Интернете;
   - присвойте каждому компьютеру NLB-кластера индивидуальный приоритет;
   - определите выделенные IP-адреса (Dedicated IP) внутренних сетевых адаптеров ISA-серверов. Эти адреса используются для адресации отдельных узлов в кластере, поэтому они должны быть уникальны в пределах кластера. В качестве этого IP-адреса разрешается использовать адрес присвоенный узлу до выбора IP-адреса кластера.

Если на сервере есть лишь один сетевой адаптер, стек TCP/IP следует настроить на использование как выделенного адреса, так и адреса кластера, причем первым следует указать выделенный адрес. Необходимо, чтобы на компьютере с двумя адаптерами сетевому адаптеру с выделенным адресом соответствовало меньшее числовое значение (и, соответственно, больший приоритет), чем сетевому адаптеру с адресом кластера.

Основной шлюз на клиентах SecureNAT нужно настроить на IP-адрес кластера. Другими словами, в качестве шлюза используется виртуальный адрес кластера, что обеспечит обработку всех запросов к кластеру службой Network Load Balancing.

Протокол CARP

Для определения оптимального пути а массиве при разрешении Web-запроса на ISA-серверах применяется протокол CARP (Cache Array Routing Protocol). Путь разрешения запроса — это либо точное указание на местоположение в массиве, где расположена в кэше запрашиваемая информация, либо директива ISA-серверу запросить ее в Интернете.

Порядок работы протокола CARP

Протокол CARP обеспечивает эффективную маршрутизацию запросов. Далее описаны предусмотренные в этом протоколе этапы обработки запроса.

1. Все серверы занесены в список членов массива, который хранится в базе данных службы Active Directory. Члены массива оповещаются о любых удалениях или добавлениях серверов.
2. Клиент Web-прокси или расположенный ниже в иерархии сервер периодически опрашивает члены массива и в случае необходимости обновляет их список. При этом клиент Web-прокси направляет запрос array.dll?get.routing.script, а серверы — запрос array.dll?get.info.v1.
3. При запросе объекта для определения сервера, который должен его обслужить, клиент или сервер более низкого уровня в иерархии использует список членов массива и предварительно вычисленный хеш URL-адреса.
4. Для каждого из ISA-серверов хеш URL-адреса объединяется с хешем каждого из ISA-серверов. Сервер, для которого эта комбинация имеет наибольшее значение, становится «владельцем» кэшируемой информации.
5. Сервер проверяет, должен ли он обрабатывать запрос. Если нет, запрос пересылается другому члену массива по его IP-адресу внутри массива.

Таким образом определяется местоположение всей кэшированной информации, что позволяет браузерам и серверам более низкого уровня иерархии получать точное локальное местоположение информации, расположенной по запрашиваемому URL-адресу (или место, где она хранится после кэширования). Так как статистический разброс вычисляемых на этапе 3 хешей очень широк, нагрузка распределяется между серверами массива практически равномерно. Кроме того, благодаря эффективному алгоритму определения пути разрешения запросов средствами CARP не требуется поддерживать объемные таблицы с информацией о местоположении кэшируемой информации. Чтобы определить место хранения информации, браузер просто вычисляет определенные значения (хеши).

Отдельные ISA-серверы массива могут отличиться составом оборудования и мощностью, поэтому иногда требуется распределять нагрузку кэширования неравномерно. Для этой цели в параметрах протокола CARP для отдельных членов массива указывается коэффициент их нагрузки.

Кроме того, CARP настраивается на различный порядок обработки входящих и исходящих Web-запросов. Например, использование CARP разрешается для всех исходящих Web-запросов (запросов к Web-серверу в Интернете) и запрещается — для всех входящих запросов (из Интернета к внутреннему Web-серверу).

Настройка протокола CARP

По умолчанию CARP разрешен для исходящих Web-запросов и запрещен для входящих. То есть по умолчанию ISA-сервер использует CARP для кэширования объектов исходящих Web-запросов на любом из серверов массива, но при включенном обратном кэшировании при публикации серверов объекты входящих Web-запросов кэшируются на одном определенном сервере.

▶ **Включение протокола CARP**

1. В дереве консоли **ISA Management** щелкните правой кнопкой мыши выбранный массив и в контекстном меню выберите **Properties.**

   Откроется диалоговое окно *<имя_массива>* **Properties.**

2. На вкладке **Incoming Web Requests** (входящие Web-запросы) или **Outgoing Web Requests** (исходящие Web-запросы) установите флажок **Resolve requests within array before routing** (разрешать запросы внутри массива до маршрутизации).

Когда член массива определяет, что запрашиваемый объект отсутствует в его кэше, он посылает запрос другому члену массива по внутреннему IP-адресу. Обычно этот IP-адрес не отличается от используемого для взаимодействия с этим ISA-сервером клиентами и другими ISA-серверами. Поскольку этот адрес должен реплицироваться на все ISA-серверы массива, его не рекомендуется изменять.

► **Настройка взаимодействия компьютеров внутри массива**

1. В дереве консоли **ISA Management** щелкните **Computers.**
2. В области сведений щелкните правой кнопкой мыши нужный сервер и в контекстном меню выберите **Properties.** Откроется диалоговое окно свойств выбранного сервера.
3. На вкладке **Array Membership** в текстовом поле введите IP-адрес компьютера внутри массива.
4. Щелкните кнопку OK.

Примечание Чтобы использовать протокол CARP для входящих Web-запросов, убедитесь, что IP-адрес, применяемый для взаимодействия компьютеров внутри массива (по умолчанию это внутренний IP-адрес), «прослушивает» Web-запросы на том же порту, что и IP-адрес, настроенный на прослушивание входящих Web-запросов. (По умолчанию используется порт 80.) Для этого настройте свойства входящих Web-запросов массива на использование одной конфигурации прослушивания всех IP-адресов. Этот параметр устанавливается на вкладке **Incoming Web Requests** диалогового окна свойств массива. Кроме того, разрешается добавить адрес, используемый для взаимодействия компьютеров внутри массива в список прослушивания поступающих Web-запросов.

Настройка коэффициента нагрузки

Как уже говорилось ранее, существует возможность настроить члены массива на обслуживание различной нагрузки. Например, если жесткий диск одного из серверов массива в 4 раза больше, чем у остальных, настройка коэффициента нагрузки позволит добиться, чтобы он хранил и обслуживал во столько же раз больший кэш- Изменяя это значение, вы сможете отрегулировать нагрузку на ISA-сервер.

► **Настройка коэффициента нагрузки**

1. В дереве консоли **ISA Management** щелкните папку **Computers.**
2. В области сведений щелкните правой кнопкой мыши выбранный компьютер и в контекстном меню выберите **Properties** Откроется диалоговое окно свойств сервера.
3. На вкладке **Array Membership** введите в области **Load Factor** значение относительного коэффициента нагрузки.
4. Щелкните кнопку OK.

CARP и загрузка содержимого по расписанию

Выполняя загрузку содержимого по расписанию, ISA-сервер использует параметры CARP для исходящих Web-запросов. Это касается заданий в соответствии с Web-запросами обоих типов: исходящих и входящих. Поэтому, чтобы при загрузке содержимого по расписанию объекты кэшировались на всех серверах массива, рекомендуется отключить CARP для исходящих Web-запросов.

Резюме

ISA-сервер устанавливается как изолированный сервер или как член массива. Для изолированного сервера членство в домене Windows 2000 не обязательно, и на него не действуют политики предприятия. Массивы объединяют несколько ISA-серверов и при соответствующей настройке наследуют политики предприятия. Чтобы создать массив из нескольких серверов, нужно установить первый ISA-сервер как член массива, остальные ISA-серверы присоединяются к созданному массиву. Прежде чем создавать массив, необходимо выполнить процедуру инициализации предприятия — расширить схему службы каталогов Active Directory путем внесения схемы ISA-сервера. Инициализация предприятия также позволяет выдвигать изолированные серверы в члены массива.

Массивы обладают рядом преимуществ перед изолированными серверами, в частности, они более надежны и производительны. При обслуживании клиентов брандмауэра отказоустойчивость достигается путем использования двух и более ISA-серверов совместно с DNS-сервером. В этом случае всем ISA-серверам присваивается одно и то же DNS-имя, а сервер DNS конфигурируется на циклическое обслуживание. При обслуживании клиентов сервером SecureNAT отказоустойчивость достигается использованием двух и более ISA-серверов под управлением *службы балансировки сетевой нагрузки* (Network Load Balancing, NLB). Эта служба поставляется в составе Windows 2000 Advanced Server или Windows 2000 Datacenter Server.

Массивы также позволяют повысить производительность кэширования. Для оптимизации Web-кэширования и маршрутизации Web-запросов применяется протокол CARP (Cache Array Routing Protocol). По умолчанию ISA-сервер использует CARP для кэширования объектов исходящих Web-запросов на всех серверах массива, но объекты, кэшируемые по входящим Web-запросам, хранятся лишь на одном из серверов.

ISA-сервер содержит средства архивирования и восстановления информации о конфигурации массива, в том числе: правил политики доступа, правил публикации, элементов политик, конфигурации оповещений, конфигурации кэша и свойств массива.

Занятие 3. Обеспечение безопасности виртуальных частных сетей средствами ISA-сервера

ISA-сервер применяется для обеспечения безопасности при подключении мобильных пользователей и филиалов с применением *виртуальных частных сетей* (Virtual Private Network, VPN). Для упрощения настройки VPN-подключений используются мастеры ISA-сервера, запуск которых выполняется из узла **Network Configuration** дерева консоли ISA **Management.**

Изучив материал этого занятия, вы сможете:

- ✓ настраивать ISA-сервер для обеспечения безопасного доступа перемещающихся пользователей, которые подключаются через Интернет к сети с ISA-сервером;
- ✓ настраивать ISA-сервер для обеспечения безопасного VPN-подключения филиалов.

Продолжительность занятия - около 35 минут.

Интеграция виртуальных частных сетей с ISA-серверами

При связи компьютеров локальной и удаленной сети через ISA-сервер данные инкапсулируются и отправляются по VPN-туннелю. Для управления туннелями и инкапсуляции частных данных используются протоколы PPTP (Point-to-Point Tunneling Protocol) или L2TP (Layer 2 Tunneling Protocol). Данные, пересылаемые по VPN-подключению, следует шифровать.

На рис. 7-5 показано VPN-подключение двух сетей, в каждой из которых имеется ISA-сервер.

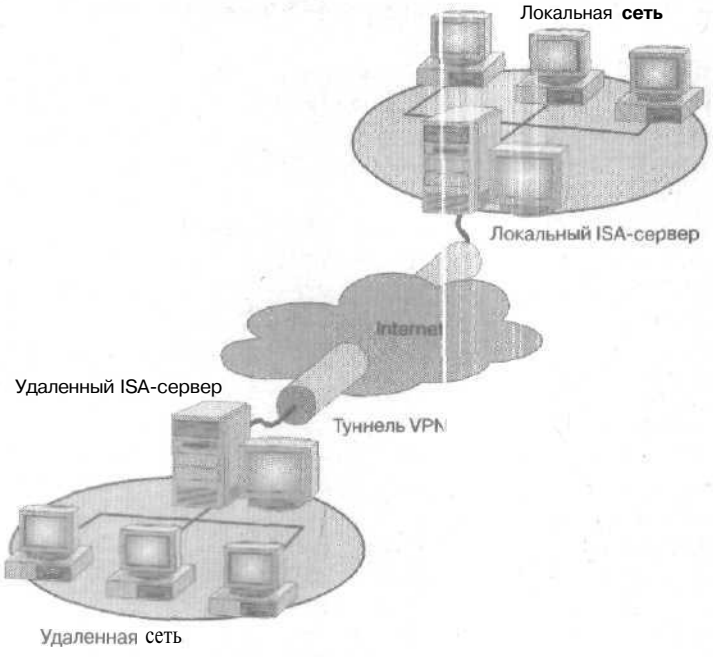


Рис. 7-5. Интеграция VPN-подключения и ISA-серверов

Настройка сети для использования VPN

При использовании VPN ISA-сервер устанавливается в смешанном (Integrated) режиме. На ISA-сервере следует настроить по крайней мере два интерфейса: один — для связи с интернет-провайдером, а другой — для подключения к внутренней сети.

Мастеры ISA-сервера позволяют сконфигурировать его как VPN-сервер и предоставить уделенным пользователям доступ к сетевым ресурсам. Клиентам, подключающимся к ISA-серверу через **VPN,** следует предоставить доступ к таким корпоративным сетевым ресурсам, как DNS и WINS.

Клиенты устанавливают VPN-подключение к удаленному ISA-серверу либо в качестве перемешающихся пользователей, подключающихся через интернет-провайдеров, либо из филиалов — в этом случае связь осуществляется через локальный ISA-сервер.

Перемещаюшиеся пользователи должны, во-первых, настроить соединение с местным провайдером [обычно это подключение по телефонной линии, настраиваемое *к* окне **Network and Dial-up Connections** (Сеть и удаленный доступ к сети)], а во-вторых, сконфигурировать клиент VPN-подключения. Для этого в Windows 2000 нужно запустить мастер Network Connection (Мастер создания сетевого подключения) и выбрать переключатель **Connect to a private network through the internet** (Подключение к виртуальной частной сети через Интернет). Далее следует указать в качестве адреса назначения VPN-подключения адрес ISA-сервера.

Для пользователей филиала, в сети которого работает другой ISA-сервер, для настройки подключения запускают мастеров конфигурации VPN на локальном и удаленном ISA-серверах.

Использование мастеров конфигурации VPN

В состав ISA-сервера входят мастеры, обеспечивающие настройку VPN и механизмов безопасности. Они позволяют сконфигурировать VPN для работы в самых различных ситуациях, например для подключения мобильных пользователей к локальной сети или филиалов между собой.

Для создания VPN-подключений в ISA-сервере предусмотрены три мастера, доступные из контекстного меню узла **Network Configuration** дерева консоли **ISA Management.**

- **Мастер Local ISA Server** VPN — применяется для настройки локального ISA-сервера, принимающего подключения. Локальный ISA-сервер также можно настроить на инициирование подключения к другому компьютеру.
- **Мастер Remote ISA Server VPN** — применяется для настройки удаленного ISA-сервера, инициирующего и принимающего подключения других компьютеров.
- **Мастер ISA Virtual Private Network** — применяется для подключения к VPN перемещающихся пользователей.

Мастер Local ISA Server VPN

Этот мастер позволяет настроить локальный ISA-сервер сети VPN, принимающий подключения от удаленного VPN-сервера на базе ISA. Мастер создает интерфейсы *вызова по требованию* (dial-on-demand), используемые для подключения удаленных серверов к локальному серверу. Кроме того, он позволяет определить фильтры IP-пакетов для защиты подключения (IP-фильтры определяются для конкретных протоколов) и сконфигурировать статические маршруты пересылки трафика локальной сети через туннель в удаленную сеть.

В процессе работы мастер создает файл параметров VPN с расширением .vpc, который затем применяется при настройке удаленного ISA VPN-сервера.

► **Настройка VPN на локальном ISA-сервере**

1. В дереве консоли **ISA Management** щелкните правой кнопкой узел **Network Configuration.**
2. В контекстном меню выберите пункт **Set Up Local ISA VPN Server,** чтобы открыть окно мастера Local ISA Server VPN.
3. Следуйте указаниям мастера.

До запуска мастера Local ISA Server VPN нужно иметь в виду, что:

- в процессе настройки конфигурации система предложит ввести имя домена или удаленного сервера, на котором предполагается создать учетную запись пользователя для VPN-подключения. Если сервер одновременно является контроллером домена, введите имя соответствующего домена. В противном случае укажите NetBIOS-имя компьютера;
- ISA-сервер, установленный в режиме кэширования, нельзя настроить для поддержки VPN.

Мастер Remote ISA Server VPN

Этот мастер позволяет настроить удаленный ISA VPN-сервер, который будет подключаться к локальному ISA VPN-серверу. Он использует VPC-файл, создаваемый мастером Local ISA Server VPN для настройки интерфейсов вызова по требованию, необходимых для инициирования соединения с данным локальным сервером. Кроме того, данный мастер позволяет определить фильтры IP-пакетов для защиты подключения и сконфигурировать статические маршруты для пересылки трафика локальной сети через туннель к узлам удаленной сети.

Конкретные фильтры IP-пакетов зависят от протоколов, выбираемых при создании VPC-файла мастером Local ISA Server VPN.

► **Настройка VPN на удаленном ISA-сервере**

1. В дереве консоли **ISA Management** щелкните правой кнопкой узел **Network Configuration.**
2. В контекстном меню выберите команду **Set up Remote ISA VPN Server,** чтобы открыть окно мастера Remote ISA Server VPN.
3. Следуйте указаниям мастера.

Мастер ISA Virtual Private Network

Этот мастер позволяет установить на ISA-сервере VPN-сервер поддержки перемещающихся клиентов. VPN-сервер поддерживает протоколы PPTP и IPSec/L2TP и открывает соответствующие порты ISA-сервера для доступа клиентов.

► **Настройка ISA-сервера на поддержку VPN-запросов от удаленных клиентов**

1. В дереве консоли **ISA Management** щелкните правой кнопкой узел **Network Configuration.**
2. В контекстном меню выберите команду Allow **VPN Client Connections,** чтобы открыть окно мастера ISA Virtual Private Network.
3. Следуйте указаниям мастера.

Изменение конфигурации VPN

После настройки ISA VPN-сервера часто требуется обеспечить поддержку других протоколов. Например, сервер настроен на работу по протоколу PPTP, однако по прошествии некоторого времени потребовалась поддержка протокола L2TP.

▶ **Настройка на ISA-сервере дополнительных протоколов**

1. В оснастке **Routing and Remote Access** (Маршрутизация и удаленный доступ) найдите нужный сетевой интерфейс.
2. Откройте окно свойств интерфейса и на вкладке **Networking** выберите соответствующий протокол.
3. Для добавления поддержки PPTP в окне оснастки ISA Management в узле **Access Policy** создайте фильтр IP-пакетов, разрешающий использование PPTP.

   Фильтр IP-пакетов следует настроить следующим образом;
   - использовать оба предопределенных фильтра — **PPTP call и PPTP receive;**
   - на вкладке **Local Computer** определить внешний IP-адрес локального ISA VPN-сервера;
   - на вкладке **Remote Computer** указать IP-адрес удаленного ISA VPN-сервера.
4. Для добавления поддержки L2TP создайте два фильтра IP-пакетов. Первый фильтр следует настроить следующим образом:
   - разрешить применение фильтра только к локальному серверу;
   - режим фильтра — **Allow** (разрешить);
   - тип фильтра — **Custom,** протокол — UDP, порт — 500;
   - на вкладке **Local Computer** задать внешний IP-адрес локального ISA VPN-сервера;
   - на вкладке **Remote Computer** указать IP-адрес удаленного ISA VPN-сервера.

   Второй фильтр IP-пакетов должен быть настроен следующим образом:
   - разрешить применение фильтра только к локальному серверу;
   - режим фильтра — **Allow** (разрешить);
   - тип фильтра — **Custom,** протокол — UDP, порт — 1701;
   - на вкладке **Local Computer** указать внешний IP-адрес локального ISA VPN-сервера;
   - . на вкладке **Remote Computer** определить IP-адрес удаленного ISA VPN-сервера.

ISA-сервер и IPSec

При настройке ISA-сервера в качестве VPN-сервера, использующего протокол SPSec/L2TP, включается драйвер IPSec.

При включении IPSec протоколы AH (Authentication Header) и ESP (Encapsulating Security Payload) (IP-протоколы 50 и 51) управляются драйвером IPSec, а не драйвером фильтров пакетов ISA-сервера. Трафиком по туннелю управляет драйвер IPSec. Он гарантирует, что в сеть проходит лишь разрешенный трафик протоколов AH и ESP.

Когда на ISA-сервере не включен драйвер IPSec, управление пакетами выполняется политиками ISA-сервера. Политики ISA-сервера также используются для ведения журналов трафика, проходящего через ISA-сервер, в том числе по протоколам AH и ESP.

Если ISA-сервер настроен на блокирование IP-фрагментов, блокируются все IP-фрагменты, в том числе и фрагменты AH и ESP, даже если IPSec включен,

Пример крупной сети с VPN и маршрутизацией

ISA-сервер часто устанавливается в крупных географически распределенных сетях. Для удовлетворения потребностей пользователей массивы ISA-серверов развертываются в главном офисе и при необходимости — в филиалах. Это позволяет администраторам корпоративной сети обеспечить централизованную политику безопасности и кэширования в масштабе всей корпорации. Развертывание ISA-серверов также позволяет повысить производительность работы филиалов благодаря обслуживанию запросов пользователей к Интернету из локального кэша.

Описание крупной сети с поддержкой VPN

В этом разделе описан пример развертывания ISA-серверов для поддержки виртуальной частной сети крупной корпорации. Штаб-квартира корпорации расположена в США, а два филиала — в Канаде и Великобритании. Требуется обеспечить безопасный доступ к Интернету в соответствии со следующими требованиями:

- правила доступа к Интернету, определенные в штаб-квартире в США, должны применяться во всей корпорации. Они предусматривают доступ всех сотрудников к любым Web-узлам по популярным протоколам Интернета: HTTP, HTTPS (Secure Hypertext Transfer Protocol) и FTP;
- сеть филиала в Великобритании следует защитить дополнительным брандмауэром;
- необходимо минимизировать затраты на подключение британского филиала к штаб-квартире в США;
- ISA-серверы британского филиала должны кэшировать содержимое Web-серверов региона (то есть тех, что размешены в Великобритании);
- в канадском филиале следует разместить кэширующий сервер для снижения интернет-трафика.

Выполнение требований к сети

Поскольку корпорации требуется обеспечить общую политику во всех филиалах, ISA-серверы следует устанавливать как члены массивов во всех филиалах даже при условии, что в некоторых есть лишь один сервер.

Массив ISA-серверов в штаб-квартире в США

Каждый член массива штаб-квартиры оборудован двумя сетевыми адаптерами: один для подключения ко внутренней сети, а другой для подключения к Интернету. Разумно предположить наличие прямого соединения с интернет-провайдером посредством маршрутизатора и линии TI/E1.

Массив ISA-серверов в канадском филиале

ISA-сервер филиала в Канаде используются для снижения сетевого трафика путем кэширования Web-содержимого. Это также позволяет снизить загрузку ISA-серверов в штаб-квартире. ISA-сервер в Канаде установлен в режиме кэширования (Cache) и соединен с ISA-серверами штаб-квартиры. ISA-сервер в Канаде также оборудован двумя сетевыми адаптерами: один подключен к локальному маршрутизатору, а другой — к маршрутизатору штаб-квартиры.

Массив ISA-серверов в британском филиале

ISA-сервер филиала в Великобритании оснащен двумя адаптерами для подключения к локальной сети и модемом или ISDN-адаптером для подключения к Интернету. Пользовательские запросы на Web-серверы, расположенные в Великобритании, направляются через интернет-провайдера. Все остальные запросы пересылаются в штаб-квартиру.

Массив ISA-серверов в Великобритании работает в смешанном (Integrated) режиме, то есть совмещает функции брандмауэра филиала и сервера кэширования. Он подключен к массиву штаб-квартиры через VPN.

Конфигурация сети показана на рис. 7-6.

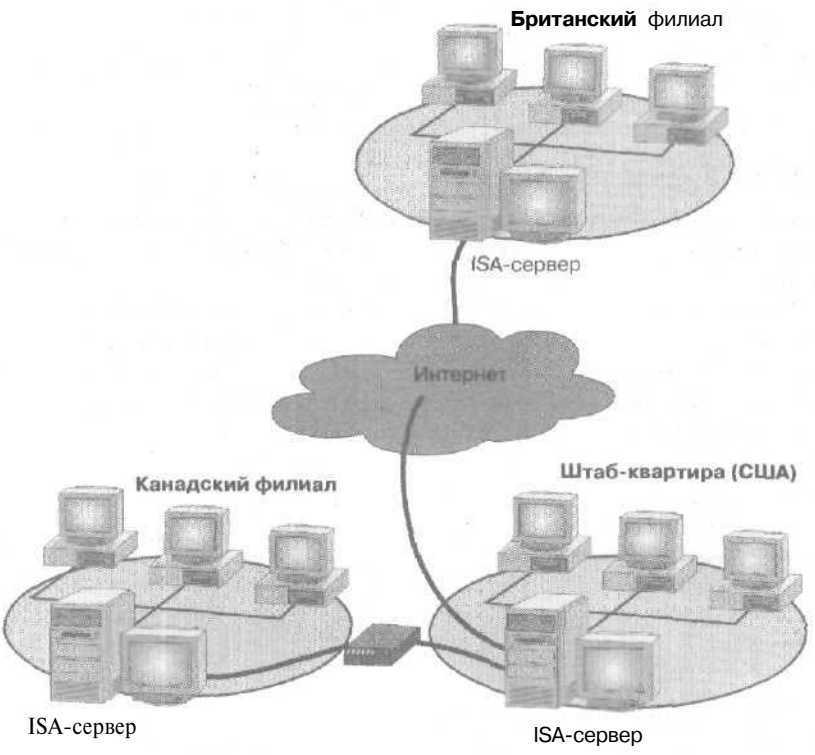


Рис. 7-6. Конфигурация сети с VPN

Политика предприятия в штаб-квартире

После установки ISA-серверов в штаб-квартире администратор средствами оснастки ISA Management определяет и реализует политику предприятия. Она разрабатывается в штаб-квартире и применяется во всех массивах предприятия — в канадском и британском филиалах, а также в самой штаб-квартире.

Чтобы настроить сеть и применить корпоративную политику, администратор предприятия в штаб-квартире выполняет действия, описанные далее.

1. Создает политику предприятия с именем Corporate Policy со следующими правилами:
   - правило узлов и содержимого, разрешающее круглосуточный доступ любых пользователей ко всем Web-узлам;
   - правило протоколов, разрешающее всем пользователям использовать протоколы FTP, HTTP и HTTPS.
2. Устанавливает Corporate Policy в качестве политики по умолчанию, наследуемой всеми филиалами.
3. Настраивает VPN-подключение британского филиала к массиву ISA-серверов штаб-квартиры. Хотя бы один из ISA-серверов в США следует сконфигурировать как VPN-сервер.
4. Добавляет в таблицу LAT американского ISA-сервера диапазон адресов сети в Великобритании.
5. Средствами мастера Local ISA Server VPN настраивает ISA-сервер на прием VPN-подключений. Мастер создает фильтры IP-пакетов в соответствии с выбранным протоко-

лом: L2TP или PPTP. Кроме того, администратор настраивает статические маршруты из локальной к удаленной сети через туннель. И, наконец, создает VPC-файл, который в дальнейшем применяется для настройки ISA-сервера на удаленном VPN-сервере в Великобритании.

Политика ISA-сервера в канадском филиале

Так как ISA-сервер в Канаде входит в сеть штаб-квартиры, для подключения к ISA-серверам штаб-квартиры требуется внешний сетевой адаптер (а не модем).

Политика предприятия по умолчанию автоматически применяется к ISA-серверу в Канаде. Поэтому в канадском филиале не нужно настраивать правила политики доступа.

Задания загрузки содержимого по расписанию настроены на предварительное кэширование определенного Web-содержимого из штаб-квартиры. Это позволяет дополнительно повысить производительность работы сети.

Сетевой администратор в Канаде выполняет следующие действия по настройке локального ISA-сервера.

1. Создает правило маршрутизации для перенаправления запросов клиентов Web-прокси на ISA-сервер в штаб-квартире.
2. Создает задания загрузки содержимого по расписанию, чтобы часто используемые объекты загружались в локальный кэш загодя и при необходимости возвращались клиентам. Запросы отсутствующей в кэше информации ISA-сервер штаб-квартиры перенаправляет в Интернет.

Политика ISA-сервера в британском филиале

Филиал в Великобритании подключен через Интернет посредством VPN к штаб-квартире в США.

Сетевой администратор в Великобритании конфигурирует ISA-сервер в качестве VPN-сервера.

1. Настраивает дополнительный DNS-сервер локальной сети, используемый для разрешения имен корпоративных сетевых доменов, к которым обычно осуществляется доступ. Запросы на разрешение других имен этот DNS-сервер пересылает DNS-серверу, отвечающему за разрешение имен Интернета.
2. Добавляет в таблицу LAT локального ISA-сервера адреса корпоративной сети в США. Любые внешние IP-адреса (адреса Интернета) из этой таблицы исключаются.
3. Средствами мастера Remote ISA Server VPN настраивает ISA-сервер на поддержку VPN. При этом используется VPC-файл, созданный администратором предприятия в штаб-квартире.

   Мастер Remote ISA Server VPN конфигурирует ISA-сервер как VPN-сервер, способный инициировать подключения к удаленным ISA VPN-серверам.
4. Создает правило маршрутизации, по которому все запросы объектов Интернета в Великобритании (с суффиксом .uk в доменном имени) перенаправляются через Интернет, а также правило маршрутизации для перенаправления всех остальных запросов в массив ISA-серверов в штаб-квартире.

Резюме

При связи компьютера локальной сети с компьютером удаленной сети через Интернет при помощи ISA-сервера для управления туннелями и инкапсуляции частных данных применяется один из протоколов — PPTP или L2TP. Обычно такой метод организации подключения называется виртуальной частной сетью (VPN).

В составе ISA-сервера поставляются мастера, помогающие настраивать VPN и механизм безопасности частных сетей. Они облегчают подключение перемещающихся пользователей к локальной сети или филиалов друг с другом.

Мастер Local ISA Server VPN позволяет сконфигурировать локальный ISA-сервер на инициирование и прием подключений. Мастер Remote ISA Server VPN применяется для настройки удаленного ISA-сервера на инициирование и прием подключений. Мастер ISA Virtual Private Network используется для подключения к VPN перемешающихся пользователей.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Ответы для самопроверки — в приложении А «Вопросы и ответы» в конце книги.

1. Вы создали политику предприятия и хотите применить ее к массиву Branch1. Какие возможны варианты применения политики предприятия к массиву? При каких условиях удаляются политики уровня массива? В каких случаях применить политику предприятия к массиву невозможно?

2. Как изменить политику предприятия по умолчанию, если она уже действует в существующих массивах?

3. Как разрешить компьютеру — члену массива обрабатывать больше сетевых запросов, чем другие компьютеры массива?

4. Обязательно ли устанавливать изолированные ISA-серверы в домене? Можно ли применить политику предприятия к изолированному ISA-серверу?

5. В составе ISA-сервера поставляются три мастера, упрощающие настройку VPN. Расскажите, для чего используется каждый из них.

ГЛАВА 8

Безопасные видеоконференции с применением привратника H.323 Gatekeeper

Занятие 1. Настройка клиентов для использования привратника H.323 Gatekeeper 234

Занятие 2, Маршрутизация вызовов конференций средствами H.323 Gatekeeper 244

Закрепление материала 255

В этой главе

Стандарт H.323 представляет собой набор протоколов для проведения интерактивных видеоконференций в реальном времени в простых и сложных сетях. Как правило, клиенты, которые работают в сетях, защищенных брандмауэрами, достаточно трудно настроить для работы по стандарту H.323 из-за сложности и динамической природы подключений H.323. Для упрощения проведения безопасных видеоконференций используется привратник Microsoft H.323 Gatekeeper, который поддерживает работу с брандмауэром на базе ISA-сервера и его фильтром приложений H.323. После регистрации клиентов на H.323 Gatekeeper управление видеоконференциями на основе правил маршрутизации и других форм управления осуществляется так же легко, как и контроль любого другого сетевого трафика.

Прежде всего

Для изучения материалов этой главы необходимо:

- выполнить процедуры установки, описанные в разделе «Об этой книге»;
- выполнить все задания глав 1–4.

Замятие 1. Настройка клиентов для использования привратника H.323 Gatekeeper

Привратник H.323 Gatekeeper упрощает вызов участников конференций и позволяет проводить сеансы связи в реальном времени через брандмауэр ISA-сервера, Чтобы воспользоваться преимуществами привратника H.323 Gatekeeper, нужно прежде всего зарегистрировать на нем клиенты H.323 (например Microsoft NetMeeting 3.0).

Изучив материал этого **занятия**, вы сможете:

- ✓ описать средства для поддержки видеоконференций, обеспечиваемые H.323 Gatekeeper;
- ✓ регистрировать клиенты на H.323 Gatekeeper.

Продолжительность **занятия** – около 40 минут.

Протокол H.323

Стандарт H.323 — это набор протоколов, разработанный *Международным союзом телекоммуникаций* (International Telecommunications Union, ITU) для проведения видеоконференций в самых различных сетевых окружениях. H.323 поддерживает обмен мультимедийной информацией в реальном времени даже в сетях, не обеспечивающих *гарантированного качества обслуживания* (quality of service, QoS). Кроме того, H.323 позволяет создавать мосты аудио- и видеосеансов из сетей коммутации пакетов, например из Интернета или интрасетей, в сети коммутации каналов или сотовой коммутации, такие как ISDN, ATM или телефонные сети общего пользования. Например, клиент H.323 может позвонить по телефонному номеру общедоступной телефонной сети. Стандарт H.323 предусматривает также возможность связи между телефоном общедоступной сети и компьютером.

В протоколе H.323 предусмотрено четыре основных компонента системы проведения сетевых конференций: терминалы, шлюзы, привратники и узлы управления многосторонней связью. Терминалы — это клиентские конечные точки локальной сети, на которых выполняются совместимые с H.323 приложения, например NetMeeting 3.0. Шлюз H.323 обеспечивает взаимодействие между сегью, поддерживающей H.323, и сетью, не поддерживающей H.323, например телефонной сетью общего пользования. *Привратник* (gatekeeper) является центральным узлом конференции и обеспечивает управление вызовами и их маршрутизацию между зарегистрированными конечными точками. *Узел управления многосторонней связью* (multipoint control unit, MCU) позволяет проводить конференции между тремя и более конечными точками.

Привратник H.323 Gatekeeper

Привратник H.323 Gatekeeper является центральной точкой сети H.323. Благодаря взаимодействию с фильтром протокола H.323 он предоставляет зарегистрированным клиентам услуги по разрешению адресов, аутентификации и маршрутизации вызовов. Зарегистрированные клиенты используют H.323 Gatekeeper для участия в конференциях по обмену данными, аудио- и видеоинформацией в сетях любого типа: локальных или глобальных, защищенных брандмауэрами, а также в Интернете. Кроме того, H.323 Gatekeeper используется для «интеллектуальной» маршрутизации вызовов, основанной на адресе вызываемой стороны.

Оснастка H.323 Gatekeepers

Для управления привратником H.323 Gatekeeper применяется оснастка H.323 Gatekeepers. После установки H.323 Gatekeeper она доступна в узле дерева консоли ISA Management. В процессе полной установки ISA-сервера в дереве консоли создается узел **H.323 Gatekeepers**, тем не менее для использования оснастки H.323 Gatekeepers необходимо создать новый привратник. Для этого щелкните правой кнопкой мыши узел **H.323 Gatekeepers** и в контекстном меню выберите команду **Add gatekeeper.**

После добавления привратника оснастка H.323 Gatekeepers становится доступной для конфигурирования правил маршрутизации вызовов на уровне телефонных номеров, *псевдонимов* (alias) пользователей или IP-адресов. Кроме того, она применяется для регистрации статических пользователей и определения адресатов для правил маршрутизации, которые планируется создать позже.

Примеры использования H.323 Gatekeeper

В приведенных далее примерах показаны различные варианты связи в реальном времени по схеме «точка — точка» и многосторонних конференций с применением H.323 Gatekeeper.

Конференция с участием пользователей одного предприятия

В этом примере многочисленные пользователи одной организации применяют совместимые с H.323 приложения, например NetMeeting версии не ниже 3.0. В сети установлены и запушены ISA-сервер и привратник H.323 Gatekeeper. Пользователи регистрируются на H.323 Gatekeeper, указывая известный псевдоним (например адрес электронной почты) и телефонный номер. Они вызывают друг друга по псевдониму или телефонному номеру и могут обменяться аудио- и видеоданными, данными по стандарту T.120 (многосторонними), а также совместно использовать приложения.

На рис. 8-1 показана схема проведения конференции внутри предприятия с применением H.323 Gatekeeper.

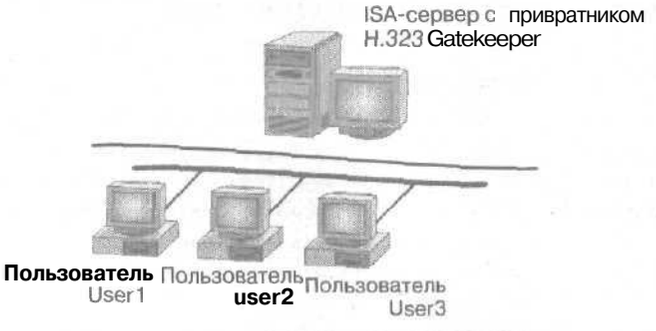


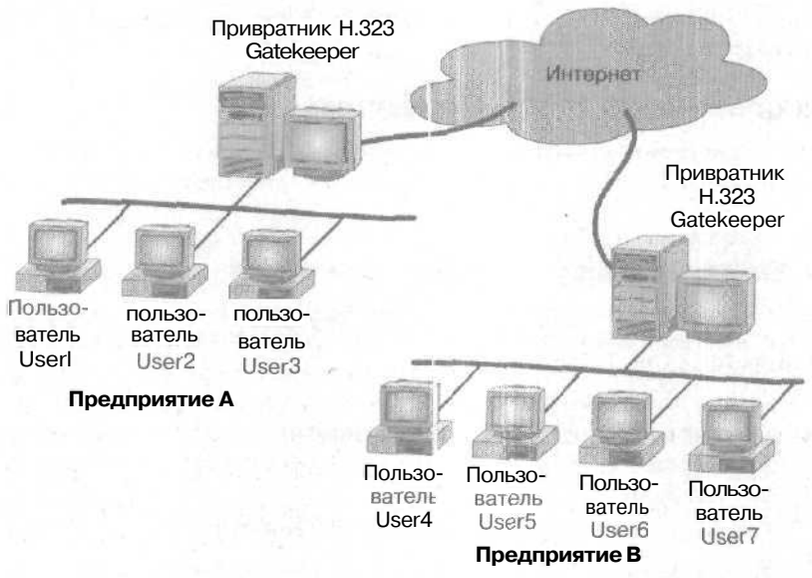
Рис. 8-1. Проведение конференций с участием пользователей одного предприятия

Конференция с участием пользователей разных предприятий

В этом примере многочисленные пользователи двух организаций применяют совместимые с H.323 приложения, например NetMeeting версии не ниже 3.0. В обеих организациях установлены и запущены ISA-сервер (в режиме брандмауэра), привратник H.323 Galekeeper и фильтр протокола H.323. Пользователи регистрируются на своем привратнике H.323 Gatekeeper, указывая известный псевдоним. Любой пользователь одной организации мо-

жет вызвать любого пользователя другой организации по его псевдониму и обменяться с ним аудио- и видеоинформацией, данными по стандарту T. 120, а также совместно использовать приложения. Например, чтобы связаться с пользователем User4, пользователю User1 достаточно ввести в диалоговом окне **Place A Call** (Создание вызова) программы NetMeeting 3.0 адрес электронной почты *User4@organizationB.microsoft.com* и щелкнуть кнопку **Call** (Вызвать). Пользователь User4 получит вызов независимо от его местоположения в сети предприятия B. При этом IP-адрес User4 скрыт от User1 и остальных пользователей предприятия A.

На рис. 8-2 показана схема проведения конференции между предприятиями е применением привратника H.323 Gatekeeper.



Рнс. 8-2. Проведение конференций с участием пользователей разных предприятий

Вызов по телефонной сети общего пользования

Телефонная сеть обшего пользования представляет собой сеть коммутации каналов, оптимизированную для передачи голосовой информации в реальном времени. При вызове абонента выполняется набор номера, что вызывает замыкание коммутатора и организацию прямого канала связи с абонентом. Телефонная сеть гарантирует качество обслуживания, обеспечивая поддержку канала вызова абонента на все время сеанса связи, причем поддержка канала не зависит от того, ведется ли разговор с абонентом, или оба участника разговора молчат.

В данном примере многочисленные пользователи организации пользуются совместимыми с H.323 приложения, например NetMeeting 3.0. В сети установлен и запущен привратник H.323 Gatekeeper, Пользователи регистрируются на H.323 Gatekeeper, указывая известный псевдоним (например адрес электронной почты) и телефонный номер. Кроме того, в сети установлен и запущен шлюз H.323, конфигурация которого позволяет H.323 Gatekeeper выполнять прямые вызовы между IP-сетями и телефонными сетями. Пользователи имеют возможность выполнять звонки на телефоны общего пользования, набирая номер прямо на компьютере в программе NetMeeting, а также принимать звонки из телефонной сети (при условии наличия NetMeeting версии не ниже 3,0).

На рис. 8-3 показана схема проведения конференции с участием клиентов H.323 и абонентов общедоступной телефонной сети,

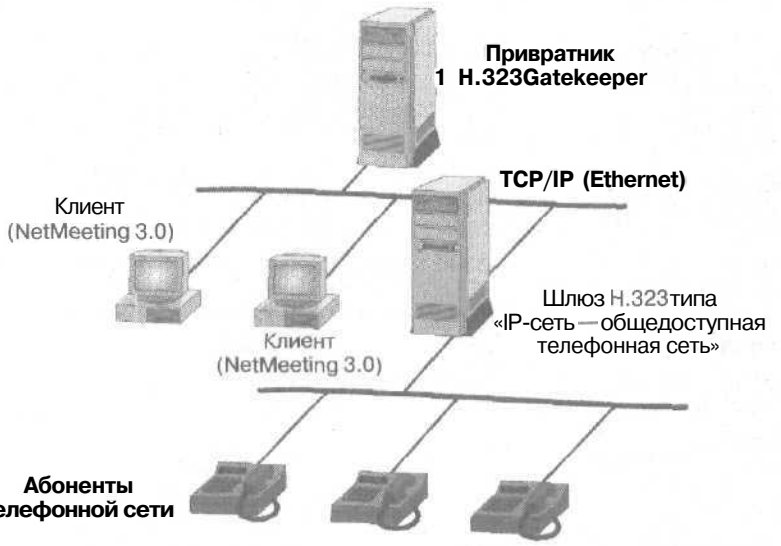


Рис. 8-3. Проведение конференции с участием пользователей IP-сети и абонентов телефонной сети

Регистрация клиентов на H.323 Gatekeeper

Каждое взаимодействие (транзакция) по протоколу H.323 имеет две конечных точки: исходную и точку назначения. В качестве конечных точек обычно выступают клиент H.323 (например терминал с NetMeeting), прокси-сервер (например ISA-сервер со службой Web-прокси) или шлюз. Конечные точки H.323 Gatekeeper обычно регистрирует автоматически по протоколу H.323 RAS (H.323 Registration, Admission, and Status protocol — протокол регистрации, доступа и состояния в H.323). Конечные точки, не поддерживающие регистрацию по механизму H.323 RAS, регистрируются статически средствами оснастки H.323 Gatekeepers.

Примечание Статически зарегистрированные клиенты не способны принимать входящие вызовы.

Привратник H.323 Gatekeeper поддерживает три типа адресации по механизму H.323 RAS:

- **адресация на основании телефонных номеров E164,** в которой используются цифры из диапазона 0–9;
- **адресация на основании идентификаторов H.323 (H323-ID),** в которой применяются такие строки, как адреса электронной почты или DNS-адреса, содержашие имена учетных записей или имена компьютеров. Синтаксис для этого типа адресации не определен;
- **адресация на основании идентификаторов электронной почты (Email-ID).**

Атрибуты конечных точек

При регистрации конечной точки по протоколу H.323 RAS указываются следующие атрибуты:

- **адрес конечной точки в формате Q931** — в вызовах по **H.323** этот адрес представляет собой сочетание IP-адреса конечной точки и порта, используемого для связи по протоколу H.323 (порт по умолчанию - 1720). Например, 192.168.0.2:1720 и 10.0.0.5:1720 представляют собой допустимые адреса Q931;

Примечание Протокол Q.931 является протоколом управления подключениями, который применяется для создания подключений и разбивки данных на кадры. Он аналогичен протоколу TCP и используется для управления созданием и разрывом подключений при вызовах по протоколу **H.323.**

- **RAS-адрес конечной точки** — состоит из IP-адреса и номера порта, используемого для связи по протоколу RAS. Кроме того, каждому зарегистрированному терминалу присваивается уникальный номер **RAS** ID;
- **список** псевдонимов.

Псевдонимы

Псевдоним (alias) состоит из двух полей — типа и имени, причем тип — это E164, H323-ID или Email-ID.

Например, при регистрации NetMeeting-клиента на H.323 Gatekeeper, как показано на рис. 8-4, имя учетной записи регистрируется на H.323 Gatekeeper как псевдоним типа H323-ID, а номер телефона — как псевдоним типа E164.

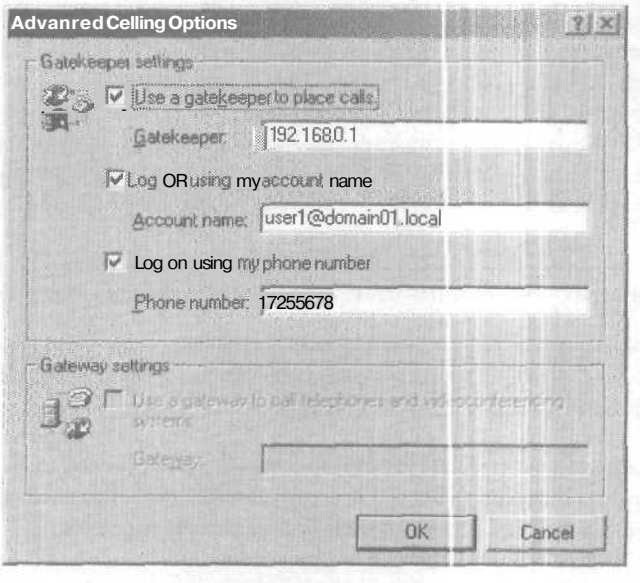


Рис. 8-4. Поля NetMeeting, используемые для регистрации на H.323 Gatekeeper

При выборе узла Active **Terminals в** дереве консоли **ISA** Management псевдонимы H323-ID (или Email-ID) и E164 отображаются в области сведений в столбцах **Account и Phone** соответственно. Все зарегистрированные псевдонимы отображаются на странице свойств.

Чтобы открыть страницу свойств, щелкните правой кнопкой мыши нужный терминал и выберите в контекстном меню команду **Properties.** На рис. 8-5 показано диалоговое окно свойств терминала, зарегистрированного NetMeeting-клиентом, показанным на рис. 8-4.

Примечание Регистрируемые на H.323 Gatekeeper адреса формата Q931 должны быть уникальными, однако это не значит, что запрещены одинаковые псевдонимы. Допустимость не- с- кольких регистрации одного и того же псевдонима с уникальным адресом Q931 позволяет клиенту регистрироваться с различных терминалов. Активна только самая последняя регистрация псевдонима, и она применяется при разрешении запросов к псевдониму.

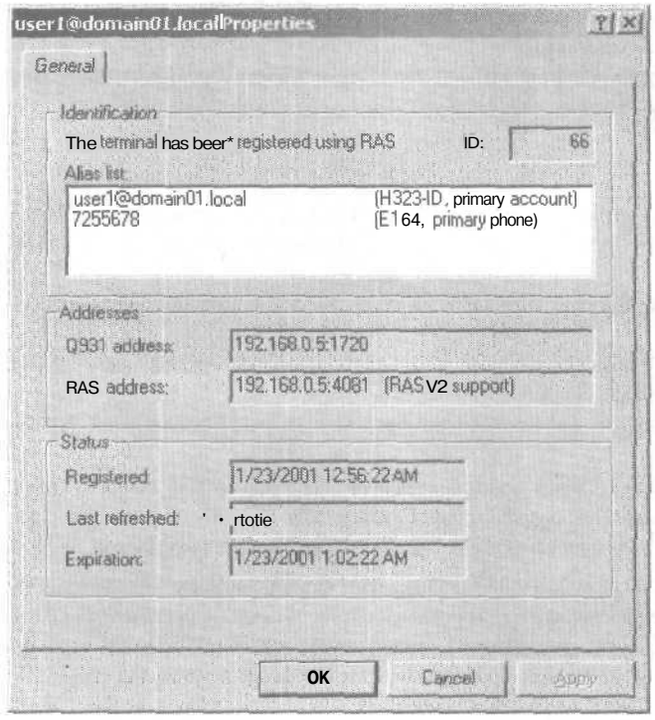


Рис. 8-5. Псевдонимы NetMeeting-клиента типов E164 и H.323-ID

Преобразование адресов клиентов

Чтобы клиент стал доступным по определенному псевдониму, ему следует зарегистрироваться на H.323 Gatekeeper. (В качестве такого «известного» псевдонима часто используется адрес электронной почты, например *someone@microsoft.com.)* Кроме того, необходимо зарегистрироваться на привратнике H.323 Gatekeeper, если требуется преобразование при исходящих вызовах, например, когда NetMeeting версии не ниже 3.0 обращается к абоненту телефонной сети.

Примечание Исходящие вызовы, не требующие преобразования, разрешается выполнять без помощи H.323 Gatekeeper.

Допустим, вы находитесь в офисе своей компании и хотите связаться по Интернету с адресатом по имени Someone, который работает в Microsoft и зарегистрировался на H.323 Gatekeeper компании Microsoft под псевдонимом *someone@microsoft.com*. Регистрация на H.323 Gatekeeper позволяет связаться с ним по известному псевдониму *someone@microsoft.com*, даже если в действительности такого адреса электронной почты не существует. В следующих разделах описано, как происходят вызов абонента *someone@microsoft.com* средствами NetMeeting 3.0.

В сети компании клиента

1. NetMeeting 3.0 подключается к H.323 Gatekeeper компании клиента.
2. H.323 Gatekeeper устанавливает, что microsoft.com не является внутренним адресом, и пересылает вызов ISA-серверу компании.
3. ISA-сервер находит адрес microsoft.com и выполняет запрос адреса microsoft.com через Интернет.

В сети компании-адресата

1. Получив запрос абонента *someone@microsoft.com*, ISA-сервер в сети корпорации Microsoft обращается к внутреннему привратнику H.323 Gatekeeper за локальным адресом вызываемого абонента.
2. H.323 Gatekeeper корпорации Microsoft преобразует псевдоним в сетевой адрес и возвращает его ISA-серверу.
3. ISA-сервер корпорации Microsoft отправляет подтверждение ISA-серверу компании клиента и создает подключение.
4. С этого момента и до окончания связи ISA-сервер поддерживает созданный H.323 Gatekeeper канал связи.
5. У Someone не обязательно должен быть действительный, доступный для маршрутизации извне IP-адрес. Локальный ISA-сервер скроет его от других конечных точек, так как H.323 Gatekeeper выполняет преобразование адресов внутренних клиентов.

Конфигурированием фильтра приложений H.323 на ISA-сервере можно управлять, то есть разрешить или запретить передачу аудио- и видеоданных, данных стандарта T.120 и совместное использование данных приложениями. Также существует возможность установить ограничения по времени и расписанию доступности связи по протоколу H.323.

Установка привратника H.323 Gatekeeper

При полной установке ISA-сервера (то есть при выборе варианта **Full Installation**) **H.323** Gatekeeper устанавливается автоматически. В противном случае его можно установить вручную в любой удобный момент.

► **Установка H.323 Gatekeeper**

1. В меню **Start** (Пуск) перейдите к **Settings** (Настройка) и щелкните команду **Control Panel** (Панель управления). Дважды щелкните значок **Add/Remove Programs** (Установка и удаление программ).
2. В списке **Currently Installed Programs** (Установленные программы) шелкните **Microsoft Internet Security And Acceleration Server** и затем — кнопку **Change** (Заменить).
3. В окне **Microsoft ISA Server (Enterprise Edition) Setup** щелкните кнопку **Add/Remove.**
4. В диалоговом окне **Custom Installation** выберите **Add-in services** и затем шелкните кнопку **Change Option.**
5. Выделите флажком **Install H.323 Gatekeeper Service** и щелкните кнопку **OK.**
6. Для завершения установки щелкните кнопку **Continue.**

Перед установкой или конфигурированием H.323 Gatekeeper следует иметь в виду следующие сособенности:

- H.323 Gatekeeper не обеспечивает какой бы то ни было защиты;
- при удаленном управлении ISA-сервером или H.323 Gatekeeper с компьютера, работающего под управлением Microsoft Windows 2000 Professional, вы не получите доступ ко всем инструментам и разделам справочной системы, пока не установлен ISA-сервер и пакет инструментальных средств H.323 Gatekeeper Administration Tools;
- H.323 Gatekeeper не требует уникальности псевдонимов, используемых при регистрации, но все Q931-адреса должны быть уникальными. H.323 Gatekeeper применяет для каждого псевдонима только последний зарегистрированный активный терминал, что позволяет пользователям регистрироваться под одним псевдонимом из разных мест;
- фильтр приложений H.323 не поддерживает передачу данных по протоколу H.225 через ISA-сервер. Например, пользователь NetMeeting 3.0, находящийся в локальной сети, не сможет зарегистрироваться на привратнике в Интернете. Аналогичным образом H.323 Gatekeeper локальной сети не сможет обмениваться *запросами на поиск* (location request) с привратником в Интернете;
- ISA-сервер поддерживает быструю подкачку аудио и видео в режиме ядра по протоколу RTP (Real-Time Transport Protocol), если вызов пользователей через ISA-сервер выполняется с NetMeeting версии не ниже 3.0.

Практикум. Настройка клиента для использования H.323 Gatekeeper

Чтобы обеспечить клиентам H.323 возможность вызывать друг друга по псевдонимам, а не IP-адресам, необходимо зарегистрировать клиентов на привратнике H.323 Gatekeeper. Сейчас вы добавите привратник в существующую копию ISA-сервера и настроите NetMeeting для выполнения вызовов через привратник. Затем вы проверите корректность регистрации псевдонима клиента на H.323 Gatekeeper.

Предполагается, что выполнена полная установка ISA-сервера и создано правило протокола, разрешающее любой IP-трафик. Также необходимо, чтобы в домене существовал пользователь с именем User1. Предполагается также, что учетная запись User1 создана в соответствии с инструкциями, указанными в практикуме главы 4.

Задание 1. Добавление привратника

При полной установке ISA-сервера в дереве консоли ISA Management имеется узел **H.323 Gatekeepers,** однако, чтобы его использовать, необходимо добавить привратник.

▶ **Добавление привратника**

1. Войдите в систему Server1 под учетной записью Administrator (Администратор).
2. В дереве консоли ISA Management щелкните правой кнопкой мыши узел H.323 Gatekeepers и в контекстном меню выберите **Add gatekeeper.** Откроется диалоговое окно **Add Gatekeeper.**
3. Оставьте переключатель в положении **This computer** и щелкните кнопку **OK.**
4. В дереве консоли у узла **H.323 Gatekeepers** появится подузел **Server1.**

Задание 2. Регистрация NetMeeting на H.323 Gatekeeper

Протокол H.323 RAS обеспечивает автоматическую регистрацию терминалов (клиентов) H.323 на H.323 Gatekeeper. Чтобы зарегистрировать клиент на базе NetMeeting, необходимо просто настроить его для пересылки вызовов через привратник. В этом задании вы сначала настроите NetMeeting, а затем зарегистрируете клиент на H.323 Gatekeeper.

► **Регистрация NetMeeting на H.323 Gatekeeper**

1. Войдите в домен domain01 с сервера Server2 под учетной записью User1.
2. В меню **Start** (Пуск) последовательно перейдите **к Programs** (Программы), **Accessories** (Стандартные), **Communications** (Связь) и щелкните значок **NetMeeting.**
3. В окне программы **NetMeeting,** описывающем ее возможности, щелкните кнопку **Next** (Далее). Откроется окно, предлагающее вам ввести информацию о себе.
4. В поле **First Name** (Имя) введите **Test.**
5. В поле **Last Name** (Фамилия) введите **User.**
6. В поле **Email Address** (Электр. почта) введите *testuser@domain01.local.*
7. Щелкните кнопку **Next** (Далее). Откроется окно, предлагающее ввести информацию о сервере каталогов.
8. Сбросьте флажок **Log on to a directory server when NetMeeting starts** (Подключаться к серверу каталогов при запуске).
9. Щелкните кнопку **Next** (Далее). Откроется окно, предлагающее указать скорость подключения.
10. Выберите переключатель **Local Area Network** (Локальная сеть).
11. Щелкните кнопку Next (Далее). Откроется окно, в котором можно создать ярлыки для рабочего стола и области быстрого запуска панели задач.
12. Щелкните кнопку **Next** (Далее). Откроется окно мастера **Audio Tuning** (Мастер настройки звука).
13. В этом и всех остальных окнах щелкайте кнопку **Next** (Далее), принимая параметры по умолчанию и игнорируя предупреждающие сообщения, относящиеся к качеству работы звуковой карты, микрофона или аудиосистемы.
14. Щелкните кнопку **Finish** (Готово) для выхода из мастера **Audio Tuning.** Откроется консоль **NetMeeting — Not in a Call** (Microsoft NetMeeting — нет связи).
15. В консоли **NetMeeting — Not In A Call** последовательно выберите пункты меню **Tools** (Сервис) и **Options** (Параметры). Откроется диалоговое окно **Options.** (Параметры)
16. Щелкните кнопку **Advanced Calling** (Расширенный вызов). Откроется диалоговое окно **Advanced Calling Options** (Расширенные параметры вызова).
17. Установите флажок Use **a gatekeeper to place calls** (Использовать привратника для вызовов).
18. В поле **Gatekeeper** (Привратник) введите **server1.**
19. Установите флажок **Log on using my account name** (Регистрация моей учетной записи).
20. В поле **Account Name** (Имя учетной записи) введите **MyName.**
21. Щелкните кнопку OK.
22. В диалоговом окне **Options** также щелкните кнопку OK.

Задание 3. Проверка конфигурации

В этом задании вы просмотрите в консоли ISA Management список активных терминалов H.323, чтобы проверить, распознал ли привратник NetMeeting-клиента.

► **Проверка конфигурации**

1. На компьютере Server1 откройте консоль ISA Management.
2. В дереве консоли последовательно раскройте узлы **H.323 Gatekeepers и Server1.**

3. В дереве консоли щелкните значок **Active Terminals.** В области сведений должен отображаться значок терминала MyName. Наличие значка свидетельствует, что клиент MyName готов отправлять и принимать вызовы через привратник H.323 Gatekeeper.

Резюме

H.323 — это стандарт, разработанный ITU для проведения интерактивных видеоконференций в реальном времени в различных сетевых средах. H.323 Gatekeeper ISA-сервера является центральной точкой сети, поддерживающей работу по протоколу H.323 и обеспечивающей зарегистрированным клиентам услуги по разрешению адресов, аутентификации и маршрутизации вызовов. Кроме того, H.323 Gatekeeper позволяет поддерживающим H.323 клиентам проводить конференции через Интернет в сетях, защищенных брандмауэром ISA-сервера. NetMeeting версии не ниже 3.0 является примером клиента с поддержкой H.323.

Любой клиент, желающий стать доступным по псевдониму, а не IP-адресу, должен зарегистрироваться на H.323 Gatekeeper. Обычно клиенты регистрируются автоматически по протоколу H.323 **RAS.** Кроме того, средства оснастки H.323 Gatekeepers позволяют статически зарегистрировать конечные точки, не поддерживающие регистрацию с применением H.323 RAS. Привратник H.323 Gatekeeper поддерживает три типа псевдонимов; E164 (телефонный номер), H.323-ID (открытый синтаксис, допускающий адреса электронной почты, строки DNS, имена учетных записей и компьютеров) и Email-ID (формат адресов электронной почты).

Для управления H.323 Gatekeeper применяется оснастка H.323 Gatekeepers, которая доступна в виде отдельного узла H.323 Gatekeepers дерева консоли ISA Management. При полной установке ISA-сервера (то есть при выборе варианта **Full Installation)** H.323 Gatekeeper устанавливается автоматически. Привратник H.323 Gatekeeper также можно установить вручную в любой удобный момент.

Занятие 2. Маршрутизация вызовов конференций средствами H.323 Gatekeeper

Клиенты H.323 (в том числе на базе NetMeeting 3.0) регистрируются на H.323 Gatekeeper под псевдонимами, которые более удобны для запоминания, чем IP-адрес. В качестве псевдонима обычно применяется имя пользователя или адрес электронной почты. Правила маршрутизации необходимы привратнику H.323 Gatekeeper для разрешения псевдонимов и определения, нужна ли маршрутизация вызовов конференций и, если да, то на какой адрес.

Изучив материал этого занятия, вы сможете:

- ✓ рассказать о назначении правил маршрутизации вызовов;
- ✓ объяснить, как H.323 Gatekeeper обрабатывает правила маршрутизации вызовов;
- ✓ настраивать правила маршрутизации вызовов H.323 Gatekeeper для переадресации вызовов конференций.

Продолжительность занятия - около 45 минут.

Правила маршрутизации вызовов

Для поддержки конференций между конечными точками в реальном времени H.323 Gatekeeper должен «знать», как выполнять маршрутизацию вызовов адресатов по псевдонимам. Правила маршрутизации вызолов H.323 сопоставляют адресата и параметры маршрутизации запрашиваемому псевдониму или его части. Если в запросе вызова не указан уникальный Q931-адрес, H.323 Gatekeeper сравнивает каждое из правил маршрутизации H.323 с запрашиваемым псевдонимом.

На рис. 8-6 показаны типы правил маршрутизации и параметры, которые можно для них настроить в оснастке H.323 Gatekeepers. Правила маршрутизации вызовов, используемые H.323 Gatekeeper по умолчанию, разрешают все запрашиваемые адресаты, которые указаны в локальной регистрационной базе данных или расположены в локальной сети. Это означает, что для проведения видеоконференций только в своей локальной сети не требуется создавать никаких дополнительных правил маршрутизации.

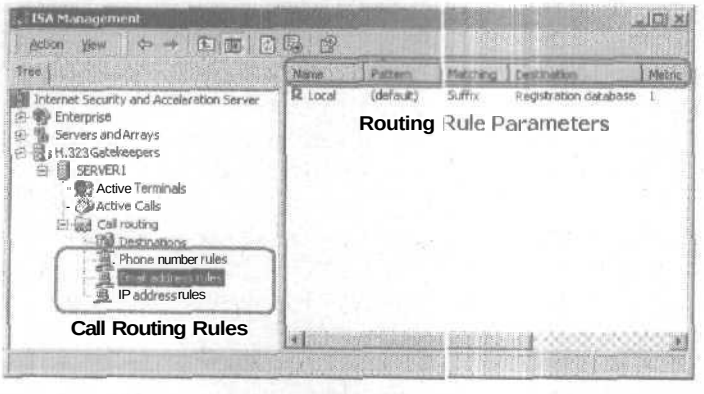


Рис. 8-6. Правила маршрутизации вызовов и их параметры

Создание правила маршрутизации

1. В дереве консоли ISA Management раскройте папку **Call Routing.**
2. Выполните одно из следующих действий:
   - для создания правила телефонных номеров щелкните правой кнопкой папку **Phone number** rules, выберите в контекстном меню **Add routing rule** и следуйте инструкциям мастера New Routing Rule;
   - для создания правила адресов электронной почты щелкните правой кнопкой мыши значок **Email address rules,** выберите в контекстном меню **Add routing rule** и следуйте инструкциям мастера New Routing Rule;
   - для создания правила IP-адресов щелкните правой кнопкой мыши значок **IP address** rules, выберите в контекстном меню **Add routing rule** и следуйте инструкциям мастера New Routing Rule.

Далее мы расскажем о том, как H.323 Gatekeeper выполняет поиск *псевдонима* зарегистрированного активного терминала в правилах маршрутизации.

Правила телефонных номеров

В правилах телефонных номеров (E164) указываются параметры, перечисленные в таблице 8-1. В скобках указаны имена параметров, используемые в мастере New Routing Rule, если они отличаются от заголовков соответствующих столбцов в области сведений оснастки ISA Management.

Таблица 8-1. Параметры правил телефонных номеров

Параметр	Описание
Name	Имя правила
Description	Пояснение для данного правила
Pattern (Prefix or phone number)	Строка сопоставления — образец (шаблон) строки для телефонных номеров, к которым применяется данное правило
Matching (флажок Route all phone numbers using this prefix)	Режим сопоставления. Указывает, как определять, соответствует ли номер параметру Pattern, — при совпадении строки с началом телефонного номера (тип Prefix) или точном совпадении строки со всем телефонным номером (тип Exact). Выбору параметра Prefix соответствует установка флажка **Route all phone numbers** using this **prefix** в мастере New Routing Rule. В противном случае используется проверка точного соответствия
Destination type	Сервер, на который маршрутизируется вызов в соответствии с данным правилом
Discard digits	Количество цифр, удаляемых из телефонного номера перед маршрутизацией. Применяется лишь к телефонным номерам (E164) или адресатам-шлюзам
Add prefix	Префикс, добавляемый к телефонному номеру. Применяется лишь к телефонным номерам (E164) или адресатам-шлюзам
Metric	Используется для определения положения данного правила по отношению к остальным правилам. Чем меньше Metric, тем раньше обрабатывается правило
Status	Указывает, активно или отключено данное правило

В *процессе* обработки вызова H.323 Gatekeeper определяет правила, соответствующие псевдониму, указанному в запросе. Псевдонимы в виде телефонного номера могут состоять из цифр 0–9, знаков «решетка» (#), «звездочка» (*) и запятой (,).

Примеры правил телефонных номеров

Предположим, клиент, осуществляющий вызов, запрашивает преобразование телефонного номера 95551234#3344.

H.323 Gatekeeper сравнивает цифры последовательно, пока не встретится специальный символ или конец строки. Таким образом, для телефонного номера 95551234#3344 псевдонимом, используемым для сопоставления с правилами, является строка 95551234.

В таблицах 8-2 и 8-3 приведены примеры образцов строк и режимов сопоставления, используемых в правилах телефонных номеров.

Как показано в таблице 8-1, при установке режима Prefix строка сопоставления правила маршрутизации считается совпадающей, если она совпадает с первыми цифрами псевдонима на основе телефонного номера. В режиме Exact строка сопоставления считается совпадающей, если совпадает весь телефонный номер. Следует иметь в виду, что в режиме Prefix пустая строка или строка нулевой длины всегда считается совпадающей.

Примечание Режим Prefix устанавливается, если установлен флажок **Route all phone numbers using this prefix.** В противном случае устанавливается режим Exact.

В таблице 8-2 показаны примеры правил, соответствующих номеру 95551234#3344. В первых трех примерах сравниваются строки в режиме Prefix и выявляются те, которые совпадают с префиксом данного номера. При сопоставлении в режиме Exact существует лишь одна-единственная строка, совпадающая с псевдонимом на основе телефонного номера. В последнем примере сравнивается пустая строка в режиме Prefix — такая строка в указанном режиме совпадает с любым псевдонимом на основе телефонного номера. Именно поэтому правило телефонных номеров по умолчанию предусматривает режим Prefix и содержит пустую строку.

Таблица 8-2. Примеры правил телефонных номеров, соответствующих номеру 95551234#3344

Строка сопоставления	Режим сопоставления (Matching)
9	Prefix
9555	Prefix
95551234	Exact
<пусто>	Prefix

В таблице 8-3 показаны примеры строк, не соответствующих номеру 95551234#3344. В первом примере строка «8» не соответствует номеру, который начинается с цифры 9. Во втором примере строка «9555» сравнивается в режиме Exact и поэтому не совпадает с номером, так как точный псевдоним на основе телефонного номера — 95551234, а не 9555.

Таблица 8-3. Примеры правил телефонных номеров, не соответствующих номеру 95551234#3344

Строка сопоставления	Режим сопоставления (Matching)
8	Prefix
9555	Exact

Правила IP-адресов

Правила IP-адресов применяются только для запросов на преобразование строк IP-адресов вида a.b.c.d., например 192.168.154.13.

Параметры правил IP-адресов перечислены в таблице 8-4.

Таблица 8-4. Параметры правил IP-адресов

Параметр	Описание
Name	Имя правила
Description	Описание правила
Pattern	Строка сопоставления IP-адреса, с которой выполняется сравнение. Содержит маску подсети
Destination	Адресат, к которому маршрутизируется запрос вызова при условии применимости данного правила
Metric	Используется для определения положения данного правила по отношению к остальным правилам. Чем меньше Metric, тем раньше обрабатывается правило
Status	Указывает, активно или отключено данное правило

Когда IP-адрес соответствует критериям правила и правило активно, выполняется маршрутизация вызова адресату, указанному в правиле IP-адресов. В правилах IP-адресов разрешается указывать следующие типы адресатов:

- **None (no destination)** — адресат не указан, поэтому соответствующий вызов отключается;
- **Gateway or proxy** server — вызов переадресуется указанному шлюзу H.323, прокси-серверу или брандмауэру Интернета;
- **Gatekeeper** — вызов переадресуется привратнику, расположенному в другой зоне;
- **Multicast group** — вызов переадресуется группе привратников многоадресной рассылки;
- **Local network** — вызываемый клиент расположен в одной локальной сети с вызывающим. Вызов возвращается для разрешения вызывающему клиенту.

Пример разрешения на основе правил IP-адресов

Допустим, вызывающий клиент запросил трансляцию строки адреса вида a.b.c.d. После сравнения цифр этой строки с адресами, указанными в правилах IP-адресов, H.323 Gatekeeper обнаружил три подходящих правила.

После определения применимых правил маршрутизации выполняется их сортировка по следующим правилам:

- правила с большим количеетвом бит в маске подсети обладают приоритетом по отношению к правилам с меньшим количеством бит в маске подсети. Например, строка IP-адреса 192.168.154.13 с маской подсети 255.255.255.192 имеет большее количество бит в маске подсети, чем та же строка IP-адреса 192.168.154.13 с маской подсети 255.255.255.0;
- если два правила содержат одинаковые адреса, правило с меньшим значением параметра Metric обладает приоритетом перед правилом с большим значением.

Правила адресов электронной почты

Параметры правил адресов электронной почты перечислены в таблице 8-5. В скобках указаны имена параметров, используемые в мастере New Routing Rule, если они отличаются от заголовков соответствующих столбцов в области сведений оснастки ISA Management.

Таблица 8-5. Параметры правил адресов электронной почты

Параметр	Описание
Name	Имя правила
Description	**Описание** правила
Pattern (DNS domain name)	Текстовая строка для сопоставления
Matching (флажок Route all e-mail addresses that include this general DNS domain name)	Режим сопоставления. Указывает, как определять, соответствует ли адрес параметру Pattern — при совпадении строки с суффиксом адреса (тип Suffix) или точном совпадении строки с доменной частью адреса электронной почты (тип Exact). Под суффиксом обычно подразумевается часть адреса электронной почты, следующая после знака «собака» (@). Параметр Suffix выбирается, когда установлен флажок **Route all e-mail addresses that include this** general DNS **domain name.** В противном случае используется проверка точного соответствия
Destination	Сервер, на который маршрутизируется запрос вызова при условии, что данное правило можно применять
Metric	Используется для определения положения данного правила по отношению к остальным правилам. Чем меньше Metric, тем раньше обрабатывается правило
Status	Указывает, активно или отключено данное правило

При проверке правил маршрутизации H.323 Gatekeeper выполняет сравнение доменной части псевдонима на основе адреса электронной почты. В таблице 8-6 показано, как из псевдонима выделяется доменная часть.

Таблица 8-6. Доменные части некоторых псевдонимов

Пример псевдонима	Доменная часть
Someone@microsoft.com	microsoft.com
accountingl.microsoft.com	accounting1.microsoft.com
accounting1	Невозможно выделить

Примечание Псевдоним accounting1 является примером так называемого «бесточечного» псевдонима. Это нестандартный форма" псевдонима.

В таблице 8-7 приведены примеры четырех правил адресов электронной почты, которые применимы к псевдониму *someone@microsoft.com*. В первых двух примерах указан режим сопоставления Suffix, а соответствие обеспечивается тем, что суффиксы «com» и «microsoft.com» соответствуют доменной части. В третьем примере псевдоним также содержит суффикс «microsoft.com», причем он полностью совпадает с доменной частью, поэтому соответствие обеспечивается даже в режиме Exact. Это единственная строка, которая соответствует *someone@microsoft.com* в режиме Exact. В четвертом примере пустая строка в режиме сопоставления Suffix соответствует любому псевдониму на основе адреса электронной почты. Правило адресов электронной почты по умолчанию предусматривает режим Suffix и содержит пустую строку.

Таблица 8-7. Примеры правил адресов электронной почты, соответствующих адресу *someone@microsoft.com*

Строка сопоставления	Режим сопоставления (Matching)
Com	Suffix
microsoft.com	Suffix
microsoft.com	Exact
<пустая строка>	Suffix

Правила с параметрами, перечисленными в таблице 8-8, не соответствуют псевдониму *someone@microsoft.com*. Указанные примеры предусматривают режим сопоставления Exact строк («com» и пустой строки), которые не равны в точности доменной части псевдонима.

Таблица 8-8. Примеры правил адресов электронной почты, не соответствующих адресу *someone@microsoft.com*

Строка сопоставления	Режим сопоставления (Matching)
Com	Exact
<пустая строка>	Exact

Если псевдоним запроса состоит из someone и пустой доменной части, единственными правилами, соответствующими такой доменной части, являются правила, перечисленные в таблице 8-9.

Таблица 8-9. Примеры правил адресов электронной почты, соответствующих бесточечному псевдониму

Строка сопоставления	Режим сопоставления (Matching)
<пустая строка>	Exact
<пустая строка>	Suffix

После определения применимых правил маршрутизации привратник выполняет их сортировку по следующим правилам:

- правила, содержащие больше доменных элементов, обладают приоритетом по отношению к правилам, содержащим меньше доменных элементов. Например, правило со строкой «accountingl.accounting.microsoft.com» приоритетнее, чем правило со строкой «microsoft.com»;
- если два правила содержат одну и ту же строку сопоставления, правило с режимом сопоставления Exact приоритетнее, чем правило с режимом Suffix;
- если два правила содержат одинаковые строку и режим сопоставления, правило с меньшим значением параметра Metric приоритетнее правила с большим значением Metric.

Обработка правил и адресаты

После создания упорядоченного списка правил, соответствующих указанному при вызове псевдониму, H.323 Gatekeeper обрабатывает правила последовательно в указанном порядке. Порядок обработки правил зависит от указанных в них типов адресатов.

Правила маршрутизации вызовов служат для указания адресата. В правилах разрешается указывать один из перечисленных далее девяти типов адресатов. Чтобы создать пра-

вило с конкретным шлюзом или прокси-сервером, сервером со службой ILS (Internet Locator Service), привратником или их группой в качестве адресата, нужно предварительно воспользоваться мастером Add Destination и создать соответствующий адресат (или адресаты). Для запуска мастера Add Destination щелкните правой кнопкой мыши узел **Destinations** в оснастке H.323 Gatekeepers и выберите в контекстном меню команду Add Destination.

Адресат None (no destination)

Данный адресат применяется для остановки обработки правил. Даже если после правила с таким адресатом и есть другие применимые для данного псевдонима правила с меньшими значениями параметра Metric, H.323 Gittekeeper отвергает запрос и возвращает сообщение о невозможности разрешения («Cannot be resolved»).

Адресат Registration database

Данный адресат предусматривает поиск псевдонима в локальной регистрационной базе данных. Для псевдонима типа E164 привратник H.323 Gatekeeper ищет телефонный номер до первого специального символа, не включая этот символ. Например, для исходной строки 95551212#3344 H.323 Gatekeeper выполнит поиск только 95551212. Сопоставление IP-адреса на основании сведений базы данных выполняется по этой строке.

Для псевдонимов типа Email-ID или H323-ID выполняется поиск всего псевдонима, а не только его доменной части. Так как эти два типа взаимозаменяемы, адрес пользователя, зарегистрированного под псевдонимом *someone@microsoft.com* типа Email-ID, удастся успешно разрешить в запросе, в котором указан псевдоним *someone@microsoft.com* типа H323-ID, и наоборот. Если удается найти запись о пользователе, в качестве подтверждения клиенту возвращается адрес, и обработка правил останавливается. В противном случае обработка продолжается со следующего правила.

Данный тип адресата нельзя использовать для псевдонимов в виде IP-адресов.

Адресат Gateway or proxy server

Адресат данного типа указывает на конкретный прокси-сервер или шлюз H.323 и содержит список IP-, DNS- или NetBIOS-адресов. Шлюзы H.323 необходимы, когда требуется маршрутизация вызова через общедоступную телефонную сеть. В состав ISA-сервера шлюз H.323 не входит.

В сетях с несколькими прокси-серверами или шлюзами для разрешения имени H.323 Gatekeeper случайным образом выбирает из списка один IP-адрес. Случайная выборка IP-адресов позволяет H.323 Gatekeeper балансировать сетевую загрузку сети между несколькими прокси-серверами и шлюзами. Полученный адрес возвращается клиенту. Дальнейшей отправкой вызова и подключением к возвращенному адресу клиент занимается самостоятельно. Если удается найти нужную запись, в качестве подтверждения клиенту возвращается адрес и обработка правил останавливается. В противном случае обработка продолжается, начиная со следующего правила.

Адресат ILS server

Адресат данного типа указывает на Microsoft Site Server со службой разрешения имен Internet Locator Service, который применяется только для разрешения запросов пространства имен адресов электронной почты. Этот формат не является общеупотребительным и предназначен для обратной совместимости.

Сначала H.323 Gatekeeper выполняет разрешение имени, чтобы получить IP-адрес сервера, на котором работает служба ILS. Затем при необходимости H.323 Gatekeeper запрашивает сам сервер.

H.323 Gatekeeper выполняет по крайней мере один запрос, указывая полный псевдоним. Если запрос оказался неудачным, а псевдоним имеет стандартный формат адреса электронной почты в виде *someone@microsoft.com*, привратник H.323 Gatekeeper извлекает имя пользователя и снова запрашивает ILS, чтобы найти записи, начинающиеся с «someone». Это позволяет клиенту, пытающемуся найти запись, соответствующую псевдониму *someone@microsoft.com,* обнаружить записи ILS вида *someone@accounting5.accounting.microsoft.com.* Если ни один из запросов не возвратил нужную запись, H.323 Gatekeeper переходит к обработке следующего правила.

Адресат Gatekeeper

Адресат этого типа указывает IP-, DNS- или NetBIOS-адрес другого привратника H.323 Gatekeeper. Локальный H.323 Gatekeeper разрешает имя, пытаясь определить IP-адрес привратника-адресата. Затем локальный привратник отправляет удаленному привратнику специальный *запрос на поиск* (location request). Получив запрос на поиск, привратник H.323 Gatekeeper пытается разрешить псевдоним на основании сведений локальной регистрационной базы независимо от имеющихся правил. Если удаленный H.323 Gatekeeper возвращает Q931-адрес, локальный H.323 Gatekeeper пересылает его клиенту. В противном случае обработка правил продолжается.

Адресат Multicast group

В качестве адресата указывается группа многоадресной рассылки. H.323 Gatekeeper отправляет запрос на поиск по протоколу групповой рассылки. H.323 Gatekeeper прослушивает и обрабатывает поступающие запросы на поиск только по группе многоадресной рассылки 224.0.1.41, даже если существуют другие такие группы. Если удается найти нужную запись, в качестве подтверждения адрес возвращается клиенту и обработка правил прекращается. В противном случае обработка продолжается со следующего правила.

Адресат DNS

Этот тип адресата используется только для запросов по адресам электронной почты. H.323 Gatekeeper разрешает доменную часть псевдонима средствами DNS и игнорирует имя пользователя. Например, в *someone@microsoft.com* доменной частью псевдонима является microsoft.com. Если запись найдена, адрес возвращается клиенту в качестве подтверждения и обработка правил прекращается. В противном случае обработка продолжается со следующего правила.

Адресат Active Directory

Active Directory указывается в качестве адресата только в правилах адресов электронной почты. Когда адресатом является база данных Active Directory, она опрашивается на предмет наличия атрибута ipPhone, соответствующего объекту пользователя, и осуществляется маршрутизация вызова на этот номер TP-телефона.

Адресат Local network

Этот тип адресата допускается только для псевдонимов в виде IP-адресов. Привратник H.323 Gatekeeper возвращает адрес, содержащийся в псевдониме. Так как разрешение или трансляция не требуются и адрес назначения достижим напрямую, в качестве адреса запроса используется IP-адрес, содержащийся в запрашиваемом псевдониме.

Применение правил к запросам

В данном разделе приведены примеры применения правил маршрутизации к входящим и исходящимвызовам,

Входящие вызовы

Получив входящий запрос, привратник H.323 Gatekeeper сначала определяет тип псевдонима — E164, H.323-ID или Email-ID, а затем сравнивает псевдоним с имеющимися правилами, отбирает те из них, которые соответствуют псевдониму, и сортирует по возрастанию параметра Metric. Привратник обрабатывает правила в порядке отсортированного списка, пока не удастся разрешить псевдоним или не окажется, что поиск безрезультатен. В конце, в зависимости от того, удалось найти адрес или нет, H.323 Gatekeeper отправляет клиенту подтверждение или отказ.

В частности, так обрабатываются запросы адресов электронной почты. Допустим, вы сотрудник Microsoft и при помощи Net Meeting 3.0 хотите связаться с другим сотрудником Microsoft по его псевдониму на основе адреса электронной почты *someone@microsoft.com.*

Привратник H.323 Gatekeeper отправляется *запрос на доступ* (admission request) к псевдониму *someone@microsoft.com.* При этом он просматривает список правил (таблица 8-10).

Таблица 8-10. Пример полного списка правил

Домен	Параметр сопоставления	Имя правила	Относительное значение параметра Metric
Microsoft.com	Suffix	Registration database (регистрационная база данных)	1
Microsoft.com	Suffix	Gatekeeper «otherzone» (привратниц, находящийся в другой зоне)	2
Microsoft.com	Suffix	ILS Server named «Bogus» (ILS-сервер «Bogus»)	3
Microsoft.com	Suffix	Aclive Directory	4
Microsoft.com	Suffix	None (cannot beresolved) (невозможно разрешить)	6
<пустая строка>	Suffix	Gateway/Proxy named «Bogus2» (шлюз или прокси-сервер «Bogus2»)	10
<пустая строка>	Exact	Registration database (регистрационная база данных)	2
<пустая строка>	Exact	None (cannot beresolved) (невозможно разрешить)	10

Отобрав и отсортировав правила, соответствующие доменной части microsoft.com, H.323 Gatekeeper создает список, показанный в таблице 8-11.

Таблица 8-11. Правила, соответствующие псевдониму

Домен	Параметр сопоставления	Имя правила	Относительное значение параметра Metric
rnicrosoft.com	Suffix	Registration database	1
microsoft.com	Suffix	Gatekeeper «otherzone»	2
microsoft.com	Suffix	ILS Server named «Bogus»	3
microsoft.com	Suffix	Active Directory	4
microsoft.com	Suffix	None (cannot be resolved)	6
<пустая строка>	Suffix	Gateway/Proxy named «Bogus2»	10

H.323 Gatekeeper сначала обрабатывает первое правило и пытается найти псевдоним *someone@microsofl.com в* локальной регистрационной базе данных. Если такой псевдоним зарегистрирован, H.323 Gatekeeper возвращает клиенту подтверждение вместе с найденным адресом. Если адрес найти не удалось, H.323 Gatekeeper продолжает поиск и переходит для разрешения запроса к правилу Gatekeeper «otherzone». Привратник H.323 Gatekeeper обрабатывает список сверху вниз, пока не получает адрес или не дойдет до правила None (cannot be resolved). В последнем случае запрос оказывается неразрешенным, и клиент получает сообщение «Cannot be resolved». После того как привратник доходит до правила None (cannot be resolved) никаких других правил он не обрабатывает, причем такое поведение никак не зависит от значения параметра Metric.

Исходящие вызовы

Инициируя исходящий вызов, зарегистрированный клиент направляет привратнику H.323 Gatekeeper запрос на доступ, в котором указывает псевдоним адресата. Если привратнику H.323 Gatekeeper удается разрешить адрес, соответствующий псевдониму адресата, он направляет клиенту подтверждение доступа и найденный адрес. В противном случае H.323 Gatekeeper продолжает обработку правил по списку, пытаясь разрешить запрос.

Исходящий запрос в другой домен перенаправляется удаленному ISA-серверу и разрешается в удаленной сети. Этот процесс иллюстрируется следующим примером.

Допустим, клиент в компании Acme, использующий NetMeeting 3.0, вызывает абонента *someone@microsoft.com.* Предположим, доменное имя внешнее или неизвестно привратнику H.323 Gatekeeper и первым соответствующим псевдониму оказывается правило, указанное в таблице 8-12.

Таблица 8-12. Пример отсортированного списка правил

Домен	Параметр сопоставления	Имя правила	Взвешенное значение параметра Metric
<пустая строка>	Suffix	Gateway/Proxy named «Outbound» (шлюз или прокси-сервер с именем «Outbound»)	10

Привратник H.323 Gatekeeper информирует ISA-сервер, что адрес является внешним по отношению к сети, и ISA-сервер инициирует разрешение имени средствами DNS. Если в результате запроса возвращается полное доменное имя компьютера, H.323 Gatekeeper инициирует дополнительный DNS-запрос на разрешение IP-адреса адресата.

Резюме

Правила маршрутизации вызовов позволяют привратнику H.323 Gatekeeper разрешать имена псевдонимов и определять, нужна ли маршрутизация вызовов видеоконференций и, если да, то на какой адрес. Если в запрос вызова не указан глобально уникальный IP-адрес, привратник H.323 Gatekeeper выполняет сопоставление запрашиваемого псевдонима и всех имеющихся правил маршрутизации.

Существует три вида правил маршрутизации вызовов: правила телефонных номеров, правила адресов электронной почты и правила IP-адресов. В правилах телефонных номеров указаны строки телефонных номеров, которые используются для сопоставления с псевдонимами на основе телефонных номеров и определения применимости тех или иных правил. В правилах адресов электронной почты указываются суффиксы доменных имен, которые используются для определения того, применимы ли правила к псевдонимам H.323-ID. Правила IP-адресов сопоставляются IP-адресами и служат для переадресации вызова определенным адресатам. После определения списка правил маршрутизации, соответствующих псевдониму, H.323 Gatekeeper сортирует правила для дальнейшей обработки.

Получив входящий запрос, привратник H.323 Gatekeeper сначала определяет тип псевдонима — E164, H.323-ID или Email-ID, а затем сравнивает псевдоним с имеющимися правилами, отбирает те из них, которые соответствуют псевдониму, и сортирует по возрастанию параметра Metric. Привратник обрабатывает правила в порядке отсортированного списка, пока не удастся разрешить псевдоним или не окажется, что поиск безрезультатен. В зависимости от того, удалось найти адрес или нет, H.323 Gatekeeper отправляет клиенту подтверждение или отказ.

Инициируя исходящий вызов, зарегистрированный клиент направляет привратнику H.323 Gatekeeper запрос на доступ, в котором указывает псевдоним адресата. Если привратнику H.323 Gatekeeper удается разрешить адрес, соответствующий псевдониму адресата, он направляет клиенту подтверждение доступа и найденный адрес. В противном случае H.323 Gatekeeper продолжает обработку правил по списку, пытаясь разрешить запрос.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Ответы для самопроверки — в приложении А «Вопросы и ответы» в конце книги.

1. Какие четыре основных компонента определены в стандарте H.323, созданном для поддержки сетевых интерактивных видеоконференций в реальном времени?

2. Какие функции выполняет H.323 Gatekeeper при обслуживании клиентов видеоконференций по протоколу H.323?

3. Опишите, что происходит, когда клиент H.323, зарегистрированный на привратнике H.323 Gatekeeper одной сети, вызывает по псевдониму на основе адреса электронной почты клиент H.323, зарегистрированный на H.323 Gatekeeper другой сети.

4. Клиент H.323 пытается вызвать другой клиент по псевдониму *someone@microsoft.com*. Этому псевдониму соответствует два правила адресов электронной почты. Первое правило предусматривает режим сопоставления Suffix, содержит строку сопоставления «microsoft.com» и значение его параметра Metric — 4. Второе правило предусматривает режим сопоставления Exact, содержит строку microsoft.com, а его параметр Metric равен 5. Какое из этих правил будет использовано для обработки вызова?

5. Каковы преимущества правила маршрутизации с типом адресата Gateway?

ГЛАВА 9

Контроль и оптимизация производительности ISA-сервера

Занятие 1. Настройка оповещений 258

Занятие 2. Ведение журнала работы ISA-сервера 267

Занятие 3, Создание отчетов ISA-сервера 283

Занятие 4. Управление пропускной способностью 292

Занятие 5. Дополнительные средства настройки и наблюдения 300

Закрепление материала 317

В этой главе

В составе ISA-сервера поставляется множество средств мониторинга, оптимизации и настройки производительности. Узел **Monitoring Configuration** в оснастке ISA Management предоставляет инструменты для настройки оповещений, журналов и отчетов. Кроме того, политики пропускной способности позволяют управлять подключениями, проходящими через ISA-сервер, и оптимизировать их производительность путем назначения приоритетов различным видам трафика в соответствии с любыми определяемыми администратором критериями. ISA-сервер также настраивается в соответствии с ожидаемым количеством ежедневных подключений. Производительность кэша обычно оптимизируется путем регулирования объема оперативной памяти, выделенной для хранения Web-содержимого. И, наконец, ISA-сервер содержит множество объектов и счетчиков, которые применяются для наблюдения за различными параметрами работы системы как в реальном времени, так и с применением отчетов, журналов и оповещений в оснастке Performance (Производительность) в Windows 2000.

Прежде всего

Для изучения материалов этой главы необходимо:

- выполнить процедуры установки, описанные в разделе «Об этой книге»;
- выполнить все упражнения глав 1–8.

Занятие 1. Настройка оповещений

Служба оповещений ISA-сервера отвечает за регистрацию событий, проверку наличия определенных условий и выполнение соответствующих действий. В окне оснастки ISA Management отображается список всех событий ISA-сервера, которым вы вправе сопоставлять какое-либо действие.

Изучив материал этого занятия, вы сможете:

- ✓ просматривать сообщения о событиях ISA-сервера в оснастке Event Viewer (Просмотр событий);
- ✓ просматривать оповещения ISA-сервера в окне оснастки ISA Management;
- ✓ настраивать критерии, местоположение и пороги инициации оповещений, а также ответные действия.

Продолжительность занятия — около 35 минут.

Предустановленные оповещения

По умолчанию ISA-сервер поставляется с 45 оповещениями, 39 из которых включены. Список этих оповещений отображается в папке **Alerts** узла **Monitoring Configuration** в оснастке ISA Management (рис. 9-1).

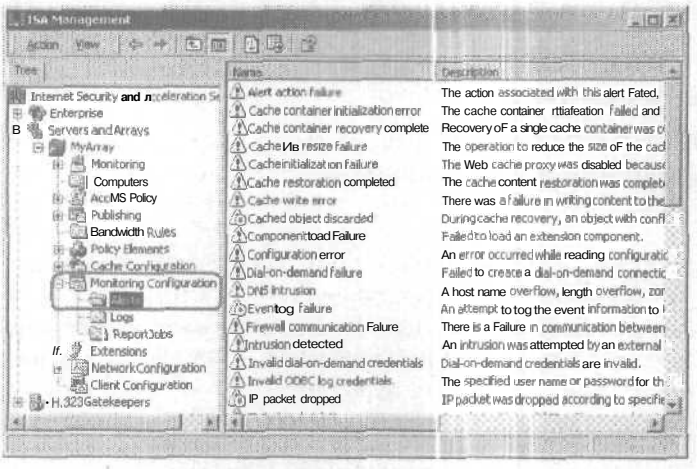


Рис. 9-1. Предустановленные оповещения ISA-сервера

▶ **Включение оповещения**

1. В дереве консоли ISA Management разверните узел **Monitoring Configuration** и выберите папку **Alerts.**
2. В области сведений щелкните правой кнопкой мыши нужное событие и в контекстном меню выберите команду **Enable.**

Каждое оповещение сопоставляется определенному событию ISA-сервера. По умолчанию при возникновении события, сопоставленного включенному оповещению, создается запись в журнале событий Windows 2000. Эти записи доступны для просмотра в **Application Log** (Журнал приложений) оснастки **Event Viewer** (Просмотр событий). На рис. 9-2 показан пример журнала событий Windows 2000 с записями о событиях ISA-сервера.

Примечание Список событий ISA-сервера также хранится в папке **Alert** узла **Monitoring** в окне консоли ISA Management, однако здесь отображается только первое событие с момента предыдущего останова. Для получения полной информации о событиях следует воспользоваться оснасткой Event Viewer.

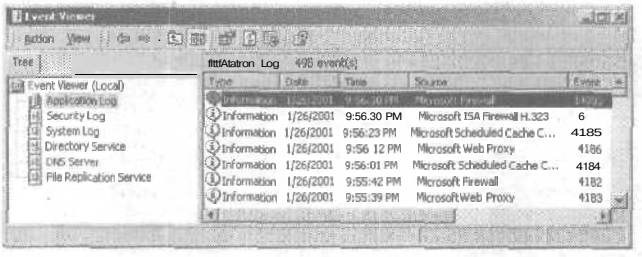


Рис. 9-2. События ISA-сервера в Event Viewer

Администраторы могут создавать новые или изменять существующие оповещения, Новые оповещения создаются средствами мастера New **Alert wizard.**

▶ **Создание нового оповещения**

В дереве консоли ISA Management разверните узел **Monitoring Configuration**.

1. Щелкните правой кнопкой мыши папку **Alert, в** открывшемся меню выберите New и в развернувшемся списке выберите команду **Alert.**
2. Последовательно выполняйте инструкции мастера.

Условия возникновения оповещения

Новые оповещения создаются на основе существующих, но обычно они содержат дополнительные, более точные условия, при выполнении которых инициируется оповещение, Например, оповещение о нарушениях в работе доменной системы имен обычно возникает при любом виде атаки на DNS (в дополнительных условиях инициирования оповещения **DNS intrusion** выбран вариант **Any DNS Intrusion).** Однако на основе этого оповещения можно создать специальное оповещение о переполнении буфера имен узлов. Для этого достаточно в качестве события, при котором возникает оповещение, выбрать вариант **DNS Intrusion,** и дополнительным условием определить **Host Overflow** (рис. 9-3). Так изменяются условия любого предустановленного оповещения.

▶ **Изменение условий инициирования оповещения**

1. В дереве консоли ISA Management разверните узел **Monitoring Configuration** и щелкните папку **Alerts.**
2. В области сведений щелкните правой кнопкой мыши нужное оповещение и выберите команду **Properties.**
3. На вкладке **Events:**
   - в поле со списком **Event** выберите событие, при возникновении которого инициируется оповещение;
   - если для инициирования оповещения требуются дополнительные условия, выберите их в списке **Additional condition;**
   - в поле со списком **By Server** выберите сервер, события которого должны отслеживаться, или, если следует наблюдать за всеми серверами массива, оставьте вариант **<Any>**.

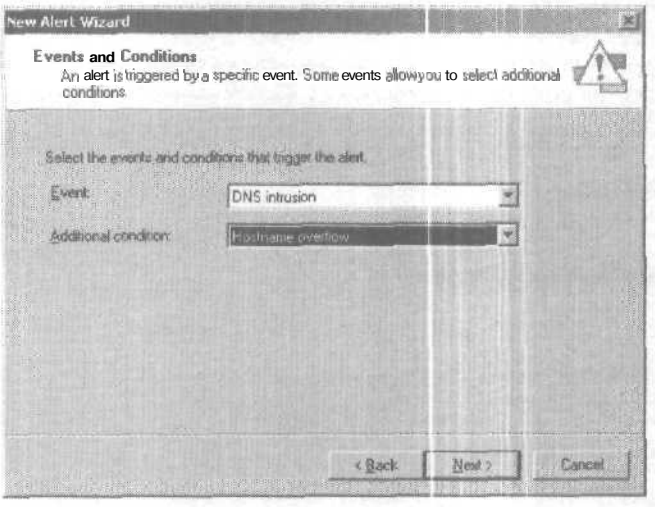


Рис. 9-3. Создание оповещения о переполнении буфера имен узлов

Местоположение события

Иногда создают оповещение, возникающее при тех же условиях, что и любое из предустановленных, но только для конкретного сервера массива. Компьютер, на котором обнаружено соответствующее событие, называется *местоположением события* (event location). По умолчанию все предустановленные оповещения отслеживают события на всех серверах массива, хотя ничто не мешает вам изменить параметры оповещения для реагирования на события лишь одного или определенного подмножества серверов.

Порог инициирования оповещения

После настройки оповещения определяется порог, при котором оно инициируется. В качестве порога задается:

- число событий в секунду, при котором инициируется оповещение (частотный порог события);
- число событий до инициирования оповещения;
- время до инициации повторного оповещения.

Пороги оповещений настраиваются на вкладке Events диалогового окна **Properties** (см. рис. 9-4) соответствующего оповещения.

▶ **Настройка порогов инициирования оповещений**

1. В дереве консоли ISA Management разверните узел **Monitoring Configuration** и щелкните папку **Alerts**.
2. В области сведений щелкните правой кнопкой мыши нужное оповещение и выберите команду **Properties.**
3. На вкладке **Events** установите флажок **Number of occurrences before the alert is issued** и укажите, после какого числа событий инициируется оповещение.
4. Установите флажок **Number of events per second before the alert is issued** и введите частоту возникновения события (число событий в секунду), при которой инициируется оповещение.
5. Выберите один из следующих вариантов:

- если при повторном возникновении события оповещение должно инициироваться немедленно, установите переключатель в положение **Immediately;**
- если новое оповещение *должно* инициироваться только после сброса *предыдущего*, установите переключатель в положение **After manual reset of alert;**
- если повторное оповещение должно инициироваться по истечении определенного периода времени, установите переключатель в положение **If time since last execution is more than** *<число_минут>* **minutes и** укажите число минут, по истечении которого инициируется повторное оповещение.

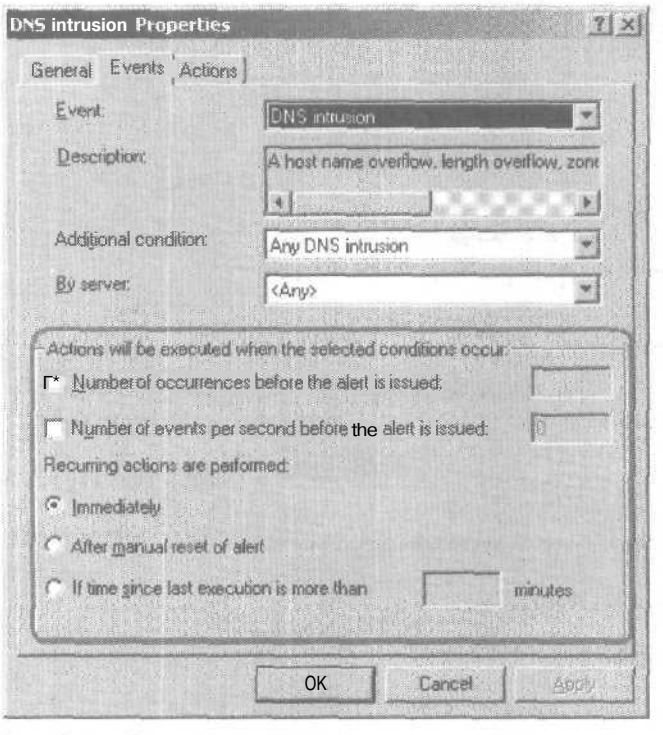


Рис. 9-4. Настройка порогов инициирования оповещений

Действия, выполняемые в ответ на оповещение

Вы вправе определить одно или несколько действий, которые будут выполняться при возникновении оповещения:

- отправка сообщения по электронной почте;
- запуск определенной программы;
- создание записи в журнале событий Windows 2000;
- запуск или останов какой-либо службы ISA-сервера: брандмауэра, Web-прокси или службы загрузки Web-содержимого по расписанию.

Если в ответ на оповещение должна запускаться программа, в некоторых случаях требуется указать учетную запись, под которой она будет работать. Следует предусмотреть наличие у этой учетной записи привилегии Logon As A Batch Job (Вход в качестве пакетного задания). Привилегии пользователей назначаются в окне **Local Security Policy.** Путь, указанный в команде на выполнение программы, должен храниться на всех серверах мас-

сива. При определении пути используйте переменные среды (например *%SystemDrive%*), чтобы задать корректный путь для разных серверов массива.

Действия, выполняемые в ответ на оповещения, определяются при создании нового оповещения или при изменении параметров существующего на вкладке **Actions** диалогового окна **Properties** (рис. 9-5).

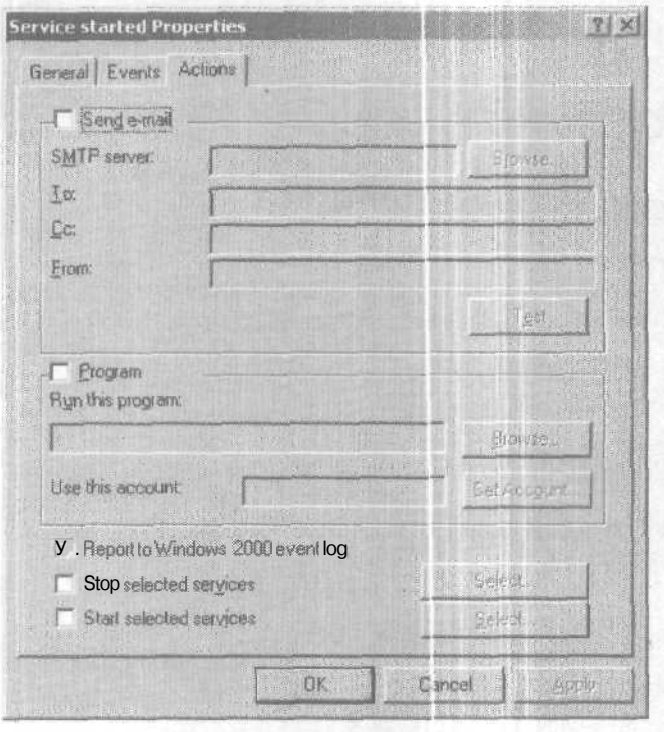


Рис. 9-5. Настройка ответных действий оповещения

▶ Настройка ответных действий оповещения

1. В дереве консоли ISA Management разверните узел **Monitoring Configuration** и щелкните папку **Alerts.**
2. В области сведений щелкните правой кнопкой мыши нужное оповещение и выберите команду **Properties.**
3. На вкладке **Actions** выполните следующие действия:
   - для отправки сообщения по электронной почте установите флажок **Send e-mail** и укажите имя SMTP-сервера, адрес получателя и отправителя;
   - для запуска приложения установите флажок **Program и затем** введите команду для запуска и имя учетной записи, под которой она будет выполняться;
   - для создания записи о событии установите флажок **Report to Windows 2000 event log;**
   - для остановки определенных служб установите флажок **Stop selected services,** затем щелкните кнопку **Select** и укажите службы;
   - для запуска определенных служб установите флажок **Start selected services,** затем щелкните кнопку **Select** и выберите службы.

Примечание При использовании для отсылки сообщений внешнего SMTP-сервера следует создать статический фильтр пакетов, пропускающий трафик протокола SMTP.

События ISA-сервера

В таблице 9-1 перечислены события поддерживаемые ISA-сервером и (где это необходимо) дополнительные параметры. Вновь создаваемым оповещениям сопоставляется одно из перечисленных событий.

Таблица 9-1. События ISA-сервера

Событие	Описание
Alert action failure	Сбой при выполнении действия, выполняемого по данному оповещению
Asymmetric installation	На данном сервере отсутствует компонент, сконфигурированный для всего массива— *<%понятное_пользователю_описание_компонента%>*
Cache container initialization error	Ошибка при инициализации и игнорирование контейнера кэша
Cache container recovery complete	Завершено восстановление контейнера кэша
Cache file resize failure	Сбой при уменьшении размера кэш-файла
Cacheinitializationfailure	Кэширующий Web-прокси отключен из-за глобальною сбоя
Cache recovery completed	Завершено восстановление содержимого кэша
Cache write error	Не удается выполнить запись в кэш
Cached object ignored	При восстановлении кэша обнаружен конфликт содержимого объекта. Объект проигнорирован
Client/servercommunication failure	Сбой связи между клиентом брандмауэра и службой брандмауэра на ISA-сервере
Component load failure	Ошибка при загрузке компонента расширения. *<%имя_модуля%>*
Configuration error	Неверная конфигурация ISA-сервера *<%путь_к_хранилищу%>.*
Dial on demand failure	Не удалось установить подключение вызова по требованию — нет ответа или линия занята
DNS Intrusion	Переполнение буфера имени узлов, превышение длины, максимального номера порта или атака на механизм межзонного переноса
Event logging failure	Сбой при записи события в журнал
Failed to retrieve object	Объект по адресу *<URL>* загрузить не удается - *<описание_ошибки>*
Intra-array credentials	Неверные реквизиты внутренней учетной записи массива
Intrusion detected	Попытка вторжения извне
Invalid dial-on-demand credentials	Неверная учетная запись вызова по требованию
Invalid ODBC log credentials	Указан неверный пароль или имя пользователя при доступе к базе данных по протоколу ODBC
IP packet dropped	Отброшен IP-пакет, не удовлетворяющий требованиям политики безопасности

(см. след. стр.)

Таблица 9-1. *(окончание)*

Событие	Описание
IP Protocol violation	Обнаружен и отброшен пакет с неверными IP-параметрами
IP Spoofing	Недействительный адрес отправителя IP-пакета
Log failure	Не удается внести запись в журнал указанной службы
Network configuration changed	Обнаружено изменение в конфигурации сети, влияющее на работу ISA-сервера
OS component conflict	Конфликт одного из компонентов операционной системы: редактора NAT, службы общего доступа к подключению Интернета (ICS) или службы RRAS
Oversize UDP packet	ISA-сервер отбросил UDP-пакет из-за превышения максимального размера, значение которого определено в реестре
POP Intrusion	ISA-сервер обнаружил переполнение буфера протокола POP
Report Summary Generation	Ошибка при создании сводного отчета Failure на основании файлов журналов
Resource allocation failure	Ошибка распределения системных ресурсов (например нехватка памяти)
RPC filter - server connectivity changed	Изменения в подключении к механизму вызова удаленных процедур (RPC) *<имя_сервера>*
Server Publishing Failure	Не удалось применить правило публикации на сервере
Service Initialization failure	Сбой при инициализации службы
Service not responding	Остановка или неработоспособность службы ISA-сервера
Serviceshutdown	Нормальное завершение работы службы — *<имя_службы>*
Service started	**Успешный запуск службы** *<имя_службы>*
SMTP Filter Event	Произошло событие SMTP-фильтра
SOCKS configuration failure	Порт, указанный в параметрах SOCKS, уже используется другим протоколом
SOCKS request was refused	В запросе SOCKS отказано из-за несоответствия требованиям политики безопасности
The server is out of array 's site	Все серверы массива должны находиться в одном сайте, однако данный сервер расположен в другом сайте
Unregistered event	Произошло неизвестное системе событие. Внутренний идентификатор события %1
Upstream chaining credentials	Неверные реквизиты учетной записи при обращении к вышестоящему серверу цепочки
Web Proxy routing failure	Службе Web-прокси не удалось обработать запрос к вышестоящему прокси-серверу
Web Proxy routing recovery	Маршрутизация службой Web-прокси на вышестоящий прокси-сервер восстановлена
WMT live stream splitting failure	Ошибка разбиения потоков WMT (Windows Media Technology) в фильтре потокового мультимедийного приложения

Практикум. Настройка оповещения для отправки сообщения по электронной почте

Сейчас вы настроите оповещение о попытке вторжения путем отправки администратору соответствующего сообщения по электронной почте. По умолчанию оповещение создает запись в журнале событий Windows 2000. Оповещение следует настроить так, чтобы сообщение получали все администраторы ISA-сервера.

Задание 1. Настройка оповещения по электронной почте о попытке вторжения

В этом упражнении вы настроите оповещение Intrusion Detected, в котором при обнаружении ISA-сервером попытки внешнего вторжения в сеть отправляется сообщение по электронной почте. Основная часть упражнения выполняется на сервере Server1, однако в сети также должен присутствовать сервер Server2 с корректно настроенной службой SMTP.

► **Настройка события Intrusion Detected для отправки сообщения по электронной почте**

1. Войдите в систему сервера Server1 под учетной записью Administrator (Администратор).
2. Откройте оснастку ISA Management и разверните узел **Monitoring Configuration.**
3. Щелкните папку Alerts.
4. В области сведений щелкните правой кнопкой мыши оповещение **Intrusion detected** и в контекстном меню выберите команду **Properties.** Откроется окно свойств оповещения **Intrusion detected.**
5. Перейдите на вкладку **Actions.**
6. Установите флажок **Send e-mail.**
7. В текстовом поле **SMTP server** введите **192.168.0.2.**
8. В текстовом поле To введите **testuser@server2.domain01.local.**
9. В текстовом поле **From** введите **testuser@server2.domain01.local.**
10. Щелкните кнопку Test. Вы увидите сообщение о том, что проверка прошла успешно.
11. Щелкните кнопку **OK.**
12. В диалоговом окне **Properties** щелкните кнопку **OK.**

По прошествии нескольких минут в папке C:\Inetpub\mailroot\Drop на Server2 должно появиться тестовое сообщение, свидетельствующее о нормальной работе оповещения.

Резюме

По умолчанию ISA-сервер содержит 45 оповещений, 39 из которых включены. Каждому оповещению сопоставлено событие и четыре свойства: условия возникновения, местоположение, порог инициирования и ответные действия.

Условия возникновения оповещения определяют обстоятельства, при наступлении которых оно инициируется. Многие предустановленные оповещения, например DNS intrusion, по умолчанию инициируются при возникновении любого из возможных событий, сопоставленных данному оповещению. Однако существует возможность определения более точных условий для оповещения только при возникновении какого-то конкретного события.

Местоположение события — это сервер, на котором оно должно произойти для инициирования оповещения. Все предустановленные оповещения по умолчанию инициируются при возникновении события на любом компьютере из массива ISA-сервера. Тем не менее в качестве местоположения события администратор вправе указать конкретный компьютер.

По умолчанию при возникновении события, сопоставленного включенному оповещению, создается запись в журнале событий Windows 2000. Кроме того, оповещение разрешается настраивать на отсылку сообщения по электронной почте, на запуск программы, запуск или остановку любой из служб ISA-сервера.

Пороги инициирования оповещения определяют, сколько раз должно произойти то или иное событие для инициирования оповещения. Также они определяют период времени, после которого ISA-сервер отправляет повторное оповещение. По умолчанию пороги предусматривают инициирование оповещения после первого события и немедленное выполнение ответных действий.

Все установленные оповещения доступны для просмотра и изменения в папке **Alerts** узла **Monitoring Configuration** в окне консоли ISA Management.

Занятие 2. Ведение журнала работы ISA-сервера

Особенностью работы ISA-сервера является ведение подробных журналов безопасности и доступа, создаваемых в стандартных форматах W3C (World Wide Web Consortium) и ISA. ISA-сервер поддерживает ведение журналов служб брандмауэра, Web-прокси и механизма фильтрации пакетов. Новые журналы можно создавать ежедневно, еженедельно, ежемесячно и ежегодно.

Изучив материал этого занятия, вы сможете:

- ✓ находить и просматривать журналы ISA-сервера для служб брандмауэра, Web-прокси и механизма фильтрации пакетов;
- ✓ изменять такие параметры ведения журналов, как расположение журналов, регистрируемые поля и сжатие файла журнала;
- ✓ настраивать ISA-сервер на использование ODBC-базы данных для хранения журналов.

Продолжительность занятия — около 75 минут.

Управление журналами ISA-сервера

ISA-сервер ведет журналы брандмауэра, Web-прокси и фильтров IP-пакетов. По умолчанию для каждой службы ежедневно создается новый файл журнала. Он размещается в подкаталоге ISALogs, находящемся в установочной папке ISA-сервера. Обычно путь к этому каталогу выглядит так: *%ProgramFiles%*\Microsoft ISA Server\ISALogs\.

Вы вправе изменить порядок ведения этих журналов, например формат записи. По умолчанию запись ведется в формате W3C, но можно использовать формат ISA или вести запись в базу данных формата ODBC. Также разрешается изменять периодичность записи информации в журнал. ISA-сервер настраивается на ежедневное, еженедельное, ежемесячное или ежегодное создание отчетов. Кроме того, вы можете задать перечень полей, регистрируемых в журнале, и путь размещения файлов журналов.

Параметры ведения отдельных журналов настраиваются в папке Logs узла Monitoring Configuration в окне консоли ISA Management (рис. 9-6).

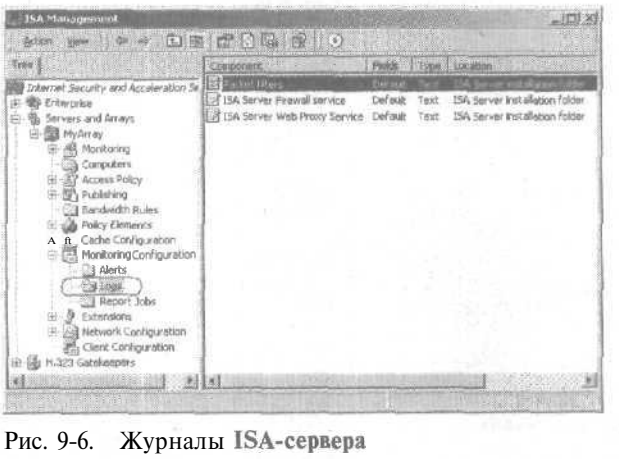


Рис. 9-6. Журналы ISA-сервера

Чтобы открыть окно свойств журнала, достаточно дважды щелкнуть соответствующий значок в области сведений. На рис, 9-7 показана вкладка Log окна свойств журнала, в которой определяется формат записи и местоположение файла журнала.

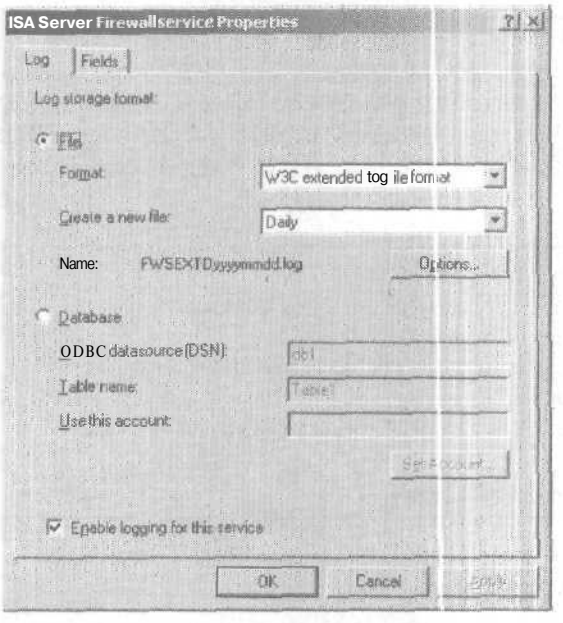


Рис. 9-7. Вкладка Log окна свойств журнала

На рис. 9-8 показана вкладка **Fields.** В ней определяются поля, включаемые в журнал.

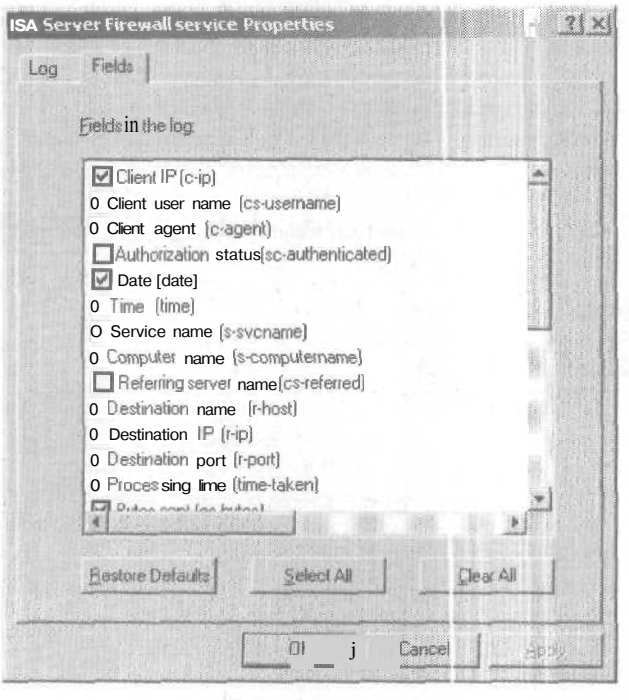


Рис. 9-8. Вкладка Fields окна свойств журнала

Для каждого сервера массива ведется отдельный журнал. Подсистема отчетности ISA-сервера объединяет данные со всех серверов в единый отчет.

Запись в файл

Существуют два типа форматов записи журналов ISA-сервера — W3C и ISA.

Конфигурация журналов определяется на уровне массива, однако для каждого сервера создается отдельный файл журнала. Местоположение файла определяется в диалоговом окне **Options** (рис. 9-9), для открытия которого достаточно щелкнуть кнопку **Options** окна свойств соответствующего журнала.

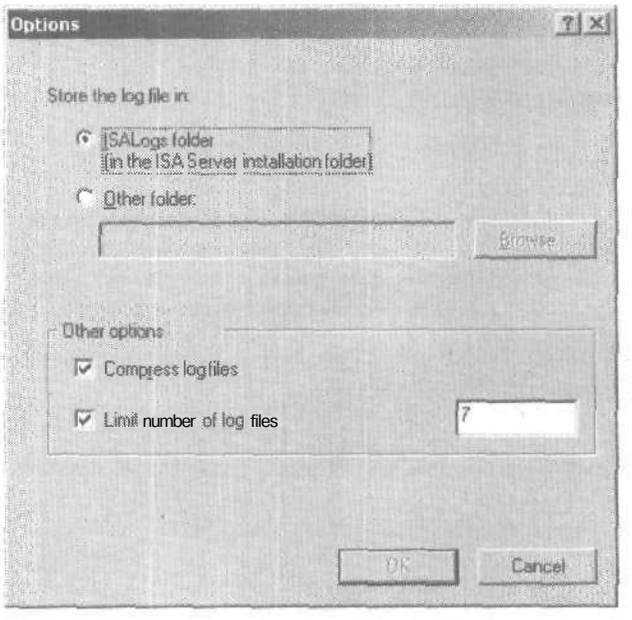


Рис. 9-9. Выбор местоположения файла журнала

По умолчанию файлы журналов размещаются в папках ISALogs на соответствующих серверах массива. Если вы выберете другой путь, следует позаботиться о том, чтобы указанная папка существовала на всех серверах.

Внимание! Файлы журналов рекомендуется размещать на разделах NTFS. Это позволяет воспользоваться такими преимуществами этой файловой системы, как безопасность NTFS и сжатие данных.

Формат W3C

Журналы в формате W3C содержат данные и специальные сведения — номер версии, дату записи и описание полей журнала. Поскольку описание полей журнала содержится в самом файле, невыбранные поля в файле не регистрируются. В качестве разделителя используется символ табуляции. Дата и время указываются по среднему времени по Гринвичу (GMT). На рис. 9-10 показан фрагмент журнала службы Web-прокси в формате W3C.

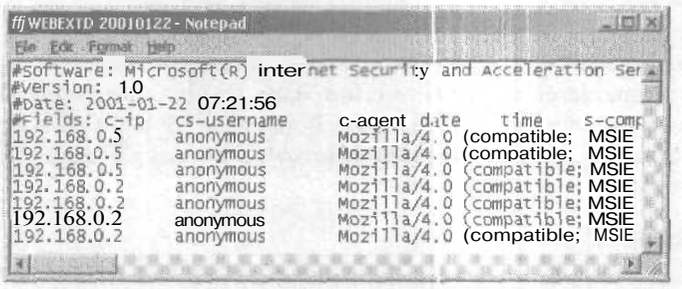


Рис. 9-Ю. Журнал Web-прокси в формате W3C

Формат ISA

В журнале формата ISA содержатся лишь данные — дополнительных сведений в нем нет. В файле регистрируются все существующие поля, невыбранные поля заполняются дефисом (-). В качестве разделителя используется запятая. Дата и время указываются в местном времени. На рис. 9-11 показан фрагмент журнала службы брандмауэра в формате ISA.

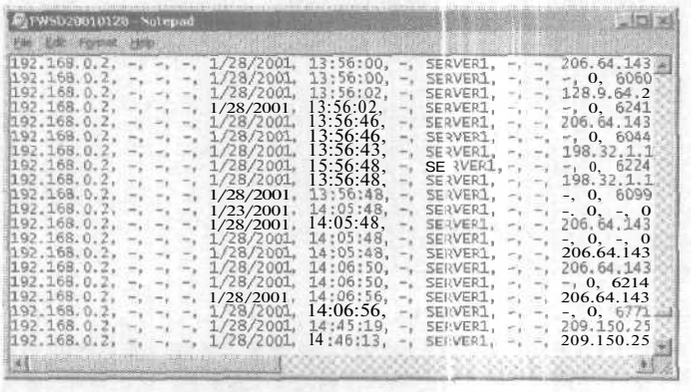


Рис. 9-11. Журнал брандмауэра в формате ISA

Имена файлов журналов

Имя файла журнала формируется из названия службы, формата и даты создания.

Первые три буквы имени файла обозначают службу, для которой ведется журнал. Журналы службы брандмауэра обозначаются сокращением FWS, служба Web-прокси — WEB, а фильтры IP-пакетов — IPP. В имени файла в формате W3C за первыми тремя буквами следует EXT; отличительной особенностью журналов в формате ISA является отсутствие этих букв. Далее следует буква, обозначающая периодичность внесения записей в журнал: D — ежедневно, W — еженедельно, M — ежемесячно и Y — ежегодно. В конце имени указывается дата создания журнала в формате ГГГГММДД. Таким образом, дата 21 мая 2002 года будет представлена как 20020521, а созданный в этот день журнал ежедневной регистрации работы службы Web-прокси в формате W3C получит имя WEBEXTD20020521.log. Файлу с ежемесячным журналом службы брандмауэра, созданному в тот же день в формате ISA, присваивается имя FWSM20020521.log.

Параметры ведения файлов журнала

Для экономии дискового пространства ISA-сервер предоставляет следующие возможности:

- сжатие файлов для уменьшения занимаемого ими места. Сжатие поддерживается лишь для файлов на разделах NTFS;
- ограничение общего числа файлов журнала в массиве;
- ограничение перечня полей, записываемых в файлы.

▶ **Настройка порядка ведения журналов**

1. В дереве консоли ISA Management разверните узел **Monitoring Configuration** и щелкните папку **Logs.**
2. В области сведений щелкните правой кнопкой мыши значок журнала нужной службы и в контекстном меню выберите команду **Properties.**
3. На вкладке **Log** установите переключатель **File.**
4. В поле со списком **Format** выберите формат записи файла.
5. В поле со списком **Create a new file** выберите период создания файла журнала — Daily (ежедневно), Weekly (еженедельно), Monthly (ежемесячно) или Yearly (ежегодно).
6. Для изменения местоположения файла щелкните кнопку **Options**, затем:
   - для размещения файла в папке назначенной по умолчанию установите переключатель в положение **ISALogs folder (in the ISA Server installation folder);**
   - для размещения в другой папке установите переключатель **Other folder** и введите имя папки или щелкните кнопку **Browse** и укажите требуемую папку.
7. Для определения максимально допустимого количества файлов журнала установите флажок **Limit number of log files** и в соответствующем текстовом поле укажите разрешенное число файлов.
8. Для сжатия файлов установите флажок **Compress log files.**

Запись журналов в базу данных

Существует возможность хранения журналов ISA-сервера в базе данных, поддерживающей протокол ODBC. Для выбора этого варианта хранения журналов следует установить переключатель **Database** на вкладке Log окна свойств для соответствующего журнала.

Перед настройкой ISA-сервера на запись журналов в базу данных следует предусмотреть наличие самой базы и создать в ней соответствующие таблицы. В папке **isa** дистрибутивного компакт-диска ISA-сервера расположены типовые сценарии для создания таблицы индексов в базе данных. Вот их список:

- Pf.sql создает таблицу с именем PacketFilterLog для записи журналов фильтров пакетов и индексы для поддержки запросов;
- W3PROXY.sql создает таблицу с именем WebProxyLog для записи журналов службы Web-прокси и индексы для поддержки запросов;
- FWSRV.sql создает таблицу с именем FirewallLog для записи журналов службы брандмауэра и индексы для поддержки запросов.

Например, для создания в базе данных SQL Server 2000 журнала с именем ISALogs, максимальный размер которого не превышает 100 Мбайт, и файла записи транзакций с размером не более 50 Мбайт следует выполнить операции, описанные далее.

1. Откройте SQL Query Analyzer и подключитесь к SQL-серверу, на котором предполагается хранить базу данных.
2. В области **Editor** окна **Query** введите следующий текст на Transact-SQL:

```
USE master
GO
CREATE DATABASE ISALogs
```

Этот фрагмент кода нужен для создания базы данных с именем ISALogs.

3. Сразу под этим текстом введите следующее:

```
ON PRIMARY
(
   NAME = ISALog_dat,
   FILENAME = 'C:\Program Files\Microsoft SQL Server\MSSQL\Data\ISALog.mdf',
   SIZE = 50,
   MAXSIZE = 100,
   FILEGROWTH = 1
)
```

Этот код необходим для определения основного файла с логическим именем ISALog_dat. Путь и имя файла, используемого операционной системой, — C:\Program Files\Microsoft SQL Server\MSSQL\Data\ISALog.mdf. Начальный размер файла составляет 50 Мбайт и может увеличиваться до 100 Мбайт порциями по 1 Мбайту.

Примечание Если на компьютере отсутствует путь, указанный в примере, то до выполнения пункта 5 следует создать такой путь или скорректировать текст примера.

4. Далее введите следующий текст;

```
LOG ON
(
   NAME = ISALog_log,
   FILENAME - 'C:\Program Files\Microsoft SQL Server\MSSQL\Data\ISALog.ldf',
   SIZE = 25,
   MAXSIZE = 50,
   FILEGROWTH = 1
)
GO
```

Этот фрагмент создает файл журнала с логическим именем ISALog_log. Путь и имя файла, используемого операционной системой, — C:\Program Files\Microsoft SQL Server\MSSQL\Data\ISALog.ldf. Начальный размер файла составляет 25 Мбайт и может увеличиваться до 50 Мбайт порциями по I Мбайту.

Примечание Если на компьютере отсутствует путь указанный в примере, то до выполнения пункта 5 следует создать такой путь или скорректировать текст примера.

5. Запустите полученный командный файл.

   На вкладке **Messages в** панели **Results** выводятся два сообщения. Первое информирует о выделении для основного файла 100 Мбайт дискового пространства, а второе — о выделении для файла транзакций 50 Мбайт.

6. Убедитесь, что в качестве текущей установлена база данных ISALogs, затем откройте и выполните все сценарии из папки isa дистрибутивного компакт-диска ISA-сервера (сценарии хранятся в файлах с расширением .sql).

7. Для каждой службы создаются таблицы журналов и индексы для поддержки запросов.

После создания базы данных, таблиц и индексов следует настроить ISA-сервер на использование имени источника данных. Выполните операции, описанные далее.

1. На компьютере с ISA-сервером щелкните кнопку **Start** (Пуск), последовательно откройте папки **Programs** (Программы) и **Administrative Tools** (Администрирование). Щелкните значок **Data Sources (ODBC)** [Источники данных (ODBC)].
2. На вкладке **System DSN** (Системный DSN) шелкните кнопку Add (Добавить).
3. В окне **Create New Data Source** (Создание нового источника данных) выберите нужный драйвер базы данных.

   Если вы используете SQL Server 2000, то в качестве драйвера выберите **SQL Server.**
4. Последовательно выполните инструкции мастера. Имя источника данных указывается в текстовом поле **ODBC data source (DSN)** при настройке записи журналов в базу данных (об этом чуть позже).

Внимание! В имени источника данных нельзя использовать пробелы, в противном случае службы ISA-сервера остановятся.

▶ **Настройка записи журналов в базу данных**

1. В дереве консоли ISA Management разверните узел **Monitoring Configuration** и шелкните папку **Logs.**
2. В области сведений щелкните правой кнопкой мыши значок журнала нужной службы и выберите команду **Properties.**
3. На вкладке **Log** установите переключатель в положение **Database.**
4. При необходимости измените значение следующих параметров:
   - **ODBC data source (DSN);**
   - **Table name** — здесь используются имена таблиц, заданные в файлах сценариев (.sql) из корневой папки дистрибутивного компакт-диска ISA-сервера. Например, таблица для журнала службы фильтров пакетов называется PacketFilterLog;
   - **User account.**
5. Щелкните кнопку **Set Account,** в текстовом поле **User** введите имя пользователя и в текстовых полях **Password и Confirm Password** введите пароль. В зависимости от конфигурации аутентификации SQL Server используется идентификатор SQL Server или учетная запись Windows.

Запись в журнал информации о пакетах

ISA-сервер поддерживает регистрацию в журнале службы фильтров пакетов информацию о любых пакетах, проходящих через ISA-сервер. Для точного определения типов пакетов, информация о которых записывается в журнал, необходимо знать особенности ISA-сервера:

- По умолчанию после установки ISA-сервера в журнал записывается информация обо всех проигнорированных (не пропущенных) пакетах. Вместе с отключением фильтрации пакетов отключается и запись в журнал.
- Разрешается не регистрировать в журнале пакеты, отброшенные конкретными фильтрами.
- ISA-сервер можно настроить и на запись в журнал сведений обо всех пакетах — и проигнорированных, и пропущенных. Если включить запись информации о пропущенных пакетах, в журнале службы фильтров пакетов регистрируются сведения обо всех пакетах, проходяших через ISA-сервер.

  Запись информации об отброшенных и принятых пакетах существенно нагружает сервер.

▶ **Запись в журнал информации о пропущенных сервером пакетах**

1. В дереве консоли ISA Management разверните узел **Access Policy,** щелкните правой кнопкой мыши папку **IP Packet Filters и** в контекстном меню выберите команду **Properties.**
2. На вкладке **Packet Filters** установите флажок **Log packets from 'Allow' filters.**

Примечание Запись в журнал информации о принятых пакетах выполняется только при включенном режиме фильтрации пакетов.

▶ **Запись в журнал информации об отброшенных пакетах**

1. В дереве консоли ISA Management разверните узел Access **Policy** и щелкните папку **IP Packet Filters.**
2. В меню View отметьте команду **Advanced.**
3. В области сведений щелкните правой кнопкой мыши блокирующий фильтр, для которого следует записывать информацию об отброшенных пакетах, и в контекстном меню выберите команду **Properties.**
4. На вкладке **General** установите флажок **Log any packets matching this filter.**

Поля записей в журналах брандмауэра и Web-прокси

На вкладке **Fields** окна свойств журнала можно выбрать поля для записи в журнал. По умолчанию в журнале фильтров пакетов регистрируется 9 полей из 12 существующих. В журналах брандмауэра и Web-прокси по умолчанию регистрируется 18 полей из 27 возможных. Вы вправе в любое время изменить их перечень или восстановить список по умолчанию, щелкнув кнопку **Restore Defaults.**

▶ **Выбор полей для записи в журнал**

1. В дереве консоли ISA Management разверните узел **Monitoring Configuration и** щелкните папку **Logs.**
2. В области сведений щелкните правой кнопкой мыши значок журнала нужной службы и в контекстном меню выберите команду **Properties.**
3. Перейдите на вкладку **Fields.** Здесь вы можете:
   - выбрать поля, записываемые в журнал, установив соответствующие флажки;
   - сбросить все флажки в списке полей, щелкнув кнопку **Clear All;**
   - установить все флажки в списке полей, щелкнув кнопку **Select All;**
   - восстановить набор полей по умолчанию, щелкнув кнопку **Restore Defaults.**

В таблице 9-2 перечислены поля, доступные для регистрации в журналах служб брандмауэра и Web-прокси. Поля, указанные в скобках, регистрируются при использовании расширенного формата журнала 3С. Обратите внимание, что в именах W3C операции клиента обозначаются префиксом «c», а операции сервера — префиксом «s». Префикс «cs» обозначает операции «клиент — сервер», а «sc» — «сервер — клиент». Префикс «r» обозначает удаленные операции.

Некоторые поля относятся только к службе брандмауэра или только к Web-прокси. Такие случаи в таблице оговорены особо. Обратите внимание, что в журналах формата ISA-сервера нерегистрируемые поля заполняются дефисами (-). В журнале формата W3C такие поля никак не отображаются.

В таблицах 9-2 — 9-6 приводятся возможные значения некоторых полей. Полный их перечень вы найдете в узле **Monitoring Configuration** оснастки ISA Management. Для этого выделите папку Logs и дважды щелкните значок соответствующего файла журнала — **ISA Server Firewall Service** (журнал брандмауэра) или **ISA Server Web Proxy** Service (журнал Web-

прокси). Чтобы просмотреть список полей, доступных для записи в журнал, перейдите на вкладку **Fields**.

Таблица 9-2. Поля журналов служб брандмауэра и Web-прокси

Номер поля	Имя поля	Описание
1	Client IP (c-ip)	IP-адрес клиента, от которого поступил запрос
2	Client user name (cs-username)	Учетная запись пользователя, от которого поступил запрос. Если механизм управления доступом не применяется, ISA-сервер использует имя *anonymous*
3	Client agent (c-agent)	Тип клиентского приложения, переданный клиентом в заголовке протокола HTTP. Если ISA-сервер работает в режиме активного кэширования, в данное поле заносится значение *ISA Server*. В службе брандмауэра в этом поле указывается информация об операционной системе клиента. Возможные значения перечислены в таблице 9-3
4	Authorization status (sc-authenticated)	Информирует о том, прошел ли клиент аутентификацию на ISA-сервере. Возможные значения — Кили *N*
5	Date (date)	Дата события
6	Time (time)	Время события (в формате W3C указывается среднее время по Гринвичу)
7	Service name (s-svcname)	Имя службы. Для исходящих Web-запросов к службе Web-прокси в этом поле указывается значение *w3proxy*. Записи службы брандмауэра отмечаются значением *fwsrv*, а входящие Web-запросы к службе Web-прокси — значением *w3reverseproxy*
8	Computer name (s-computername)	Имя компьютера в Windows 2000, на котором работает ISA-сервер
9	Referring server name (cs-referred)	В иерархиях ISA-серверов в этом поле указывается имя направившего запрос подчиненного сервера
10	Destination name (r-host)	Доменное имя удаленного компьютера, обслуживающего данное подключение. Дефис в этом поле в журнале службы Web-прокси, как правило, означает, что объект извлечен из кэша сервера Web-прокси, а не с запрашиваемого компьютера
11	Destination IP (r-ip)	IP-адрес удаленного компьютера. Дефис - в данном поле в записи службы Web-прокси обычно означает, что объект получен из кэша сервера Web-прокси, а не с сервера. Исключение — обратное кэширование. В этом случае указывается IP-адрес, по которому возвращен кэшируемый объект
12	Destination port (r-port)	Номер зарезервированного порта удаленного компьютера. Используется клиентским приложением, инициирующим запрос

(см. след. стр.)

Таблица 9-2. (*продолжение*)

Номер поля	Имя поля	Описание
13	Processing time (time-taken)	Общее время (в миллисекундах), затраченное ISA-сервером на обработку данного подключения. Указывает время, прошедшее с момента поступления первого запроса до возвращения результатов клиенту и окончания сеанса связи. Для запросов, выполняемых через службу Web-прокси, указывается время, затраченное на полную обработку запроса и возврат клиенту объекта из кэша
14	Bytes sent (cs-bytes)	Количество байт, переправленных внутренним клиентом внешнему серверу в течение данного подключения. Дефис, ноль или отрицательное значение указывают на то. что удаленный компьютер не предоставил запрошенную информацию или удаленному компьютеру не отправлено ни байта
15	Bytes received (sc-bytes)	Количество байт, отправленных внешним компьютером и полученных клиентом в течение данного подключения. Дефис, ноль или отрицательное значение указывают на то, что удаленный компьютер не предоставил запрошенную информацию или от внешнего компьютера не получено ни байта
16	Protocol name (cs-protocol)	Прикладной протокол, использовавшийся при подключении. Обычно принимает значения HTTP, FTP или HTTPS. В журнале службы брандмауэра также указывается номер порта
17	Transport (cs-transport)	Транспортный протокол, использовавшийся в подключении. Обычно принимает значения TCP или UDP
18	Operation (s-operation)	Вид выполненной операции. Для службы Web-прокси обычно принимает значения GET, PUT, POST и HEAD. Для службы брандмауэра - CONNECT, BIND, SEND, RECEIVE, GHBN (GetHostByName) и GHBA (GetHostByAddress)
19	Object name (cs-uri)	Это поле есть только в журнале службы Web-прокси и содержит URL-адрес объекта
20	Object MIME (cs-mime-type)	Присутствует только в журналах службы Web-прокси и содержит MIME-тип объекта. Поле заполняется дефисом, если тип MIME не задан или не поддерживается удаленным компьютером. Дефис проставляется и в том случае, когда поле не используется
21	Object source (s-object-source)	Присутствует только в журналах службы Web-прокси. Содержит источник текущего объекта. Возможные значения этого поля перечислены в таблице 9-4

Таблица 9-2. (*окончание*)

Номер поля	Имя поля	Описание
22	Result code (sc-status)	Возможные значения: * меньше 100 — код ошибки Windows (Win32); * значения в диапазоне 100–1000 — код состояния **HTTP;** * значения в диапазоне 10000–11004 — код ошибки Winsock. Возможные значения этого поля перечислены в таблице 9-5
23	Cache info (s-cache-info)	Это поле есть только в журналах службы Web-прокси. В нем указывается причина, по которой объект был или не был помещен в кэш. Возможные значения этого поля перечислены в таблице 9-6
24	Rule #1 (rule#1)	В этом поле записывается первое правило, согласно которому разрешена или запрещена пересылка запроса. Поле заполняется следующим образом. Если пересылка исходящего запроса разрешена (или запрещена), то в поле заносится соответствующее правило протокола, разрешившее (запретившее) пересылку запроса. Если пересылка исходящего запроса запрещена правилом узлов и содержимого, то в это поле заносится правило протокола, разрешившее пересылку запроса. Если пересылка входящего запроса запрещена, в поле заносится правило Web-публикации или правило публикации серверов, запретившее пересылку запроса. Если нет правила, разрешающего пересылку входящего или исходящего запроса, запрос блокируется и поле не заполняется
25	Rule #2 (rule#2)	В этом поле указывается второе правило, согласно которому разрешена или запрещена пересылка запроса. Для переадресованных (заблокированных) исходящих запросов в это поле заносится правило узлов и содержимого, разрешившее пересылку (выполнившее блокировку) запроса. Если правила разрешающего данный входящий или исходящий запрос не существует, он блокируется и поле остается пустым
26	Session ID (sessionid)	Это поле имеется только в журнале службы брандмауэра и информирует о подключениях сеанса. На клиентах брандмауэра каждый процесс, подключаемый через брандмауэр, инициирует отдельный сеанс, Для клиентов SecureNAT открывается один сеанс для всех подключений с одного IP-адреса
27	Connection ID (connectionid)	Это поле присутствует только в журнале службы брандмауэра и содержит записи, относящиеся к одному сокету. Для внешнего TCP-подключения обычно создается две записи на каждое подключение: при создании и при разрыве подключения. В протоколе UDP на каждый удаленный адрес приходится две записи. Этого поля нет в журнале Web-прокси

В таблице 9-3 перечислены возможные значения поля Client agent (c-agent) в журналах брандмауэра. Когда в журнале регистрируются все доступные поля, одно из значений, приведенных в этой таблице, заносится на третью позицию в журнале. Оно указывает на операционную систему клиента.

Таблица 9-3. Значения поля Client agent (c-agent)

Значение	Операционная система клиента
0:3.95	Windows 95 (16-разрядная)
2:4.10	Windows 98 (32-разрядная)
2:4.0	Windows 95 (32-разрядная)
3:4.0	Windows NT 4.0
3:5.0	Windows 2000

В таблице 9-4 перечислены возможные значения поля Object source (s-object-source) в журналах службы Web-прокси. Когда в журнале регистрируются все доступные поля, одно из значений, приведенных в этой таблице, проставляется в журнале на двадцать первой позиции. Оно сообщает, откуда получен объект.

Таблица 9-4. Значения поля Object source (s-object-source)

Значения поля	Описание
О	Информация об источнике объекта отсутствует
Cache	Объект получен из кэша
Inet	Объект получен из Интернета, а его копия размещена в кэше
Member	Объект получен от другого сервера массива
NotModified	Источником объекта является кэш. Направив запрос If-Modified-Since, клиент получил сообщение, что запрашиваемый объект не изменялся
NVCache	Объект получен из кэша, а сравнить его с оригиналом не удается
Upstream	Объект получен из кэша вышестоящего прокси
Vcache	Объект получен из кэша, так как сравнение с оригиналом показало, что объект не изменялся
VFInet	Объект получен из Интернета, так как сравнение объекта находящегося в кэше с оригиналом показало, что объект был изменен

В таблице 9-5 приведены некоторые возможные значения поля Result code (cs-status), регистрируемые в журналах брандмауэра и Web-прокси.

Часто в этом поле регистрируется код ошибки Windows (для значений, меньших 100), код состояния HTTP (для значений из диапазона 100–1000) или код ошибки Winsock (для значений из диапазона 10000–11004). Как правило, каждое подключение регистрируется в журнале дважды: при его создании и при разрыве. Значение этого поля в первой записи равно 0 (успешное создание подключения) или 13301 (отказ в соединении), в этом случае в других полях обычно указывается нулевое число байт. Значение поля во второй записи равно 20000 (нормальное завершение соединения) или 20001 (неожиданный разрыв связи), кроме этого указывается соответствующее количество байт.

Подробнее о кодах ошибок — на Web-узле Microsoft Developers Network (*http://msdn.microsoft.com)* или Microsoft Technet (*http://www.microsoft.com/technet*).

Таблица 9-5. Некоторые значения поля Result code (cs-status)

Значение	Описание
0	Успешное подключение
200	Успешное подключение (OK)
201	Подключение создано
202	Подключение принято
204	Отсутствие информационного наполнения
301	Запрашиваемое информационное наполнение перемещено
302	Запрашиваемое информационное наполнение временно перемещено
304	Запрашиваемое информационное наполнение не изменилось
400	Неверный запрос
401	Недостаточно прав для доступа
403	Доступ запрещен
404	Объект не найден
500	Внутренняя ошибка сервера
501	Не реализовано
502	Неверный шлюз
503	Служба недоступна
10054	Соединение сброшено удаленным узлом
10060	Тайм-аут подключения
10061	Отказ удаленного узла в подключении
10065	Узел недоступен
11001.	Узел не найден
13301	Подключение запрещено (из-за ограничений, налагаемых правилами фильтрации или протоколов)
20000	Нормальное завершение соединения
20001	Неожиданный обрыв связи

В таблице 9-6 приведены возможные значения поля Cache info (s-cache-info) в журналах Web-прокси. Это значение отражает причину, по которой объект помещен (или не помещен) в кэш.

Таблица 9-6. Значения поля Cache info (s-cache-info)

Значение	Описание
0x00000001	Для обслуживания запроса не использовать данные из кэша
0x00000002	Запрос содержит заголовок IF-MODIFIED-SINCE
0x00000004	Запрос содержит заголовок CACHE-CONTROL:NO-CACHE или PRAGMA:NO-CACHE
0x00000008	Запрос содержит заголовок AUTHORIZATION

(см. след. стр.)

Таблица 9-6. *(окончание)*

Значение	Описание
0x00000010	Запрос содержит заголовок VIA
0x00000020	**Запрос содержит заголовок** IF-MATCH
0x00000040	**Запрос содержит заголовок RANGE**
0x00000080	Запрос **содержит заголовок** CACHE-CONTROL:NO-STORE
0x00000100	Запрос содержит один из следующих заголовков: CACHE-CONTROL:MAX-AGE, CACHE-CONTROL:MAX-STALE или CACHE-CONTROL:MIN-FRESH
0x00000200	Не удалось **обновить кэш**
0x00000400	В заголовке IF-MODIFIED-SINCE указано более позднее время, чем время LASTMODIFIED объекта в кэше
0x00000800	**Запрос содержит заголовок** CACHE-CONTROL:ONLY-IF-CACHED
0x00001000	Запрос **содержит заголовок IF-NONE-MATCH**
0x00002000	**Запрос содержит заголовок** IF-UNMODIFIED-SINCE
0x00004000	Запрос содержит заголовок IF-RANGE
0x00008000	Запрос содержит более одного заголовка VARY
0x00010000	Ответ содержит **заголовок** CACHE-CONTROL:PUBLIC
0x00020000	Ответ содержит заголовок CACHE-CONTROL:PRIVATE
0x00040000	**Ответ** содержит **заголовок** CACHE-CONTROL:NO-CACHE **или** PRAGMA-NO-CACHE
0x00080000	Ответ содержит заголовок CACHE-CONTROL:NO-STORE
0x00100000	Ответ содержит заголовок CACHE-CONTROL:MUST-RE-VALIDATE или CACHE-CONTROL:PROXY- REVALIDATE.
0x00200000	Ответ содержит заголовок CACHE-CONTROL:MAX-AGE или S-MAXAGE
0x00400000	**Ответ** содержит **заголовок VARY**
0x00800000	Ответ содержит заголовок LAST-MODIFIED
0x01000000	**Ответ содержит** заголовок **EXPIRES**
0x02000000	Ответ содержит заголовок SET-COOKIE
0x04000000	Ответ содержит заголовок WWW-AUTHENTICATE
0x08000000	Ответ содержит заголовок VIA
0x10000000	**Ответ** содержит **заголовок AGE**
0x20000000	**Ответ содержит заголовок TRANSFER-ENCODING**
0x40000000	Ответ не следует размещать в кэше

Поля записей в журналах фильтров пакетов

Журнал ISA-сервера часто используется для наблюдения и анализа состояния фильтров пакетов. В таблице 9-7 перечислены поля, доступные для регистрации в журналах фильтров пакетов. Перечень этих полей вы найдете в узле **Monitoring Configuration** оснастки ISA Management. Для этого выделите папку **Logs,** дважды щелкните журнал **Packet filters** и перейдите на вкладку **Fields.**

Таблица 9-7. Поля журнала фильтров пакетов

Номер поля	Имя поля	Описание
1	Date (date)	Дата получения пакета
2	Time (time)	Время получения пакета
3	Source IP (source-ip)	IP-адрес (удаленного) компьютера, отправившего пакет
4	Destination IP (destination-ip)	IP-адрес (локального) компьютера, получившего пакет. Обычно это компьютер, на котором установлен ISA-сервер
5	Protocol (protocol)	Используемый в подключении транспортный протокол, например TCP, UDP или ICMP
6	Source port (or protocol type, if ICMP)(param#1)	При использовании протоколов TCP и UDP в данном поле указывается удаленный порт, через который осуществлялось подключение, а при использовании протокола ICMP — тип протокола
7	Destination port (or protocol code, if ICMP)(param#2)	При использовании протоколов TCP и UDP здесь указывается локальный порт, через который осуществлялось подключение, а при использовании протокола ICMP — код, использовавшийся при создании подключения
8	TCP flags (tcp-flags)	В этом поле регистрируется значение флага TCP в IP-заголовке пакета данных. Возможные значения: FIN, SYN, RST, PSH, ACK или URG
9	Rule (filter-rule)	Информирует, принят пакет (1) или отброшен (0). По умолчанию в журнале регистрируются только отброшенные пакеты
to	Interface IP address (interface)	Интерфейс, использовавшийся для принятия пакета, Обычно указывается только один интерфейс
!!	Header (ip-header)	IP-заголовок пакета (в шестнадцатеричном формате), инициировавшего оповещение
12	Payload (payload)	Область данных, следующая за IP-заголовком. Записывается в шестнадцатеричном формате

Практикум. Изучение журналов Web-прокси

Вы изучите образец журнала службы Web-прокси и ответите на вопросы. Обратите внимание, что заголовки колонок немного смещены по отношению к самим значениям. Файл журнала оставлен в виде, в каком его создал ISA-сервер. При просмотре журнала в Notepad (Блокнот) следует отключить перенос по словам (Word Wrap).

Задание 1. Анализ журнала Web-прокси

Для выполнения этого упражнения откройте журнал службы Web-прокси с именем WEBEXTD20010129.log. Он расположен в папке \Exercises\Chapter9\ прилагаемом к книге на компакт-диске и записан в формате W3C. Ответьте на вопросы упражнения, используя таблицы и материалы этой главы. В ответах следует указывать точные значения полей.

1. Какой из двух трафиков данных — от клиента к серверу или от сервера к клиенту — в первом подключении, зарегистрированном в журнале в 02:31:35, больше? Совет: по таблице 9-2 определите имена полей, в которых регистрируется информация о количестве отправленных (Bytes Sent) и принятых (Bytes Received) байт, и сравните эти значения в первой записи журнала.

2. Откуда возвращены данные в ответ на запрос — из Интернета или из кэша? Совет: по таблице 9-2 определите имя поля, в котором указывается источник получения объекта (Object Source). Затем сравните значение соответствующего поля журнала со значениями, приведенными в таблице 9-4.

3. Когда (в какое время) удаленный узел сбросил подключение? Совет: по таблице 9-5 определите код результата, соответствующего этому событию. Затем найдите в журнале запись с таким кодом и посмотрите время события.

4. Найден ли запрошенный в 02:31:45 объект в кэше? Был ли он изменен? Из какого источника в конечном счете объект возвращен клиенту? Совет: найдите в журнале запись о событии произошедшем в указанное время. По таблице 9-2 определите имя поля, в котором регистрируется код результата. Затем сравните значение соответствующего поля журнала со значениями, приведенными в таблице 9-5.

5. Какая операция выполнена в 04:55:14? Удалось ли обратиться к адресату? Совет: найдите в журнале запись о событии, произошедшем в указанное время. По таблице 9-2 определите имя поля, в котором содержится информация о выполненной операции, и найдите соответствующее поле в данной записи. Затем определите результат операции, используя значения из таблицы 9-5.

Резюме

ISA-сервер ведет журналы для служб брандмауэра, для Web-прокси и для фильтров IP-пакетов. По умолчанию для каждой службы ежедневно создается новый файл журнала. Он размещается в подкаталоге ISALogs. расположенном в установочной папке ISA-сервера. Параметры журналов настраиваются в папке Logs узла Monitoring Configuration оснастки (SA Management.

Существует два формата журналов ISA-сервера в виде текстовых файлов — W3C и ISA. Кроме того, можно сохранять журналы ISA-сервера в базе данных, поддерживающей протокол ODBC. Для экономии дискового пространства ISA-сервер позволяет сжимать файлы журналов и ограничивать общее число журналов в массиве.

Администратор ISA-сервера вправе выбирать поля, регистрируемые в журналах. Подробнее о перечне полей, доступных для регистрации в журналах конкретных служб, и об их возможных значениях — в справочной системе ISA-сервера.

Занятие 3. Создание отчетов ISA-сервера

ISA-сервер автоматически создает графические отчеты на основании информации в журналах. Поддерживается различная периодичность генерации отчетов: однократно, ежедневно, ежемесячно или в указанный день недели.

Изучив материал этого занятия, вы сможете:

- ✓ настроить ISA-сервер на создание отчетов по заданному расписанию;
- ✓ просматривать отчеты ISA-сервера и анализировать характер использования Интернета.

Продолжительность занятия - около 45 минут.

Конфигурирование отчетов

Механизм создания отчетов ISA-сервера позволяет создавать отчеты о характере использования Интернета клиентами и компьютерами. Отчеты создаются на основании предварительно сконфигурированных заданий в узле **Monitoring Configuration** дерева консоли ISA Management (рис. 9-12). Задания предусматривают создание одного или нескольких отчетов в соответствии с определенным расписанием, кроме того, можно генерировать итоговые цифры на основании данных журналов за заданный период времени.

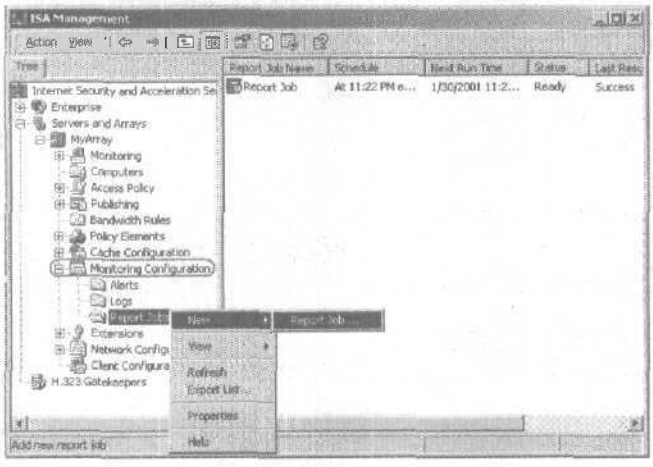


Рис. 9-12. Создание нового задания по созданию отчетов

Просмотр отчетов

Каждое задание создает набор из пяти отчетов, которые размещаются в отдельные папки узла **Monitoring** дерева консоли ISA Management (рис. 9-13). В папке **Summary** хранится сводный отчет, в папке **Web Usage** — отчет об использовании Web, в папке **Application Usage** — отчет об использовании клиентских приложений. Папка **Traffic & Utilization** содержит отчет об используемых приложениях и протоколах, а папка **Security** — отчеты об атаках на сеть. Отчет отображается в виде Web-страницы и содержит несколько вложенных отчетов.

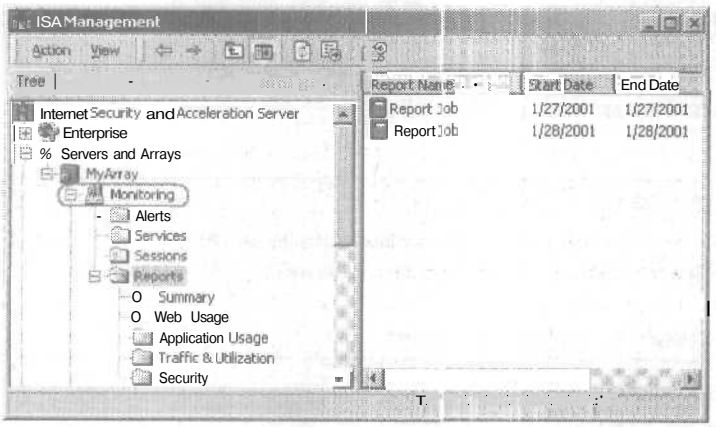


Рис. 9-13. Папки с отчетами в узле Monitoring

Сводные отчеты

Сводные отчеты — это набор отчетов об использовании сети различными приложениями. Они особенно полезны для администраторов сетей и сотрудников, отвечающих за планирование и управление использованием Интернета.

Сводные отчеты объединяют данные из журналов брандмауэра и Web-прокси. Пример сводного отчета показан на рис. 9-14.

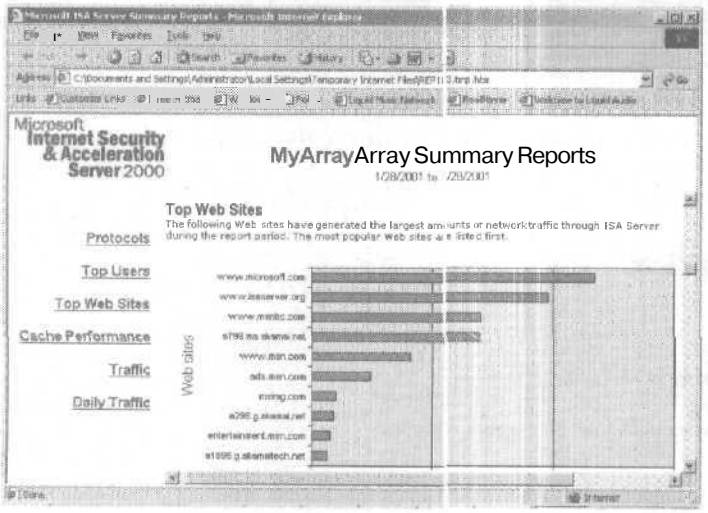


Рис. 9-14. Сводный отчет

Отчеты об использовании Web

Отчеты об использовании Web (Web Usage) содержат набор отчетов о наиболее активных пользователях Web, наиболее популярных ответах и применяемых браузерах. Эти отчеты особенно полезны для администраторов сетей и сотрудников, отвечающих за планирование и управление использованием Интернет, так как содержат информацию о работе с Web внутри компании.

Отчеты об использовании Web создаются на основе информации из журналов службы Web-прокси.

Отчеты об использовании клиентских приложений

Отчеты о применении клиентских приложений (Application Usage) содержат информацию об используемых внутри компании интернет-приложениях. Они содержат сведения о входящем и исходящем трафике, наиболее активных пользователях, клиентских приложениях и адресатах. Эти отчеты помогают выявлять перегруженность сети, поэтому они полезны администраторам сетей, управляющим работой с Интернетом.

Отчеты об использовании приложений создаются на основе информации журналов службы брандмауэра.

Отчеты о трафике и использовании Интернета

Отчеты о трафике и использовании Интернета (Traffic & Utilization) содержат информацию о работе с Интернетом различных приложений и протоколов, показывают общий объем трафика, его направление и пиковое число одновременных подключений. Кроме того, эти отчеты содержат информацию о частоте попаданий кэша, возникших ошибках и других статистических показателях. Эти отчеты помогают следить за пропускной способностью сети.

Отчеты о трафике создаются на основании данных журналов брандмауэра и Web-прокси.

Отчеты об атаках на сеть

Отчеты об атаках на сеть (Security) позволяют опознавать активные или прошедшие атаки и нарушения системы безопасности сети.

Отчеты об атаках на сеть создаются на основании данных журналов брандмауэра, Web-прокси и фильтров пакетов.

▶ **Просмотр отчета**

1. В дереве консоли ISA Management разверните узел **Monitoring** и папку **Reports.** Затем щелкните нужную папку: **Summary** — для просмотра сводных отчетов, Web Usage — для просмотра отчетов об использовании Web. Папка **Application** Usage содержит отчеты об использовании приложений, **Traffic&**Utilization — отчеты о трафике, **Security** — отчеты об атаках на сеть.
2. В области сведений щелкните правой кнопкой мыши нужный отчет и выберите команду **Open.**

▶ **Упорядочение данных в отчете**

1. В дереве консоли ISA Management разверните узел **Monitoring** и лапку **Reports.** Затем щелкните правой кнопкой мыши нужную папку и в контекстном меню выберите команду **Properties.**
2. Выберите метод упорядочения данных, выбрав на вкладке **Protocols** соответствующий переключатель в области **Sort Order.** При выборе **Requests** отчеты упорядочиваются по числу запросов, а если выбрать **Users** — по активности пользователей.

Примечание Изменения вступят в силу при следующем просмотре отчетов.

Конфигурирование заданий по созданию отчетов

Механизм создания отчетов ISA-сервера позволяет создавать отчеты на основе информации из журналов различных служб в соответствии с определенным расписанием. Отчеты

можно создавать однократно, ежедневно, ежемесячно или в указанный день недели, определив, кроме того, период времени, за который собираются обобщенные данные — за день, неделю, месяц, год или за любой другой период времени.

Для определения порядка создания отчетов следует создать соответствующее задание. В каждом таком задании указывается период времени, информация, обобщаемая в отчете, и периодичность их создания.

► **Создание отчетного задания**

1. В дереве консоли ISA Management разверните узел **Monitoring Configuration**, щелкните правой кнопкой мыши папку **Report Jobs.** В открывшемся меню выберите пункт New и в развернувшемся списке выберите **Report Job.**
2. На вкладке **General** в текстовом поле **Name** укажите имя задания.
3. В текстовом поле **Description** при необходимости указывается описание создаваемого задания.

   На вкладках **Period, Schedule** и **Credentials** укажите:
   - период времени за который выполняется обобщение;
   - периодичность создания отчетов;
   - учетную запись пользователя, под которой будет создаваться отчет.

► **Определение периода обобщения информации в существующем задании**

1. В дереве консоли ISA Management разверните узел **Monitoring Configuration и** щелкните папку **Report Jobs.**
2. В области сведений щелкните правой кнопкой мыши нужное задание и в контекстном меню выберите команду **Properties.**
3. На вкладке **Period** выполните следующие действия:
   - чтобы создаваемый отчет содержал информацию за предыдущий день, щелкните переключатель **Daily;**
   - чтобы создаваемый отчет содержал информацию за предыдущую неделю, щелкните переключатель **Weekly;**
   - чтобы создаваемый отчет содержал информацию за предыдущий месяц, щелкните переключатель **Monthly;**
   - чтобы создаваемый отчет содержал информацию за предыдущий год, щелкните переключатель **Yearly;**
   - если вы хотите создавать отчеты, обобщающие информацию за другой период времени, щелкните переключатель **Custom и** в текстовых полях **From** и **To** укажите даты начала и конца требуемого отрезка времени.

► **Определение периодичности создания отчетов**

1. В дереве консоли ISA Management разверните узел **Monitoring Configuration,** щелкните папку **Report Jobs.**
2. В области сведений щелкните правой кнопкой мыши соответствующее задание и в контекстном меню выберите команду **Properties.**
3. На вкладке **Schedule** выполните следующие действия:
   - чтобы создать отчет немедленно, установите переключатель **Immediately;**
   - чтобы создать отчет в определенное время, установите переключатель в положение At и укажите дату и время.
4. В области **Recurrence Pattern** выполните следующие действия:
   - если требуется создать лишь один отчет, установите переключатель в положение **Generate Once;**

- чтобы отчеты создавались каждый день, установите переключатель в положение Generate Every **Day;**
- чтобы отчеты создавались в определенные дни, установите переключатель в положение **Generate on the following days** и отметьте соответствующие флажки;
- чтобы отчеты создавались один раз в месяц, установите переключатель в положение **Generate once a month** и укажите, какого числа следует создавать отчет.

Учетные записи для создания отчетов

Для каждого задания (удаленного или локального) по созданию отчетов следует определить имя пользователя и пароль для учетной записи, под которой он создается. Такую операцию следует выполнить для каждого сервера массива. Отчеты вправе создавать члены группы **Domain Admins** (Администраторы домена), а также пользователи со следующими полномочиями:

- правами локального администратора на всех компьютерах ISA-серверов в массиве;
- правами на доступ и запуск объектов DCOM на всех серверах массива.

▶ **Определение учетной записи для выполнения задания по созданию отчета**

1. В дереве консоли ISA Management разверните узел **Monitoring Configuration** и щелкните папку **Report Jobs.**
2. В области сведений щелкните правой кнопкой мыши нужное задание и в контекстном меню выберите команду **Properties.**
3. На вкладке **Credentials** в текстовом поле **Username** укажите имя пользователя, обладающего правом создавать отчеты.
4. В текстовом поле **Domain** укажите домен учетной записи.
5. В текстовом поле **Password** укажите пароль учетной записи.

Конфигурирование сводок журналов

Отчеты создаются на основе сводок базы данных, в которой хранятся журналы ISA-сервера. Эти данные вносятся в базу в виде ежедневных и ежемесячных сводок.

Если включен процесс записи сводок, ежедневная сводка создается в 0:30 независимо от расписания отчетов на основании журналов всех серверов массива.

Ежемесячная сводка создается на основании всех имеющихся в базе данных ежедневных сводок. Если какой-то ежедневной сводки нет, информация считывается непосредственно из журналов. Если требуемую информацию в журналах найти не удается, механизм создания ежемесячной сводки возвращает ошибку.

Если запись ежедневных и ежемесячных сводок не ведется, информация для отчетов извлекается непосредственно из соответствующих журналов. Однако в **этом** случае отчет может оказаться неполным или не содержать наиболее свежую информацию.

▶ **Включение и настройка записи сводок**

1. В дереве консоли ISA Management разверните узел **Monitoring Configuration,** щелкните правой кнопкой мыши папку **Report Jobs** и в контекстном меню выберите команду **Properties.**
2. Перейдите на вкладку **Log Summaries** и установите флажок **Enable daily and monthly summaries.**
3. В области **Number of summaries saved** текстового поля **Daily summaries** укажите, сколько ежедневных сводок следует сохранять.
4. В текстовом поле **Monthly summaries** укажите, сколько ежемесячных сводок следует сохранять.

Примечание Число ежедневных сводок выбирается из диапазона 35–999, а ежемесячных — из диапазона 13–999. Минимальные значения обеспечивают количество сводок, достаточное для создания ежемесячных и ежегодных отчетов.

База данных для хранения отчетов

Механизм создания отчетов ISA-сервера объединяет сводки со всех компьютеров массива в базу данных на каждом сервере. Таким образом, при создании отчета базы данных со сводками объединяются в единую базу данных для отчетности. Место размещения новой базы данных указывается при создании задания на создание отчета (рис. 9-15). По умолчанию она размещается в подпапке ISAReports установочной палки ISA-сервера. Обычно путь к этому каталогу выглядит следующим образом: *%ProgramFiles%*\MicrosoftISAServer\ISA Reports.

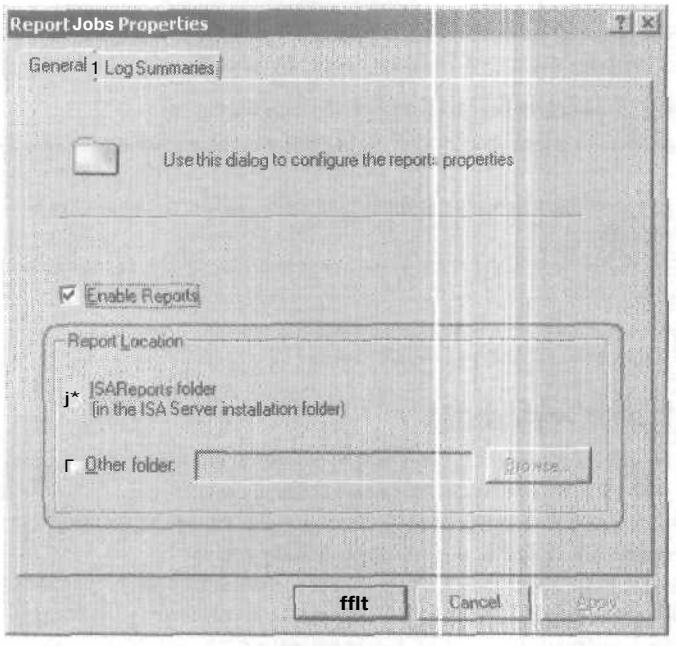


Рис. 9-15. Выбор местоположения базы данных для отчетов

Просмотреть отчет можно только на том компьютере, где есть файл с базой данных. Запустив оснастку ISA Management с другого компьютера массива, просмотреть отчет не удастся.

▶ **Выбор местоположения базы данных с отчетом**

1. В дереве консоли ISA Management разверните узел **Monitoring Configuration,** щелкните правой кнопкой мыши папку **Report Jobs** и в контекстном меню выберите команду **Properties.**
2. Убедитесь, что на вкладке **General** установлен флажок **Enable Reports.**
3. Далее выполните следующие операции:
   - чтобы отчеты сохранялись в подпапке ISAReports установочной папки ISA-сервера, установите переключатель в положение **ISAReports folder (in the ISA Server installation folder).**

- чтобы разместить отчеты в другой папке, установите переключатель в положение **Other folder,** введите нужный путь или щелкните кнопку **Browse** и укажите нужную папку.

▶ **Выбор местоположения базы данных ежедневных сводок**

1. В дереве консоли ISA Management разверните узел **Monitoring Configuration,** щелкните правой кнопкой мыши папку **Report Jobs** и в контекстном меню выберите команду **Properties.**
2. На вкладке **Log Summaries** установите флажок **Enable daily and monthly summaries,**
3. Далее выполните следующие операции:
   - чтобы сводки сохранялись в подпапке **ISASummaries** установочной папки ISA-сервера, установите переключатель в положение **ISASummaries folder (in the ISA Server installation folder).**
   - чтобы разместить сводки в другой папке, установите переключатель в положение **Other Folder,** введите путь или щелкните кнопку **Browse** и укажите нужную папку.

Практикум. **Создание и просмотр отчетов**

Вы настроите задание для создания отчета о деятельности сети и просмотрите созданный отчет.

Задание 1. Создание задания для отчета

Настройте задание для создания отчета о деятельности сети за последний месяц.

▶ **Создание отчетного задания**

1. Войдите в систему сервера Server1 под учетной записью Administrator (Администратор).
2. Откройте оснастку ISA Management и разверните узел **Monitoring Configuration.**
3. Щелкните папку **Report Jobs.**
4. Щелкните правой кнопкой мыши папку **Report Jobs,** в контекстном меню выберите New и в развернувшемся списке выберите команду **Report Job.** Откроется окно свойств задания для создания отчета **Report Job Properties.**
5. На вкладке **General** в текстовом поле **Name** введите **Last Month's Activity.**
6. Перейдите на вкладку **Period.**
7. Установите переключатель в положение **Custom.** В текстовых полях **From** и **To** автоматически устанавливается текущая дата.
8. Щелкните кнопку со стрелочкой рядом с полем со списком **From.** Под списком **From** появится календарь на текущий месяц.
9. Вернитесь на один месяц назад, щелкнув стрелку влево. Теперь в окне календаря отображается предыдущий месяц. Число, совпадающее с сегодняшним числом текущего месяца, выделено синим овалом.
10. Щелкните выделенный день. В текстовом поле **From** отобразится выбранная дата.
11. Перейдите на вкладку **Schedule.** Убедитесь что в области Start **Report Generation** установлен переключатель **Immediately,** а в области **Recurrence Pattern** — переключатель **Generate Once.**
12. Перейдите на вкладку **Credentials.**
13. В текстовом поле **User Name** введите **Administrator.**
14. В текстовом поле **Domain** введите **domain01.**
15. В текстовом поле **Password** введите пароль, определенный в учетной записи domain01\Administrator.

16. Щелкните кнопку OK. В области сведений оснастки ISA Management вы увидите задание **Last Month's Activity.**
17. Щелкните правой кнопкой мыши папку **Report Jobs** и в контекстном меню выберите команду **Refresh.** Задание запушено и его состояние определено как **Running** (оно отображается в колонке **Status).**
18. Через некоторое время еще раз щелкните правой кнопкой мыши папку **Report Jobs и** в контекстном меню выберите команду **Refresh.** Повторяйте это действие до тех пор, пока состояние задания **Last Month's Activity не** изменится на **Ready,** затем переходите ко второму заданию.

Задание 2. Просмотр отчетов

Вы изучите пять отчетов, созданных сконфигурированным ранее заданием.

▶ **Просмотр отчетов ISA-сервера**

1. В дереве консоли ISA Management разверните узел **Monitoring** и щелкните папку **Reports.**
2. В области сведений найдите отчет **LastMonth's Activity.**
3. Щелкните папку **Summary.**
4. В области сведений щелкните правой кнопкой мыши значок **Last Month's Activity** и в контекстном меню выберите команду **Open.** Откроется Web-страница с отчетом **MyArray Array Summary.**
5. Просмотрите все шесть вложенных отчетов сводного отчета, переходя по ссылкам в левой части страницы.
6. Закройте страницу сводного отчета.
7. В окне консоли ISA Management щелкните папку **Web Usage.**
8. В области сведений щелкните правой кнопкой мыши значок **Last Month's Activity** и в контекстном меню выберите команду **Open.** Откроется Web-страница с отчетом **MyArray Array Web Usage.**
9. Просмотрите все восемь вложенных отчетов, переходя по ссылкам в левой части страницы.
10. Закройте отчет.
11. В окне консоли ISA Management щелкните папку **Application Usage.**
12. В области сведений щелкните правой кнопкой мыши значок **Last Month's Activity** и в контекстном меню выберите команду **Open.** Откроется Web-страница с отчетом **MyArray Array Applications Usage.**
13. Просмотрите все пять вложенных отчетов, переходя по ссылкам в левой части страницы.
14. Закройте отчет.
15. В окне консоли ISA Management щелкните папку **Traffic&Utilization.**
16. В области сведений щелкните правой кнопкой мыши значок **Last Month's Activity** и в контекстном меню выберите команду **Open.** Откроется Web-страница с отчетом **MyArray Array** Traffic **and Utilization.**
17. Просмотрите все семь вложенных отчетов, переходя по ссылкам в левой части страницы
18. Закройте отчет.
19. В окне консоли ISA Management щелкните папку **Security.**
20. В области сведений щелкните правой кнопкой мыши значок **Last Month's Activity** и в контекстном меню выберите команду **Open.** Откроется Web-страница с отчетом **MyArray Array Security.**
21. Просмотрите два вложенных отчета, переходя по ссылкам в левой части страницы.
22. Закройте отчет.

Резюме

Механизм создания отчетов ISA-сервера позволяет создавать графические отчеты о характере использования Интернета. Отчеты создаются отчетными заданиями на основании данных журналов ISA-сервера. Последние создаются и настраиваются в узле **Monitoring Configuration** оснастки ISA Management.

Каждое отчетное задание генерирует пять отчетов, отображаемых при просмотре в виде Web-страниц. Отчеты размещаются в отдельные папки узла **Monitoring** оснастки ISA Management. В папке **Summary** хранится сводный отчет, в папке **Web Usage** — отчет об использовании Web, в папке **Application Usage** — отчет об использовании клиентских приложений. Папка **Traffic & Utilization** содержит отчет об используемых приложениях и протоколах, а папка **Security** — отчеты об атаках на сеть.

Поддерживается различная периодичность создания отчетов: однократно, ежедневно, ежемесячно или в указанный день недели. Отчет может содержать обобщенные данные за день, неделю, месяц, год или за любой другой период времени. На каждом сервере массива в заданиях по созданию отчетов следует определить имя пользователя и пароль для учетной записи, под которой будет создаваться отчет.

Механизм создания отчетов ISA-сервера объединяет сводки со всех компьютеров массива в базу данных на каждом сервере. Таким образом, при создании отчета базы данных со сводками объединяются в единую базу данных для отчетности. Просмотреть отчет можно лишь на компьютере, на котором хранится файл с базой данных отчета.

Занятие 4. Управление пропускной способностью

С возрастанием интенсивности обмена данными в сети и через Интернет производительность сети обычно падает. Отчеты ISA-сервера позволяют выяснить причину перегрузок в сети и упорядочить трафик путем назначения различным видам трафика разных приоритетов. Для решения этой задачи используются приоритеты и правила пропускной способности ISA-сервера. Приоритеты пропускной способности — это элементы политики, применяемые для сопоставления входящим и исходящим потокам данных различных приоритетов из диапазона 1-200. Далее эти приоритеты назначаются конкретным подключениям в правилах пропускной способности.

Изучив материал этого занятия, вы сможете:

- ✓ настраивать фактическую пропускную способность для подключений;
- ✓ определять приоритеты пропускной способности;
- ✓ создавать правила пропускной способности.

Продолжительность занятия — около 40 минут.

Понятие фактической пропускной способности

Фактической пропускной способностью (effective bandwidth) называется реальная скорость передачи данных, доступная клиентам сети через определенное подключение к Интернету (например по телефонной или выделенной линии). Чтобы ISA-сервер правильно применял приоритеты пропускной способности, необходимо до создания правил пропускной способности определить фактическую пропускную способность в оснастке ISA Management.

Фактическая пропускная способность подключений по телефонной линии

Первое, что следует сделать при конфигурировании фактической пропускной способности, — определить максимальную пропускную способность подключений на компьютере или массиве ISA-сервера. На модемах пропускная способность определяется скоростью модема, алгоритмами сжатия данных и некоторыми другими факторами. Если значок подключения отображается на системной панели, то, чтобы увидеть скорость подключения, достаточно навести на него курсор мыши.

Фактическую пропускную способность подключений по телефонной линии определяют, изменяя свойства подключения в оснастке ISA Management (рис. 9-16). Для этого изменяют параметры на вкладке **Bandwidth** окна свойств данного подключения.

▶ **Определение фактической пропускной способности подключения по телефонной линии**

1. В дереве консоли ISA Management разверните узел массива, в котором расположено нужное подключение. Разверните узел **Policy Elements**.
2. Щелкните папку **Dial-up Entries**.
3. В области сведений щелкните правой кнопкой мыши нужное подключение и в контекстном меню выберите команду **Properties.** Откроется окно свойств подключения <*имя_подключения*> **Properties.**
4. На вкладке **Bandwidth** установите флажок **Enable bandwidth Control.**
5. В текстовом поле **Effective bandwidth (Kbit/Sec)** укажите фактическую пропускную способность для всех устройств массива.
6. Щелкните кнопку OK.

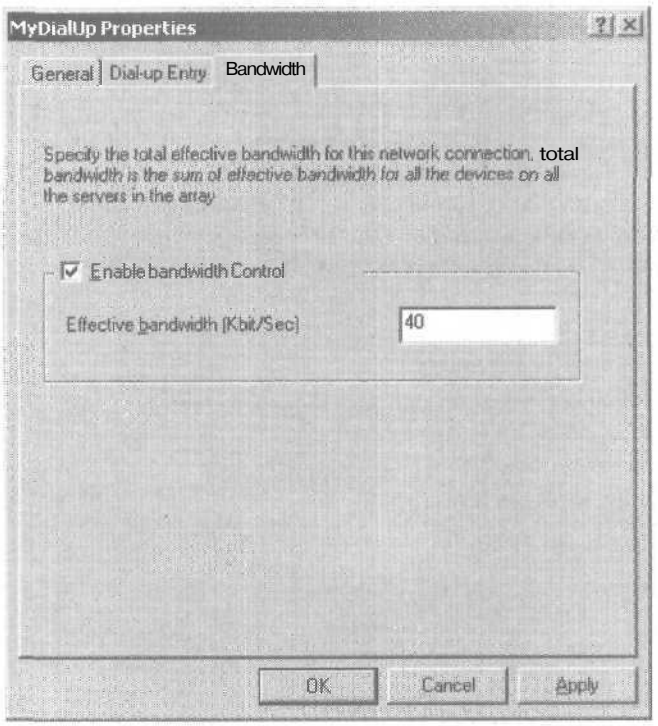


Рис. 9-16. Определение фактической пропускной способности подключения по телефонной линии

Фактическая пропускная способность подключений по выделенной линии

Максимальная скорость передачи данных в линиях ретрансляции кадров (E1/T1 или E3/T3) определяется провайдером. Если значок подключения по выделенной линии отображается на системной панели, то, чтобы увидеть скорость подключения, достаточно навести на него курсор мыши.

Фактическую пропускную способность подключений по выделенной линии определяют, изменяя свойства подключения в оснастке ISA Management (рис. 9-17).

▶ **Определение фактической пропускной способности для сетевой платы**

1. В дереве консоли ISA Management шелкните правой кнопкой мыши папку **Bandwidth Rules** и в контекстном меню выберите команду **Properties.** Откроется окно свойств **Bandwidth Rules Properties.**
2. На вкладке **General** установите флажок **Enable bandwidth Control.**
3. В текстовом поле **Effective bandwidth (Kbit/Sec)** укажите фактическую пропускную способность для сетевых подключений.
4. Щелкните кнопку OK.

Настроив максимальную пропускную способность, изучите отчеты, созданные во время максимальной нагрузки на сеть. Особое внимание уделите изучению того, какая доля пропускной способности выделяется запросам, выполняемым через внутренние и внешние сетевые платы.

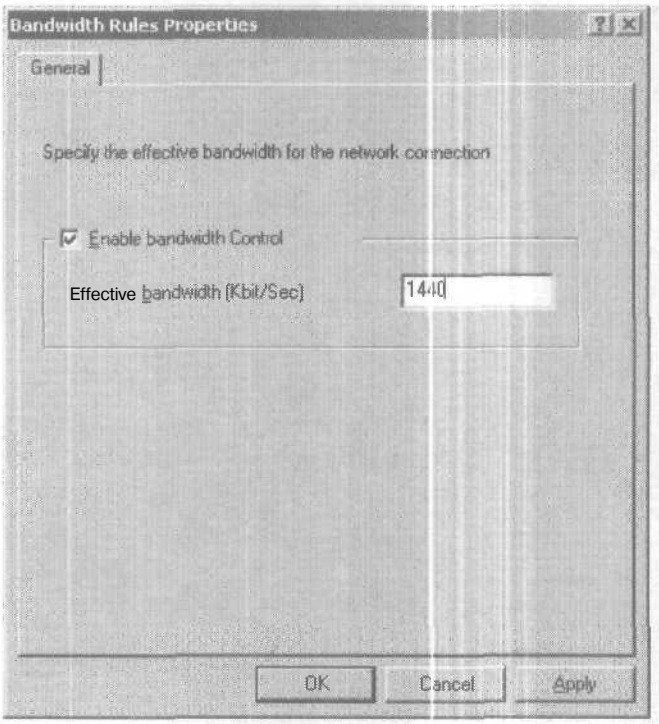


Рис. 9-17. Определение фактической пропускной способности подключения по выделенной линии

Фактическую пропускную способность следует устанавливать равной наименьшей максимальной скорости устройств на компьютере с ISA-сервером. Например, если предельная скорость устройства, поддерживающего внутренние соединения, составляет 100 кбит, а устройства, обслуживающего внешние соединения, — 56 кбит, следует установить фактическую пропускную способность равной 56 кбит.

Значение пропускной способности для внутренних подключений рассчитывают на основании нескольких параметров, в том числе:

- объема трафика между компьютерами в локальной сети;
- объема содержимого кэша, возвращаемого ISA-сервером компьютерам локальной сети;
- объема трафика между членами массива (если для таких подключений не предусмотрено отдельной сетевой платы).

Правила пропускной способности не применяются, когда ISA-сервер возвращает содержимое кэша внешнему компьютеру или пересылает его внутри массива.

Конфигурирование приоритетов пропускной способности

Приоритеты пропускной способности — это элементы политики, применяемые для сопоставления уровней приоритета подключениям, проходящим через ISA-сервер. Далее эти элементы политики применяются в правилах пропускной способности, регулирующих приоритеты отдельных подключений или видов трафика. Подключения, которым приоритет не назначен, считаются наименее важными. При прохождении через ISA-сервер подключения с более высоким приоритетом имеют преимущество перед подключениями с более низким приоритетом.

Приоритеты пропускной способности определяются раздельно для различных направлений.

- **Исходящая пропускная способность** (outbound bandwidth) — это приоритеты, присваиваемые запросам внутренними клиентами объектов в Интернете.
- **Входящая пропускная способность** (inbound bandwidth) — это приоритеты, присваиваемые запросам внешними клиентами объектов, расположенных в локальной сети.

Значения приоритетов пропускной способности выбираются из диапазона 1–200.

ISA-сервер поставляется со встроенным приоритетом с именем Default bandwidth priority. Он присваивает всем (и *входящим* и *исходящим)* подключениям приоритет 100.

Приоритеты пропускной способности используются при создании и настройке правил пропускной способности, регулирующих приоритеты тех или иных подключений. Например, приоритет Best Access (оптимальные условия доступа) с уровнем приоритета для входящих и исходящих запросов равным 150 или приоритет Good Access (хорошие условия доступа) с уровнем 80. В дальнейшем эти приоритеты применяются для конфигурирования правил пропускной способности.

Новые приоритеты пропускной способности создаются в оснастке ISA Management. Для этого щелкните правой кнопкой мыши папку **Bandwidth Priorities,** в контекстном меню выберите пункт New и в развернувшемся списке — команду **Bandwidth Priority** (рис. 9-18). Откроется диалоговое окно New **Bandwidth Priority** (рис. 9-19).

Примечание Использование в системе дополнительно созданных приоритетов требует больших ресурсов по сравнению с применением стандартных (по умолчанию) приоритетов.

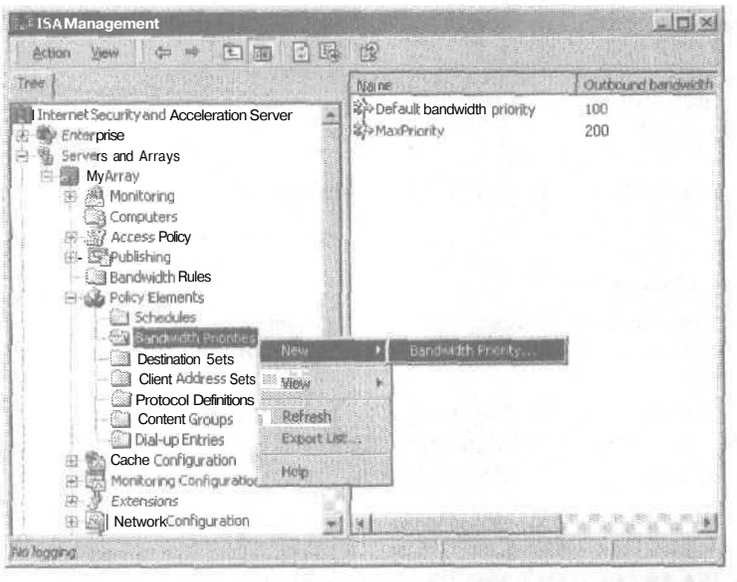


Рис. 9-18. Создание нового приоритета пропускной способности

► ***Создание приоритета*** **пропускной способности**

1. В дереве консоли ISA Management разверните узел массива, в котором требуется создать новый приоритет пропускной способности. Разверните узел **Policy Elements.**
2. Щелкните правой кнопкой мыши папку **Bandwidth Priorities,** выберите команду New и в раскрывшемся подменю щелкните команду **Bandwidth Priority.** Откроется диалоговое окно New **Bandwidth Priority.**

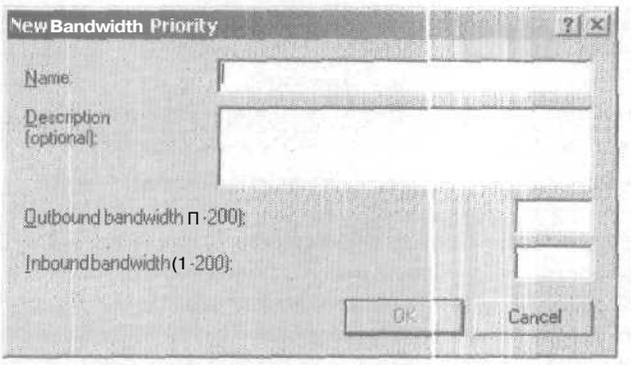


Рис. 9-19. Диалоговое окно New Bandwidth Priority

3. В текстовом поле **Name** укажите имя создаваемого приоритета.
4. В текстовом поле **Description (optional)** при необходимости введите описание нового приоритета.
5. В текстовом поле **Outbound bandwidth (1-200)** определите приоритет исходящих подключений, указав значение из диапазона 1–200.
6. В текстовом поле **Inbound Bandwidth (1-200)** определите приоритет входящих подключений, указав значение из диапазона 1–200.
7. Щелкните кнопку OK.

Конфигурирование правил пропускной способности

Правила пропускной способности применяют заранее определенные приоритеты к различным видам трафика, проходящего через ISA-сервер. Вид трафика определяется комбинацией следующих параметров:

- протокола;
- пользователя, инициировавшего запрос, или IP-адреса источника;
- адресата запроса;
- расписания;
- типа информационного наполнения.

По умолчанию всему входящему и исходящему трафику присваивается стандартный приоритет 100, поэтому, если приоритеты особо не изменялись, весь трафик через ISA-сервер подучает приоритет 100.

Чтобы создать новое правило пропускной способности, воспользуйтесь мастером New **Bandwidth Rule** в оснастке ISA Management. Для этого щелкните правой кнопкой мыши папку **Bandwidth Rules,** выберите команду New и в раскрывшемся подменю укажите команду **Rule** (рис. 9-20).

► **Создание правила пропускной способности**

1. В консольном дереве ISA Management щелкните правой кнопкой мыши папку Bandwidth Rules, выберите команду New и в раскрывшемся подменю укажите пункт **Rule.** Откроется окно мастера New **Bandwidth Rule.**
2. Последовательно выполняйте инструкции мастера.

Примечание До запуска мастера создания нового правила пропускной способности не забудьте создать все необходимые для создаваемого правила элементы политики. Вам могут понадобиться следующие элементы политики: определения протоколов, расписания, наборы адресов клиентов, подмножества адресатов, группы информационного наполнения и приоритеты пропускной способности.

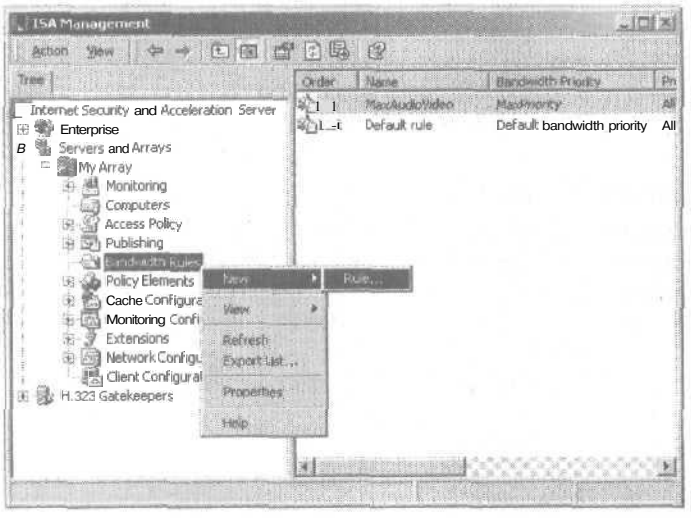


Рис. 9-20. Создание нового правила пропускной способности

▶ **Назначение приоритета существующему правилу пропускной способности**

1. В консольном дереве ISA Management щелкните папку **Bandwidth Rules.**
2. В области сведений щелкните правой кнопкой мыши нужное правило и в контекстном меню выберите команду **Properties.** Откроется окно свойств правила <*имя_правила*> **Properties.**
3. На вкладке **Bandwidth** выполните следующие операции:
   - чтобы применялись приоритеты по умолчанию, установите переключатель в положение **Default scheduling** *priority*;
   - чтобы использовать особые приоритеты, установите переключатель в положение **Specified priority** и в поле со списком **Name** выберите приоритет для данного правила, а также укажите приоритеты для входящего и исходящего трафика.

Приоритеты пропускной способности устанавливаются в одной из двух конфигураций: по умолчанию или в соответствии с предварительно сконфигурированными приоритетами пропускной способности. В первом случае всем подключениям гарантируется минимальная пропускная способность.

Следует иметь в виду, что сопоставление подключениям особых приоритетов приводит к дополнительным издержкам при установке подключения.

Порядок применения правил пропускной способности

Как и правила маршрутизации, правила пропускной способности выполняются в определенном порядке. Правила нумеруются в соответствии с их порядком в списке, отображаемом в области сведений. Правило, заданное по умолчанию, всегда применяется послед-

ним. Администратор вправе изменить порядок применения любых правил, кроме назначенных по умолчанию.

В процессе обработки правила ISA-сервер сравнивает критерии правила с параметрами подключения. Первым обрабатывается правило с номером 1. Если параметры подключения соответствуют критериям правила, оно применяется к подключению. В противном случае обрабатывается следующее правило. Последним обрабатывается и применяется правило по умолчанию. Допустим, первое сопоставленное пользователю UserX правило пропускной способности присваивает входящему и исходящему трафикам приоритет 150, второе правило для этого же пользователя применяется к аудиоданным и присваивает входящему и исходящему трафикам приоритет 200. В этом случае подключение, по которому пользователь UserX пересылает аудиоданные, получит приоритет 150, так как первым обрабатывается правило 1.

▶ **Изменение порядка обработки правил пропускной способности**

1. В дереве консоли ISA Management щелкните папку **Bandwidth Rule.**
2. В области сведений шелкните правой кнопкой мыши правило, положение которого следует изменить, и в контекстном меню выберите команду **Move Up,** чтобы поднять его в списке вверх или **Move Down** — для перемещения вниз. Команды **Move Up** и **Move Down** доступны лишь при условии наличия в списке по крайней мере трех правил.
3. Повторяйте операцию, пока не выстроите все правила в нужном порядке.

Правило пропускной способности, применяемое по умолчанию

При установке ISA-сервера создается правило по умолчанию. Оно гарантирует обслуживание подключений, для которых не определено правило пропускной способности, в соответствии с приоритетами планировщика пакетов QoS Windows 2000.

Правило по умолчанию всегда стоит последним в списке применяемых правил, и его нельзя изменить или удалить.

Практикум. Создание правила пропускной способности

Вы создадите приоритет пропускной способности и затем используете его при создании нового правила пропускной способности.

Задание 1. Создание нового приоритета пропускной способности

Вы создадите новый приоритет, предусматривающий для входящего и исходящего трафика приоритет 200.

▶ **Создание нового приоритета пропускной способности**

1. Войдите в систему сервера Server1 под учетной записью Administrator (Администратор).
2. Откройте оснастку ISA Management, разверните узел MyArray и узел **Policy Elements.**
3. Щелкните правой кнопкой мыши папку **Bandwidth Priorities,** выберите команду New и в раскрывшемся подменю выберите команду **Bandwidth Priority.** Откроется диалоговое окно New **Bandwidth Priority.**
4. В текстовом поле Name введите MaxPriority.
5. В текстовом поле **Outbound Bandwidth (1-200)** введите 200.
6. В текстовом поле **Inbound Bandwidth (1-200)** введите **200.**
7. Щелкните кнопку **OK.**

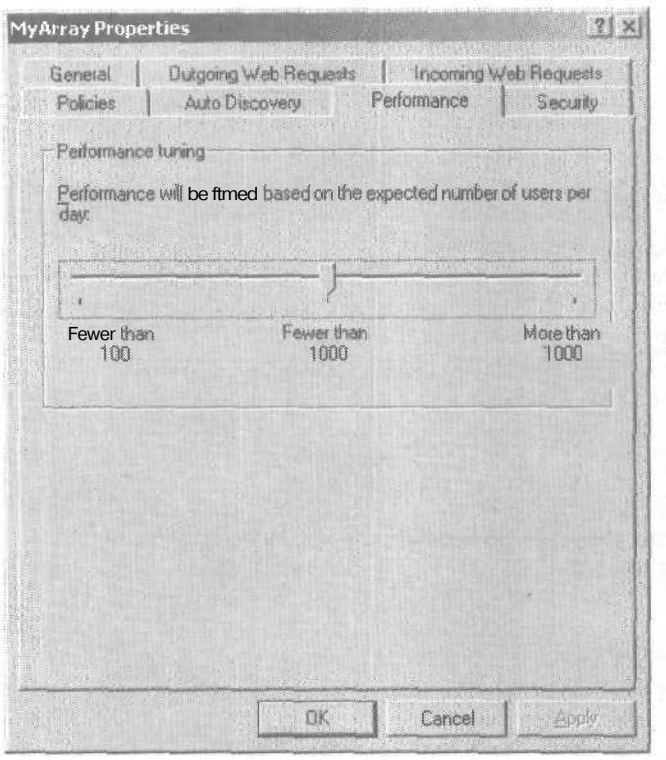


Рис. 9-21. Настройка производительности ISA-сервера

Повышение производительности кэша

При хранении Web-содержимого в кэше ISA-сервер размещает определенную его часть в оперативной памяти. Настраивая объем оперативной памяти, выделяемый для кэша, вы можете влиять на производительность кэша. Увеличение доли памяти, используемой для кэширования, снижает время отклика: ведь больший объем данных хранится в оперативной памяти, а не на жестких дисках. Однако, если доля оперативной памяти, выделенная под кэш слишком велика, общая производительность снизится, так как уменьшится объем памяти, доступной другим приложениям и заданиям ISA-сервера, а также операционной системе.

Объем оперативной памяти регулируется на вкладке **Advanced** окна **Cache Configuration Properties** (рис. 9-22).

▶ **Настройка объема оперативной памяти, выделяемой для кэширования**

1. В дереве консоли ISA Management щелкните правой кнопкой мыши узел **Cache Configuration** и в контекстном меню выберите команду **Properties.** Откроется окно **Cache Configuration Properties.**
2. Перейдите на вкладку **Advanced** и в текстовом поле **Percentage of free memory to use for caching** укажите число из диапазона 1 — 100 (доля памяти для кэширования измеряется в процентах).

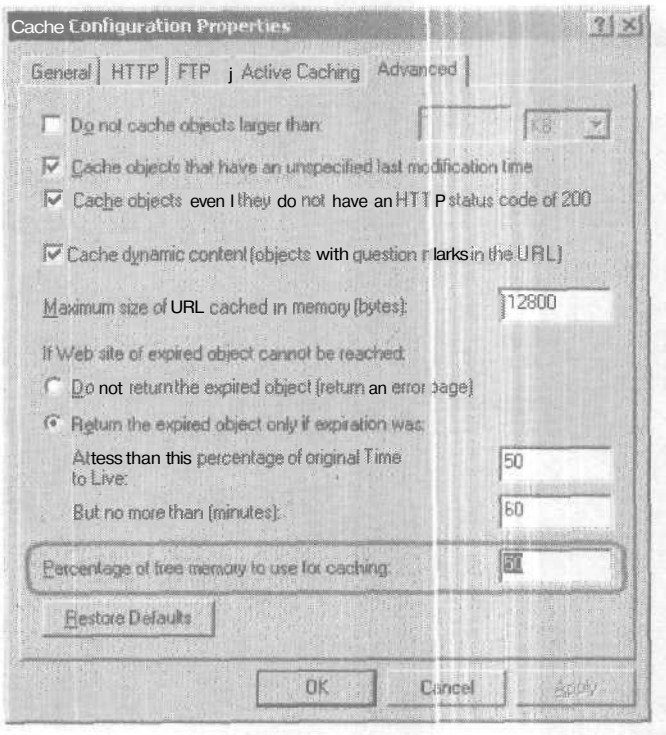


Рис. 9-22. Настройка объема выделяемой под кэш оперативной памяти

Объекты и счетчики производительности ISA-сервера

Данные счетчиков производительности являются важным источником информации о работе сервера. Они позволяют оценивать рабочую нагрузку сервера и использование ресурсов системы, динамику изменения производительности, позволяют более точно настраивать конфигурацию и планировать будущие изменения, отслеживать влияние изменений на работу системы и диагностировать неполадки производительности.

При установке ISA-сервера в консоли Performance (Быстродействие) Windows 2000 появляется семь дополнительных объе <тов производительности:

- ISA Server Firewall Service;
- ISA Server Cache;
- ISA Server Web Proxy Service;
- ISA Server Packet Filter;
- ISA Server Bandwidth Control;
- H.323 Filter;
- SOCKS Filter.

Каждому из них соответствует несколько счетчиков, применяемых для наблюдения за работой ISA-сервера как в реальном времени, средствами узла **System Monitor,** так и с применением журналов счетчиков, трассировки и оповещений в узле **Performance Logs and Alerts.**

Оснастка ISA Server Performance Monitor

В составе ISA-сервера поставляется встроенная оснастка Windows 2000 с именем **ISA Server Performance Monitor,** Ее расположение в меню **Start** (Пуск) показано на рис, 9-23.

Консоль содержит узлы System **Monitor, Performance** Logs **and Alerts** и применяется для наблюдения за производительностью ISA-сервера. В узле System **Monitor** расположен 21 счетчик, из которых 6 относятся к объекту ISA Server Cache, 8 — к объекту ISA Server Firewall service, 1 — к ISA Server Packet Filter и 6 — к объекту ISA Server Web Proxy service. Общий вид консоли показан на рис. 9-24.

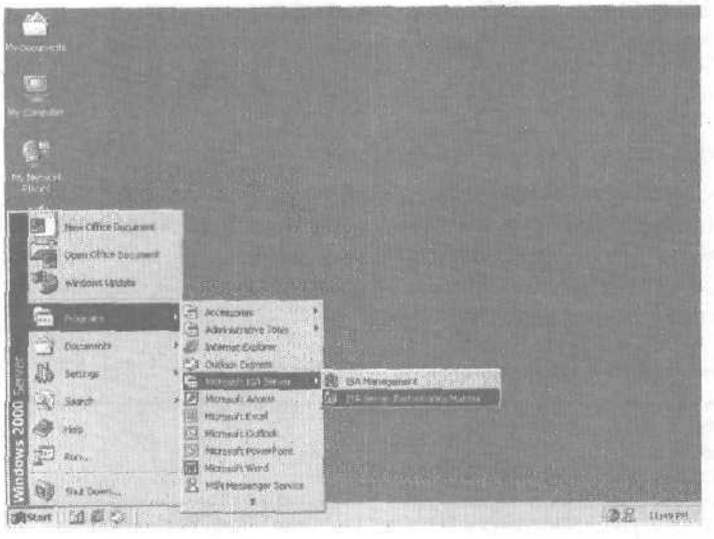


Рис. 9-23. Запуск оснастки ISA Server Performance Monitor

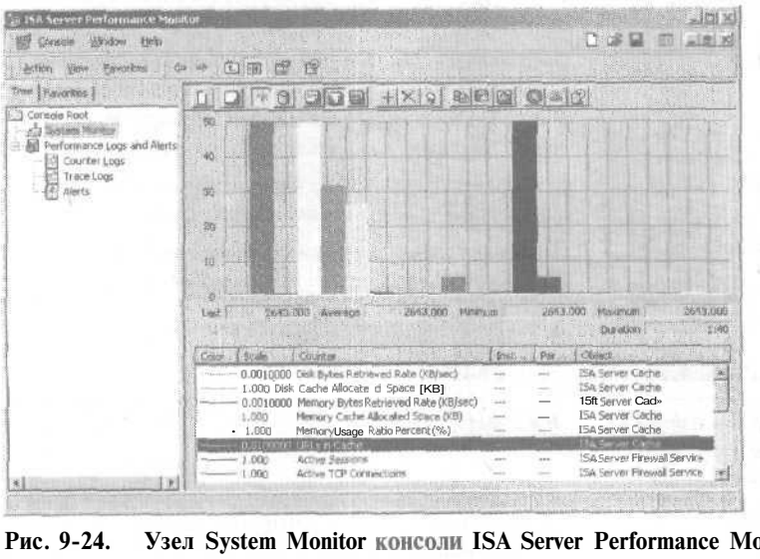


Рис. 9-24. Узел System Monitor консоли ISA Server Performance Monitor

Данные о производительности системы отображаются в виде отчета, графика или гистограммы. В отчетах содержится текстовая информация, а графические представления наглядно иллюстрируют работу ISA-сервере. Журналы производительности полезны при оценке результатов измерений в течение длительных периодов времени. Кроме того, существует возможность сконфигурировать специальное оповещение о достижении счетчиками заданного значения. В качестве действия, выполняемого в ответ на такое оповещение, можно определить создание записи в журнале, отправку сетевого сообщения или запуск программы. Подробнее о функциях и особенностях средств наблюдения за производительностью Windows 2000 — в справочной системе Windows 2000 Server.

Примечание Наблюдение за производительностью недоступно при удаленном администрировании,

Объекты и счетчики производительности ISA-сервера

Далее перечислены и кратко описаны 7 объектов производительности ISA-сервера и соответствующие им счетчики. Кроме того, указано, какие счетчики в узле **System Monitor** консоли ISA Server **Performance Monitor** загружаются автоматически.

В таблице 9-8 перечислены счетчики производительности пропускной способности (объект ISA Server Bandwidth Control).

Таблица 9-8. Счетчики производительности пропускной способности

Счетчик	Автоматическая загрузка в System Monitor	Описание
Actual inbound bandwidth	Нет	Фактическая пропускная способность входящих подключений
Actual outbound bandwidth	Нет	Фактическая пропускная способность исходящих подключений
Assigned connections	Нет	Применяется для измерения способность исходящих с определенным приоритетами пропускной способности. Подключения, для которых приоритет не определен, обладают наименьшей приоритетностью
Assigned inbound bandwidth	Нет	Применяется для измерения выделенной пропускной способности для входящих подключений
Assigned outbound bandwidth	Нет	Применяется для измерения выделенной пропускной способности для исходящих подключений

В таблице 9-9 перечислены счетчики производительности кэша (объект ISAServer Cache).

Таблица 9-9. Счетчики производительности кэша

Счетчик	**Автоматическая загрузка в System Monitor**	**Описание**
Active Refresh Bytes Rate (KB/sec)	Нет	Скорость (в кбайт/с), с которой извлекаются данные из Интернета для активного обновления кэша. Связан с конфигурацией активного кэширования

Таблица 9-9. ***(продолжение)***

Счетчик	Автоматическая загрузка в System Monitor	Описание
Active URL Refresh Rate (URL/sec)	Нет	Скорость (URL-адресов в секунду) активного обновления содержимого кэша. Связан с конфигурацией активного кэширования
Disk Bytes Retrieved Rate (KB/sec)	Да	Скорость считывания данных из дискового кэша. Этот счетчик аналогичен счетчику Disk URL Retrieve Rate, но измеряет скорость не в URL-адресах в секунду, а в килобайтах в секунду
Disk Cache Allocated Space (KB)	Да	Объем дискового пространства, занятый под данные кэша. Это значение всегда меньше или равно максимальному объему дискового пространства, отведенному под кэш
Disk Content Write Rate (Writes/Sec)	Нет	Число записей в дисковый кэш в секунду
Disk Failure Rate (Fail/Sec)	Нет	Число ошибок дискового ввода/вывода за секунду. Ошибка ввода/вывода возникает при неудачной попытке чтения или записи в кэш. Используется совместно со счетчиком Total Disk Failures для выявления неполадок дискового кэша
Disk URL Retrieve Rate (URL/Sec)	Нет	Число URL-адресов, обслуживаемых с использованием данных кэша за секунду. Полезен для наблюдения за работой дискового кэша во время максимальной и обычной активности. Совместно со счетчиком Memory URL Retrieve Rate применяется для изучения использования кэшей в оперативной памяти и на диске
Max URLs Cached	Нет	Максимальное количество URL-адресов, данные которых содержатся в кэше
Memory Bytes Retrieved Rate (KB/Sec)	Да	Скорость считывания данных из кэша в оперативной памяти. Аналогичен счетчику Memory URL Retrieve Rate, но измеряет скорость не в URL-адресах в секунду, а в килобайтах в секунду
Memory Cache Allocated Space (KB)	Да	Объем оперативной памяти, занятый данными кэша. Это значение всегда меньше или равно максимальному объему оперативной памяти, отведенному под кэш
Memory URL Retrieve Rate (URL/Sec)	Нет	Скорость (URL-адресов в секунду) обслуживания внешних запросов с применением данных кэша в оперативной памяти. Полезен для наблюдения за работой кэша во время максимальной и обычной активности и оценки эффективности использования оперативной памяти для хранения данных кэша
Memory Usage Ratio Percent (%)	Да	Соотношение числа запросов, обслуженных с использованием кэша в оперативной памяти, к общему числу обращений в кэш. При высоком значении этого счетчика имеет смысл увеличить объем кэша в оперативной памяти, а при низком — освободить часть памяти для других задач

(см. след. стр.)

Таблица 9-9. *(продолжение)*

Счетчик	Автоматическая загрузка в System Monitor	Описание
Total Actively Refreshed URLs	**Нет**	Общее число URL-адресов, данные по которым получены из Интернета в процессе активного обновления. Отражает производительность системы активного кэширования
Total Bytes Actively Refreshed (KB)	Нет	Общее число байт, полученных из Интернета в процессе активного обновления содержимого кэша. Отражает производительность системы активного кэширования
Total Disk Bytes Retrieved (KB)	Нет	Общее число байт, полученных из дискового кэша. Сумма показаний данного счетчика и счетчика Total Memory Bytes Retrieved (KB) отражает общее число байт, полученных из кэша
Total Disk Failures	Нет	Общее число неудачных попыток записи или чтения службой Web-прокси. Невысокое значение данного счетчика свидетельствует об удовлетворительной производительности работы диска. Большое количество ошибок обычно указывает на недостаток свободного пространства на диске, неудовлетворительную работу или повреждение диска
Total Disk URLs Retrieved	Нет	Общее число запросов URL-адресов, обслуженных с использованием данных дискового кэша. Сумма показаний данного счетчика и счетчика Total Memory URLs Retrieved отражает общее число URL-адресов, обслуженных с использованием данных кэша
Total Memory Bytes Retrieved (KB)	Нет	Общее число байт, полученных из кэша в оперативной памяти. Низкие показания этого счетчика обычно указывают на недостаточно эффективное использование памяти, отведенной под кэш. При высоких показаниях рекомендуется увеличить объем кэша в памяти
Total Memory URLs Retrieved	Нет	Общее количество запросов URL-адресов, обслуженных с использованием данных кэша в памяти. Низкие показания этого счетчика обычно указывают на недостаточно эффективное использование памяти, отведенной под кэш, При высоких показаниях рекомендуется увеличить объем кэша в памяти
Total URLs Cached	Нет	Общее число URL-адресов, данные которых содержатся в кэше. Низкие значения данного счетчика и счетчика URLs in Cache говорят о неоптимальной конфигурации кэша или о недостаточном его размере

Таблица 9-9. *(окончание)*

URL Commit Rate (URL/Sec)	Нет	Скорость (URL-адресов в секунду) записи в кэш данных, расположенных по URL-адресах. Если показания этого счетчика по порядку совпадают с показаниями счетчика Disk Failure Rate (Fail/Sec), большая часть попыток записи в кэш заканчивается неудачно. Это происходит из-за неверной конфигурации кэша, слишком медленной работы жесткого диска, на котором расположен кэш, или недостаточного размера кэша
URLs in Cache	**Да**	Текущее количество URL-адресов, данные которых расположены в настоящий момент в кэше

В таблице 9-10 перечислены счетчики производительности службы брандмауэра (объект ISA Server Firewall Service).

Таблица 9-10. Счетчики производительности службы брандмауэра

Счетчик	Автоматическая загрузка в System Monitor	Описание
Accepting TCP Connections	**Нет**	Число объектов-подключений, ожидающих TCP-подключения от клиентов брандмауэра
Active Sessions	**Да**	Число активных сеансов брандмауэра
Active TCP Connections	Да	Общее число TCP-подключений, активно передающих данные. Неактивные или еще не установленные подключения не учитываются
Active UDP Connections	Да	Общее число активных подключений по протоколу UDP
Available Worker Threads	Да	Число рабочих потоков брандмауэра, которые доступны или находятся в очереди порта завершения
Back-connecting TCP Connections	Нет	Общее число TCP-подключений ожидающих входящего вызова на подключение. Это подключения, устанавливаемые службой брандмауэра с клиентом после того, как брандмауэр принял подключение из Интернета на прослушивающий сокет
Bytes Read/sec	Да	Количество байт в секунду, считываемых механизмом передачи данных
Bytes Written/sec	Нет	Количество байт в секунду, записываемых механизмом передачи данных
Connecting TCP Connections	Нет	Общее количество ожидающих завершения TCP-подключений между службой брандмауэра и удаленными компьютерами
DNS Cache Entries	**Нет**	Текущее число записей доменных имен службы DNS, размещенных в кэше в процессе работы брандмауэра
DNS Cache Flushes	**Нет**	Число сбросов или очистки кэша доменных имен DNS службой брандмауэра
DNS Cache Hits	**Нет**	Число доменных имен полученных службой брандмауэра из кэша DNS

(см. след. стр.)

Таблица 9-10. (*окончание*)

Счетчик	Автоматическая загрузка в System Monitor	Описание
DNS Cache Hits %	Нет	Доля (в процентах) доменных имен, полученных из кэша DNS, в общем числе разрешенных доменных имен
DNS Retrievals	**Нет**	Общее число доменных имен, полученных службой брандмауэра
Failed DNS Resolutions	Нет	Число неудачных API-запросов gethostbyname и gethostbyaddr. Эти запросы применяются для разрешения доменных имен и IP-адресов при обслуживании подключений службы брандмауэра
Kernel Mode Data Pumps	Да	Число созданных службой брандмауэра каналов передачи данных
Listening TCP Connections	Нет	Число объектов, ожидающих подключений по протоколу TCP от удаленных компьютеров Интернета
Non-connected UDP mappings	Нет	Число сопоставлений, доступных для подключений по UDP
Pending DNS Resolutions	Нет	Число API-запросов gethostbyname и gethostbyaddr, ожидающих ответа. Эти запросы применяются для разрешения доменных имен и IP-адресов при обслуживании подключений службы брандмауэра
Secure NAT Mappings	Да	Число сопоставлений, созданных по протоколу SecureNAT
Successful DNS Resolutions	Нет	Число полученных ответов на API-запросы gethostbyname и gethostbyaddr. Эти запросы применяются для разрешения доменных имен и IP-адресов при обслуживании подключений службы брандмауэра
TCP Bytes Transferred/sec by Kernel Mode Data Pump	Нет	Количество байт, передаваемых по протоколу TCP за секунду
UDP Bytes Transferred/sec by Kernel mode Data Pump	Нет	Количество байт, передаваемых по протоколу UDP за секунду
Worker Threads	Да	Число активных рабочих потоков брандмауэра

В таблице 9-11 перечислены счетчики производительности фильтров пакетов (объект ISA Server Packet Filter).

Таблица 9-11. Счетчики производительности фильтров пакетов

Счетчик	Автоматическая загрузка в System Monitor	Описание
Packets Dropped Due to Filter Denial	Нет	Общее число пакетов, отброшенных механизмом динамической фильтрации пакетов. Этот счетчик учитывает все отброшенные пакеты, то есть пакеты, не учтенные счетчиком Packets Dropped Due to Protocol Violations. Другими словами он учитывает пакеты, отброшенные в рамках стандартной политики ISA-сервера «denyall» (игнорирование всех пакетов). Исключение составляют лишь пакеты, пропущенные специально настроенными разрешающими фильтрами
Packets Dropped Due to Protocol Violations	Нет	Общее число пакетов, отброшенных из-за несоблюдения стандартов протоколов. Здесь учитываются пакеты, отброшенные не обычными правилами фильтрации, а вследствие других причин. В частности, этот счетчик учитывает пакеты, отброшенные механизмами фильтрации IP-фрагментов или обнаружения вторжений
Total Dropped Packets	**Да**	Общее число отброшенных пакетов — независимо от причины
Total incoming connections	**Нет**	Общее число подключений, обслуживаемых через интерфейсы с настроенными фильтрами
Total Lost Logging Packets	Нет	Общее число отброшенных пакетов, сведения о которых не регистрируются в журналах

В таблице 9-12 перечислены счетчики производительности службы Web-прокси (объект ISA Server Web Proxy Service).

Таблица 9-12. Счетчики производительности службы Web-прокси

Счетчик	Автоматическая загрузка в System Monitor	Описание
Array Bytes Received/sec (Enterprise)	Нет	Скорость (байт в секунду) входящих данных от других серверов массива
Array Bytes Sent/sec (Enterprise)	Нет	Скорость (байт в секунду) исходящих данных, направленных другим серверам массива
Array Bytes Total/sec (Enterprise)	Нет	Сумма показаний двух предыдущих счетчиков. Отображает общую скорость обмена информацией между данным компьютером и другими серверами массива

(см. след. стр.)

Таблица 9-12. (*продолжение*)

Счетчик	Автоматическая загрузка в System Monitor	Описание
Cache Hit Ratio %	Да	Доля (в процентах) клиентских запросов, обслуженных с использованием данных из кэша (счетчик Total Cache Fetches) в общем числе клиентских запросов (счетчик Total Successful Requests). Наглядно представляет эффективности работы кэша. Высокое показание счетчика указывает на большую долю запросов, обслуживаемых из кэша, то есть на снижение среднего времени отклика. Низкое значение часто обусловлено неоптимальной конфигурацией кэша — недостаточным его размером или большим числом запросов, которые не подлежат кэшированию. Нулевое показание счетчика свидетельствует об отключенном кэшировании
Cache Running Hit Ratio (%)	Да	Доля (в процентах) клиентских запросов, обслуженных с использованием данных из кэша, в общем числе клиентских запросов. Отличие данного счетчика от предыдущего в том, что он измеряет попадания кэша для последних 10 000 запросов, а счетчик Cache Hit Ratio % — для всех запросов с момента последнего запуска службы Web-прокси. Таким образом, этот счетчик представляет более динамичную картину эффективности кэша
Client Bytes Received/sec	Нет	Скорость (байт в секунду) получения данных от клиентов службы Web-прокси. Значение счетчика изменяется в зависимости от объема клиентских запросов, но неизменно низкие показания часто указывают на задержки при обслуживании запросов
Client Bytes Sent/sec	Нет	Скорость (байт в секунду) передачи данных клиентам Web-прокси. Значение счетчика изменяется в зависимости от объема клиентских запросов, но неизменно низкие показания обычно указывают на задержки при обслуживании запросов
Client Bytes	Да	Сумма показаний двух предыдущих Total/sec счетчиков. Отображает общую скорость обмена между ISA-сервером и клиентами Web-прокси
Current Array Fetches Average Milliseconds/ request	Нет	Среднее время обработки запросов (в миллисекундах), обслуживаемых с обращением к другому серверу массива. Запросы, обслуживаемые по SSL-туннелям, не учитываются

Таблица 9-12. *(продолжение)*

Счетчик	Автоматическая загрузка в System Monitor	Описание
Current Average Milliseconds/ request	Да	Среднее время обработки клиентских запросов (в миллисекундах) без учета запросов, обслуживаемых по SSL-туннелям. Полезен для наблюдения за работой кэша во время максимальной и обычной активности и оценки скорости обслуживания клиентских запросов. Слишком высокие показания обычно указывают на неспособность ISA-сервера справиться со всеми запросами, а значит, задержку при их обработке
Current Cache Fetches Average Milliseconds/ request	**Нет**	Среднее время обработки клиентского запроса (в миллисекундах) с использованием кэша. Не учитываются запросы, обслуживаемые по SSL-туннелям
Current Direct Fetches Average Milliseconds/ request	Нет	Среднее время (в миллисекундах) обработки запросов клиента, при которой требуется обращение к Web-серверу или вышестоящему прокси. Не учитываются запросы, обслуживаемые по SSL-туннелям
Current Users	Да	Текущее количество клиентов Web-прокси. Применяется для наблюдения за работой кэша во время максимальной и обычной активности и оценки загруженность сервера. Показания этого счетчика сильно зависят от максимально разрешенного числа подключений. Также он полезен, если необходимо временно остановить службы ISA-сервера
DNS Cache Entries	Нет	Текущее число доменных имен, содержащихся в кэше. Высокие значения счетчика говорят о существенном приросте производительности, так как при разрешении доменных имен из кэша без обращения к серверу DNS снижается потребление системных ресурсов
DNS Cache Flushes	Нет	Число сбросов или очистки кэша доменных имен DNS службой Web-прокси. Кэш DNS сбрасывается при переполнении, то есть если не хватает места для размещения новых имен
DNS Cache Hits	Нет	Число доменных имен, полученных службой Web-прокси из кэша DNS. Сравнение показаний этого счетчика с показаниями двух предыдущих позволяет оценить эффективность работы кэша доменных имен. Низкое число попаданий кэша DNS снижает производительность, поскольку каждое обращение к серверу DNS замедляет работу, особенно если при поиске возникают затруднения

(см. след. стр.)

Таблица 9-12. *(продолжение)*

Счетчик	Автоматическая загрузка в System Monitor	Описание
DNS Cache Hits %	Нет	Доля (в процентах) доменных имен, полученных службой Web-прокси из кэша DNS, в общем количестве разрешенных доменных имен. Высокие значения счетчика информируют о высокой производительности, поскольку большинство доменных имен получено из кэша без обращения к серверу DNS
DNS Retrievals	Нет	Общее число доменных имен, полученных службой Web-прокси
Failing Requests/sec	Нет	Число ошибок обращения к службе Web-прокси t. секунду. Сравнение показаний этого счетчика с показаниями Requests/Sec дает представление о качестве обслуживания входящих запросов. Если большая часть входяших запросов завершается с ошибкой, ISA-сервер не справляется с обработкой запросов. Возможные причины: некорректная конфигурация входящих подключений или маленькая пропускная способность
FTP Requests	Нет	Число запросов FTP к службе Web-прокси. Постоянно низкие показания этого счетчика дают основания пересмотреть политику кэширования объектов FTP
Gopher Requests	Нет	Число запросов системы Gopher
HTTP Requests	Нет	Число запросов к службе Web-прокси по протоколу HTTP
HTTPS Sessions	Нет	Число защищенных сеансов HTTPS, обслуживаемых по SSL-туннелю
Maximum Users	Нет	Максимальное число одновременно подключенных пользователей. Этот счетчик полезен при определении нагрузки на сервер и оценке числа необходимых лицензий
/		
Requests/sec	Да	Число входящих запросов к службе Web-прокси за одну секунду. Чем выше показания этого счетчика, тем больше потребуется ресурсов для обработки запросов
Reverse Bytes Received/sec	Нет	Скорость (байт в секунду), с которой служба Web-прокси принимает данные от опубликованных Web-серверов в ответ на запросы извне. Показания этого счетчика помогают оценить уровень обслуживания ISA-сервером входящих запросов
Reverse Bytes Sent/sec	Нет	Скорость, с которой служба Web-прокси отправляет данные опубликованных Web-серверов в ответ на запросы внешних клиентов. Показания этого счетчика помогают оценить уровень обслуживания ISA-сервером входящих запросов

Таблица 9-12. *(продолжение)*

Счетчик	Автоматическая загрузка в System Monitor	Описание
Reverse Bytes Total/sec	Нет	Сумма показаний двух предыдущих счетчиков. Представляет собой общую скорость обмена данными между службой Web-прокси и опубликованными Web-серверами
Site Access Denied	Нет	Общее число узлов Интернета, доступ к которым был пресечен службой Web-прокси. Высокие показания этого счетчика обычно указывают на чрезмерно строгие ограничения политики доступа
Site Access Granted	Нет	Общее число узлов Интернета, доступ к которым разрешен службой Web-прокси. Сравнение показаний этого и предыдущего счетчиков позволяет оценить корректность конфигурации политики доступа
SNEWS Sessions	Нет	Общее число SNEWS-сеансов, обслуживаемых по SSL-туннелю
SSL Client Bytes Received/Sec	Нет	Скорость приема данных службой Web-прокси от защищенных клиентов Web-прокси. Аналогичен счетчику Client Bytes Recieved/Sec, но учитывает лишь данные, пересылаемые по SSL-туннелям
SSL Client Bytes Sent/sec	Нет	Скорость передачи данных службой Web-прокси защищенным клиентам. Аналогичен счетчику Client Bytes Send/Sec, но учитывает только данные, пересылаемые по SSL-туннелям
SSL Client Bytes Total/sec	Нет	Сумма показаний двух предыдущих счетчиков. Представляет собой общую скорость обмена данными по SSL-туннелям
Thread Pool Active Sessions	Нет	Число активных сеансов, обслуживаемых пулом потоков
Thread Pool Failures	Нет	Число запросов, отклоненных из-за переполнения пула потоков
Thread Pool Size	Нет	Число потоков в пуле потоков. Пул потоков представляет собой ресурсы доступные для обслуживания клиентских запросов
Total Array Fetches (Enterprise)	Нет	Общее число клиентских запросов Web-прокси, обслуженных с обращением к другим серверам массива, то есть запросов, выполняемых с применением протокола Cache Array Routing Protocol (CARP), случайным образом размещающего объекты в кэшах разных серверов массива. На показания этого счетчика влияет размер кэша отдельных серверов массива, поскольку сервер с кэшем большего размера обычно хранит больше объектов. Существует возможность настраивать коэффициент нагрузки отдельных серверов для распределения рабочей нагрузки между серверами массива

(см. след. стр.)

Таблица 9-12. *(продолжение)*

Счетчик	Автоматическая загрузка в *System* Monitor	Описание
Total Cache Fetches	Нет	Общее число клиентских запросов, выполненных с использованием данных кэша. Высокие показатели этого счетчика свидетельствуют о высокой эффективности работы кэша
Total Failed Requests	Нет	Общее количество запросов, которые служба Web-прокси не обслужила из-за ошибок, обусловленных невозможностью для службы Web-прокси обнаружить запрошенный URL-адрес или отсутствием у клиента прав на доступ к запрошенному адресу. Показания этого счетчика должны быть значительно ниже показаний счетчика Total Successful Requests. Если это не так, вероятно, ISA-сервер не справляется с обслуживанием запросов. Причина может заключаться в ошибочной конфигурации, слишком низкой скорости подключения или слишком жестких ограничениях политики доступа
Total Pending Connects	**Нет**	Общее число подключений к службе Web-прокси, находящихся в режиме ожидания
Total Requests	Нет	Общее число запросов к службе Web-прокси. Представляет собой сумму показаний счетчиков Total Successful Requests и Total Failed Requests
Total Reverse Fetches	Нет	Общее число входящих запросов, выполненных с обращением к опубликованным Web-серверам
Total SSL Sessions	Нет	Общее число SSL-сеансов, выполненных по SSL-туннелям
Total Successful Requests	Нет	Общее число успешно обработанных запросов к службе Web-прокси. Сравнение показаний этого счетчика с показаниями счетчиков Total Failed Requests и Total Requests позволяет сделать вывод об уровне эффективности обслуживания запросов ISA-сервером
Total Upstream Fetches	Нет	Общее число запросов, данные для которых запрашивались в Интернете или у вышестоящих прокси-серверов. Сравнение показаний этого счетчика с показаниями счетчика Total Cache Fetches позволяет определить соотношение запросов, обслуживаемых с использованием данных из Интернета или от вышестоящих прокси-серверов, и запросов, выполненных с использованием данных из кэша
Total Users	Нет	Общее число пользователей, подключавшихся к службе Web-прокси. Применяется для сбора статистики использования сервера
Unknown SSL Sessions	Нет	Общее число неопознанных SSL-сеансов, обслуженных по SSL-туннелям

Таблица 9-12. *(окончание)*

Счетчик	Автоматическая загрузка в System Monitor	Описание
Upstream Bytes Received/sec	Нет	Скорость (байт в секунду), с которой служба Web-прокси получает данные от удаленных серверов Интернета или вышестоящих прокси-серверов в ответ на свои запросы. Значение данного счетчика зависит от пропускной способности. Стабильно низкие показания счетчика свидетельствуют о низкой скорости подключения. Это означает, что подключение стало «узким местом». Чтобы исправить положение, следует изменить приоритеты пропускной способности или увеличить скорость подключения
Upstream Bytes Sent/sec	Нет	Скорость, с которой служба Web-прокси передает данные удаленным серверам Интернета или вышестоящим прокси-серверам. Значение данного счетчика зависит от пропускной способности. Стабильно низкие показания счетчика свидетельствуют о низкой скорости подключения. Это означает, что подключение стало «узким местом». Чтобы исправить положение, следует изменить приоритеты пропускной способности или увеличить скорость подключения
Upstream Bytes Total/sec	Нет	Сумма показаний двух предыдущих счетчиков. Представляет собой общую скорость обмена данными между службой Web-прокси и удаленными серверами Интернета или вышестоящими прокси-серверами

Существуют два счетчика для контроля работы фильтра H.323, подсчитывающие число вызовов, обслуживаемых фильтром H.323 ISA-сервера (объект H.323 Filter). Они описаны в таблице 9-13.

Таблица 9-13. Счетчики фильтра H.323

Счетчик	Автоматическая загрузка в System Monitor	Описание
Active H.323 Calls	Нет	Число активных вызовов H.323
Total H.323 Calls	Нет	Общее число вызовов, пропущенных фильтром H.323 с момента запуска ISA-сервера

Сетевой протокол SOCKS позволяет приложениям устанавливать связь через прокси-сервер. Фильтры SOCKS на ISA-сервере пересылают запросы от SOCKS-приложений службе брандмауэра. В таблице 9-14 описаны счетчики производительности этих фильтров (объект SOCKS Filter).

Таблица 9-14. Счетчики производительности фильтров SOCKS

Счетчик	Автоматическая загрузка в System Monitor	Описание
Active Connections	Нет	Число активных подключений, передающих в данный момент информацию. Не учитываются соединения, находящиеся в режиме ожидания или установка которых не завершена
ActiveSessions	Нет	Число активных сеансов SOCKS
Bytes Read/sec	Нет	Скорость **(байт в** секунду) данных, **считываемых** во всех подключениях **SOCKS**
Bytes Written/sec	Нет	Скорость (байт в секунду) данных, записываемых но всех подключениях SOCKS
Connecting Connections	Нет	Число подключений SOCKS, ожидающих соединения с удаленным компьютером
Listening Connections	Нет	Число объектов-подключений, ожидающих соединения с удаленным компьютером
Pending DNS Resolutions	Нет	Число ожидающих ответа запросов к службе DNS. Эти запросы предназначены для разрешения доменных имен и IP-адресов для подключений SOCKS
Successful DNS Resolutions	Нет	Число ответов (в секунду) на запросы службы DNS. Эти запросы предназначены для разрешения доменных имен и IP-адресов для подключений SOCKS

Резюме

Настройка параметров на вкладке **Performance** окна свойств массива в соответствии с ожидаемым количеством ежедневных подключений позволяет повысить производительность серверов массива. Производительность кэша ISA-сервера регулируется путем изменения объема оперативной памяти выделяемого для хранения Web-содержимого. Этот параметр настраивается на вкладке Advanced диалогового окна **Cache Configuration Properties.**

В дополнение к механизмам оповещений, ведения журналов и создания отчетов ISA-сервер содержит 7 объектов для наблюдения за производительностью, каждый из которых содержит счетчики, предназначенные для сбора информации о производительности ISA-сервера. Эти счетчики доступны для просмотра в окне оснастки Performance (Быстродействие) Windows 2000 или в специализированной консоли ISA-сервера ISA Server Performance Monitor, которая позволяет изучать параметры производительности только ISA-сервера, отдельно от остальных параметров системы. По умолчанию в оснастке System Monitor активизирован 21 счетчик.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Ответы для самопроверки — в приложении А «Вопросы и ответы» в конце книги.

1. Какие четыре типа ответных действий выполняются в ответ на оповещение? Какие из них настроены и выполняются по умолчанию?

2. Какое имя получит файл журнала брандмауэра, созданный в формате ISA-сервера 23 октября 2002 года?

3. Какие права необходимы пользователю, чтобы конфигурировать задания для создания отчета?

4. Опишите недостаток назначения подключению приоритета пропускной способности, отличного от приоритета по умолчанию?

5. Каковы преимущества применения консоли ISA Server Performance Monitor для просмотра показаний счетчиков производительности ISA-сервера?

ГЛАВА 10

Устранение неполадок в работе ISA-сервера

Занятие 1. Средства выявления неполадок в работе ISA-сервера 320
Занятие 2, Методики выявления неполадок в работе ISA-сервера 329
Закрепление материала 337

В этой главе

Для эффективного устранения неполадок в сложной сети необходимо хорошо знать используемые для этих целей инструментальные средства и владеть методами точного определения причин неполадок. В этой главе мы вкратце расскажем о средствах и методах устранения неполадок ISA-сервера.

Прежде всего

Для изучения материалов этой главы необходимо:

- выполнить установку в соответствии с инструкциями, приведенными в разделе «Об этой книге»;
- выполнить все упражнения глав 1–9.

Замятие 1. Средства выявления неполадок в работе ISA-сервера

Чтобы эффективно определять и устранять неполадки, возникающие при работе системы безопасности и подключений ISA-сервера, вам необходимо изучить служебные утилиты, применяемые для устранения неполадок сети. К таким средствам относятся как утилиты, предназначенные только для ISA-сервера, так и стандартные средства управления работой протокола TCP/IP и утилиты Microsoft Windows 2000. На этом занятии подробно описано большинство этих средств, а также рассказано, как их использовать для диагностики и устранения неполадок ISA-сервера.

Изучив материал этого занятия, вы сможете:

- ✓ применять средства устранения неполадок ISA-сервера;
- ✓ проверять и изменять таблицы маршрутизации;
- ✓ проверять состояние портов средствами утилит Netstat и Telnet.

Продолжительность занятия — около 45 минут.

Средства устранения неполадок

Для выяснения причин неполадок работающего ISA-сервера применяются различные инструментальные средства. В зависимости от вида неполадки используется одно или несколько из перечисленных ниже средств:

- отчеты ISA-сервера;
- оснастка Event Viewer (Просмотр событий);
- оснастка Performance Monitor (Производительность);
- утилита командной строки Netstat;
- утилита командной строки Telnet;
- Network Monitor (Сетевой монитор);
- таблицы маршрутизации.

Отчеты ISA-сервера

Отчеты ISA-сервера обычно применяются для первичной диагностики. Как правило, при выявлении причин снижения производительности просматривают один или несколько отчетов. Например, когда пользователи жалуются на медленную работу Web, следует изучить отчет Cache Performance в подборке отчетов Traffic and Utilization (рис. 10-1). Однако, даже если отчет информирует о низком значении попаданий кэша, следует просмотреть другие отчеты и определить, действительно ли это является причиной неудовлетворительного отклика на запросы Web-ресурсов. При отключенном активном кэшировании и отсутствии заданий по загрузке файлов из Интернета ISA-сервер не в состоянии извлекать ответы на HTTP-запросы из кэша, и на компьютерах конечных пользователей Web-страницы отображаются с задержкой. С другой стороны, если отчеты информируют об эффективном использовании кэша, причиной задержек может быть перегрузка сети, например, обусловленная интенсивной загрузкой данных или слишком малым значением *времени жизни* (time-to-live, TTL).

Примечание Неудовлетворительную производительность из-за неэффективного использования кэша корректируют, планируя частоту и объемную загрузку Web-содержимого в нерабочее время или увеличивая TTL средствами диалогового окна **Cache Configuration** Properties.

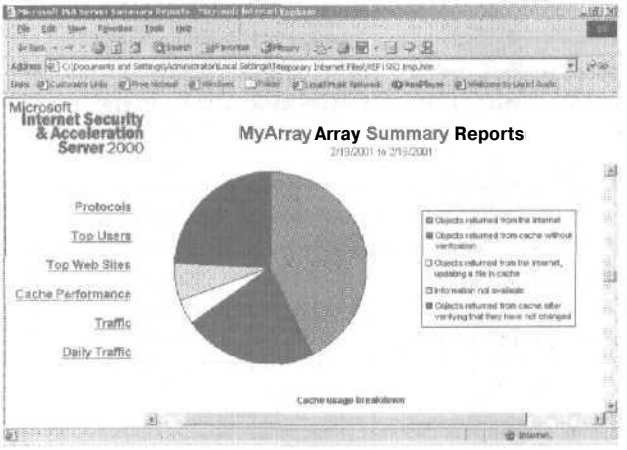


Рис. 10-1. Пример отчета о производительности кэша

Оснастка Event Viewer (Просмотр событий)

В процессе устранения неполадок ISA-сервера применяется оснастка Event Viewer (Просмотр событий) операционной системы Microsoft Windows 2000. В ней отображаются все сообщения о событиях, инициированные службами ISA-сервера. Сообщения делятся на оповещения, уведомления об ошибках и информационные уведомления. Обнаружив интересующее вас сообщение службы, откройте его двойным щелчком мыши, обратите внимание на идентификатор события (Event ID). Подробнее об идентификаторах событий и рекомендуемых способах исправления неполадки — в справочной системе ISA-сервера или в приложении «Сообщения о событиях», расположенном на компакт-диске.

Оснастка Performance Monitor (Производительность)

Оснастка Performance Monitor помогает устранить неполадки, связанные с оборудованием и конфигурацией, а также работой сети. Например, если при поиске причины низкой производительности кэша обнаруживается, что счетчик %Disk Time показывает высокие значения, а счетчик Disk Bytes/sec информирует о низкой скорости дискового обмена, то для повышения производительности кэш-памяти следует добавить новый диск. Если же значение счетчика Disk Bytes/sec не слишком низкое, но счетчик Pages/sec показывает высокий уровень ошибок страниц, то, чтобы решить проблему низкой производительности кэш-памяти, надо добавить в систему дополнительную память или выделить дополнительную память под кэш.

Для успешного выявления неполадок средствами ISA Server Performance Monitor следует установить базовые значения счетчиков, превышение которых свидетельствует о неполадках.

Утилита Netstat

Netstat — это утилита командной строки, применяемая для выявления неполадок безопасности и подключений. Она позволяет определить конфигурацию портов ISA-сервера и все входящие и исходящие подключения компьютера.

Примечание Порты используются в протоколах Transmission Control Protocol (TCP) и User Datagram Protocol (UDP) для именования конечных пунктов логических подключений. Для номеров портов выделен интервал 0–65535, он делится на три диапазона: общеизвестные порты (0-1023), зарегистрированные порты (1024–49151), динамические и/или частные порты (49152–65535). Подробнее о портах — на Web-странице *http://www.isi.edu/in-notes/iana/assignments/port-numbers*.

Кроме списка всех активных подключений, ключ **–a** команды Netstat позволяет получить список всех прослушивающих портов. При указании ключа **–n** преобразование в имена всех адресов и номеров портов не выполняется, что позволяет различить подключения к внешним и внутренним IP-адресам компьютера ISA-сервера и определить открытые порты в любой момент времени по определенному протоколу. Вы можете узнать об активных службах на каждом порту, сравнивая данные, полученные с применением команд netstat -an и **netstat –a**.

Объем информации, возвращаемый командой Netstat **–an**, можно ограничить, указав конкретные протоколы, для чего используются аргументы **–p** TCP или **–p** UDP. Например, команда Netstat **–an** -p TCP возвращает список всех активных TCP-подключений и прослушивающих портов, команда **Netstat –an –p** UDP собирает информацию о состоянии портов только протокола UDP.

Данные о конфигурации портов позволяют исследовать неполадки и конфликты, возникающие при работе портов, и изъяны в защите. Например, когда не удается подключиться к удаленному серверу, утилита netstat поможет обнаружить, что причина неполадки не в локальной сети — просто удаленный компьютер отклоняет попытки подключения. Дополнительным подтверждением является получение сбросов протокола TCP или пакетов о недоступности порта ICMP при попытке подключения.

Наконец, Netstat применяется для обнаружения атак. Например, при выполнении атаки синхронизации (SYN) создается множество полуоткрытых TCP-соединений при попытке заблокировать сервер. В этом случае предоставляется ложный удаленный адрес, причем номера портов в нем последовательны. Эта характерная особенность атаки синхронизации позволяет обнаружить ее в такой информации, возвращаемой Netstat:

```
C:\> netstat -a

C:\>netstat -n -p tcp

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1030         127.0.0.1:1032         ESTABLISHED
  TCP    127.0.0.1:1032         127.0.0.1:1030         ESTABLISHED
  TCP    10.1.1.5:21            192.168.0,1:1025       SYN_RECEIVED
  TCP    10.1.1.5:21            192.168.0.1:1026       SYN_RECEIVED
  TCP    10.1.1.5:21            192.168.0.1:1027       SYN_RECEIVED
  TCP    10.1.1.5:21            192.168.0.1:1028       SYN_RECEIVED
```

```
TCP    10.1.1.5:21      192.168.0.1:1029      SYN_RECEIVED
TCP    10.1.1.5:21      192.168.0.1:1030      SYN_RECEIVED
TCP    10.1.1.5:21      192.168.0.1:1031      SYN_RECEIVED
TCP    10.1.1.5:21      192.168.0.1:1032      SYN_RECEIVED
TCP    10.1.1.5:21      192.168.0.1:1033      SYN_RECEIVED
TCP    10.1.1.5:21      192.168.0.1:1034      SYN_RECEIVED
TCP    10.1.1.5:21      192.168.0.1:1035      SYN_RECEIVED
```

Примечание Подробнее об атаках синхронизации и конфигурировании Windows 2000 для защиты от них — в книге «Windows 2000 TCP/IP Protocols and Services Technical Reference» (Thomas Lee and Joseph Davies, Seattle, Microsoft Press, 2000).

Утилита Telnet

Указав номер порта после команды Telnet, вы определите, принимает ли на нем сервер команды. Например, команда Netstat -an -p TCP позволяет определить, прослушиваются ли входящие запросы на порту 3149. Далее можно узнать, предоставляет ли ISA-сервер доступ по протоколу Telnet, выполнив команду:

```
telnet <внешний_IP-адрес> 3149
```

где *<внешний_IP-адрес>* — внешний IP-адрес ISA-сервера. Если ответа нет или он не сигнализирует об ошибке подключения, внешний пользователь теоретически может использовать назначенные порту службы, вводя команды напрямую. В общем случае это не свидетельствует об изъяне защиты, однако, если протокол Telnet недостаточно защищен, хакер непременно воспользуется этим.

Telnet также применяется для определения активности тех или иных служб. Например, доступность порта 25 ISA-сервера свидетельствует об активности и доступности службы SMTP (Simple Mail Transfer Protocol) внешним пользователям. Существует несколько способов блокировки доступа удаленных пользователей к службе SMTP: отключение службы SMTP, включение фильтрации пакетов ISA-сервера и/или удаления всех существующих фильтров, которые разрешают прохождение входящего трафика через порт 25. Если же вы публикуете сервер и требуется проверить доступ к нему извне, воспользуйтесь командой Telnet для проверки состояния порта. Например, публикуя Web-сервер на порту 9999 ISA-сервера, для проверки возможности подключения к данному порту воспользуйтесь командой telnet *<внешний_IP-адрес>*.

Компонент Network Monitor

Network Monitor (Сетевой монитор), или Netmon, применяется для перехвата и отображения содержимого кадров, поступающих на компьютер с локальной сети. Для облегчения процедуры анализа сетевого трафика Network Monitor предоставляет подробные сведения и отображает сведения о работе 40 наиболее популярных сетевых протоколов. Другими словами, Network Monitor отображает практически всю информацию, относящуюся к сетевым сессиям, в том числе порты источника и приемника, адреса, ответы сервера, полезную нагрузку трафика.

Вот пример содержимого кадра, перехваченного средствами Network Monitor

```
Network Monitor trace  Wed 03/07/2001 08:55:17 AM  Captur 1.txt

+ Frame: Base frame properties
+ ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
```

```
+ IP; ID = 0xAD6; Proto = TCP; Len: 327
+ TCP: .AP..., len: 287, seq:3184161250-3184161537, ack:4040781620,
win;17520, src: 1225 dst: 80
+ HTTP: GET Request (from client using port 1225)
```

Для каждого кадра отображаются сведения об инкапсулированных протоколах, которые перечислены, начиная с внешней оболочки кадра или, с точки зрения сетевых технологий, — с самого низкого сетевого уровня. Щелкнув значок «+» в начале строки, вы получите более подробную информацию, относящуюся к данному протоколу. Первая строка с названием Frame добавлена сетевым монитором для представления общих сведений о перехваченном кадре. Следующая строка содержит данные о протоколе канального уровня, по которому кадр пересылается через сеть (в данном случае Ethernet). Этот протокол представляет собой самый низкий уровень кадра, соответствующий уровню 2 модели OSI. Далее следует протокол сетевого уровня, или уровня 3; в данном случае это протокол IP. Следующий — протокол транспортного уровня, или уровня 4; в данном кадре это протокол TCP. Протокол HTTP — это протокол самого высокого уровня в данном кадре.

Каждый уровень содержит сведения, относящиеся к текущему подключению или передаче. Например, в строке TCP параметры src и dst указывают на порты источника и приемника TCP-подключения, соответствующего кадру или пакету. В данном пакете источником является порт 1225, а приемником — TCP-порт 80, Строки протоколов TCP или UDP захваченного сетевым монитором кадра практически всегда позволяют определить источник и приемник трафика в сети. Эта возможность чрезвычайно важна для настройки и мониторинга брандмауэров.

Трассировка сетевой активности позволяет анализировать трафик и определять причины неполадок в сети. Допустим, что пользователи жалуются на задержки при входе в систему через VPN-подключение. Сетевой монитор позволил выявить, что во время входа в систему присутствует трафик обоих протоколов — L2TP и PPTP. Это означает, что средствами мастера Local ISA VPN для подключения к удаленной сети сконфигурирован протокол L2TP, а при его недоступности применяется PPTP. Если на удаленном VPN сервере протокол L2TP недоступен, пользователи испытывают задержку при попытке подключения по обоим протоколам. Сетевой монитор позволяет выявить нерабочее L2TP-подключение. Настройка ISA-сервера на подключение к удаленному VPN-серверу только по PPTP позволит устранить задержки при входе в систему.

Сетевой монитор помогает выявить протоколы, которые не используются, однако замедляют работу сети. Например, при подключении к частным ЛВС, в которых не применяется технология VPN, туннельный протокол PPTP не нужен.

Таблицы маршрутизации

Все компьютеры, поддерживающие сетевой протокол TCP/IP, хранят таблицу маршрутизации. Путь IP-пакета определяется таблицей маршрутизации компьютера, отправляющего сетевой пакет.

Для просмотра и изменения таблицы маршрутизации применяется утилита командной строки Route. Для просмотра таблицы маршрутизации локального компьютера выполните в командной строке команду route print (рис. 10-2).

Рис. 10-2. Данные таблицы маршрутизации, возвращенные утилитой route

Процесс определения маршрута

При определении маршрута пересылки IP-пакетов в протоколе IP используется таблица маршрутизации.

1. Для каждого маршрута в таблице протокол применяет к IP-адресу назначения и номеру подсети побитовую логическую операцию «И» (колонка **Netmask** на рис. 10-2), чтобы выяснить тип сети — локальная или удаленная. Протокол IP сравнивает результат с адресом назначения, пытаясь найти нужный маршрут. Когда он найден, протокол отмечает маршрут как соответствующий IP-адресу назначения.
2. Из списка найденных маршрутов выбирается маршрут с наибольшим числом совпадающих бит в маске сети. Этот процесс называется нахождением самого длинного, или ближайшего совпадающего, маршрута.
3. **Обнаружив несколько** совпадающих **маршрутов, IP использует маршрут с самой низкой метрикой.**
4. **При обнаружении** нескольких **совпадающих** маршрутов **с одинаково низкой метрикой** случайным **образом выбирается один из них.**

Конечным результатом процесса определения маршрута является выбор одного маршрута из таблицы маршрутизации. Если маршрут найти не удается, протокол IP объявляет ошибку маршрутизации.

Устранение неполадок в таблицах маршрутизации

Утилиты Ping и Tracert позволяют определить недоступные сегменты сети. При установке ISA-сервера в сложной сети утилита Route используется для изменения таблиц маршрутизации и конфигурирования корректных маршрутов во всех сегментах сети. Например, если у ISA-сервера нет интерфейса с удаленной подсетью, для пересылки трафика в эту подсеть необходимо создать соответствующий статический маршрут. (Статическими называются маршруты, которые не создаются в таблице маршрутизации автоматически.)

Вот пример добавления статического маршрута средствами утилиты Route:

```
route add 172.16.41.0 mask 255.255.255.0 172.16.40.1 metric 2
```

В этом примере команда **Route add** указывает, что пакеты, направляемые в подсеть 172.16.41.0 с маской 255.255.255.0, следует пересылать на шлюз 172.16.40.1. Значение метрики равно 2, так как удаленность подсети составляет два перехода. (Обычно метрика рав-

на числу переходов, или количеству пройденных к цели маршрутизаторов.) В этом случае иногда требуется определить статический маршрут к нижестоящим маршрутизаторам, чтобы указать пакетам обратный путь к полсети 172.16.40.0/24.

Так как таблица маршрутизации автоматически создается заново при каждом перезапуске компьютера, для сохранения статических маршрутов в таблице маршрутизации необходимо добавить в таблицу постоянные записи. Командой **Route add –p их можно** автоматически добавить в таблицу маршр>тизации при каждом ее построении.

Статические маршруты также создаются средствами консоли Routing and Remote Access (Маршрутизация и удаленный доступ) в Windows 2000. Статические маршруты, созданные средствами консоли Routing and Remote Access, считаются постоянными.

► **Создание статического маршрута средствами оснастки Routing and Remote Access**

1. В меню **Start** (Пуск) последовательно выберите **Programs** (Программы), **Administrative Tools** (Администрирование) и щелкните **Routing And Remote** Access (Маршрутизация и удаленный доступ).
2. Двойным щелчком раскройте объект **IP Routing** (IP-маршрутизация).
3. Щелкните правой **кнопкой Static Routes** (Статические маршруты) и в контекстном меню выберите команду New **Static Route** (Новый статический маршрут). Откроется диалоговое окно **Static Route** (Статический маршрут).
4. Заполните поля окна статического маршрута и щелкните кнопку **OK.**

Практикум. Определение состояния портов

Вы воспользуетесь командами Netstat и Telnet для определения состояния портов ISA-сервера. Этот способ применяется для проверки защиты, а также для определения доступности с внешних узлов службы, работающей на ISA-сервере.

Задание. Определение состояния портов ISA-сервера

Сейчас вы средствами утилиты командной строки Netstat найдете открытые порты на внешнем интерфейсе ISA-сервера, а затем подключитесь к ним по протоколу Telnet.

► **Проверка состояния портов ISA-сервера**

1. Войдите в систему Server1 под учетной записью Administrator (Администратор).
2. В меню **Start** (Пуск) выберите команду **Run** (Выполнить).
3. В текстовом окне **Open** (Выполнить) диалогового окна **Run** введите команду and и щелкните кнопку **OK.** Откроется окно командной строки.
4. В командной строке введите команду **netstat –an –p tcp.**

   В окне отобразится список всех активных TCP-портов ISA-сервера. В окне вывода в левой колонке IP-адресов с номерами портов указаны локальные адреса, а в правой — внешние адреса активных подключений. Большинству локальных адресов соответствует внутренний интерфейс 192.168.0.1. Однако в конце списка, возможно, есть несколько подключений, локальный адрес которых является внешним IP-адресом ISA-сервера.
5. Сколько активных подключений указано для внешнего интерфейса ISA-сервера в колонке Local Address? Посмотрите на внешние адреса подключений: действительно ли они внешние, или лишь представляют другой порт локального адреса? Какие порты этих внешних адресов используются для отправки информации на локальные адреса ISA-сервера.

   Запишите свои ответы здесь:

6. Откройте Microsoft Internet Explorer на компьютере с ISA-сервером и подключитесь к внешнему Web-узлу, например к *www.microsoft.cont.*
7. Во время загрузки Web-страницы в Internet Explorer переключитесь в окно командной строки и снова выполните команду **netstat –an –p tcp. В** окне отобразится список всех активных TCP-портов ISA-сервера.
8. Взгляните в конец списка вывода. Сколько дополнительных активных подключений (по сравнению с данными, полученными в результате выполнения пункта 5) появилось на внешнем интерфейсе ISA-сервера в колонке Local Address? Есть ли новые активные порты на внешних адресах? После просмотра данных скажите, какой внешний порт используется для отправки Web-данных на локальный внешний IP-адрес?

   Запишите свои ответы здесь:

9. На какие локальные порты внешнего интерфейса ISA-сервера отправляются Web-данные? Эти динамические порты обычно изменяются от подключения к подключению. Укажите номера этих портов.

Предположим, у вас есть доказательства несанкционированного проникновения в сеть и требуется проверить защиту путем тестирования состояния внешних портов, через которые хакеры могли бы получить доступ к сети. Для этого подключитесь средствами Telnet к внешним портам и проверьте, откликаются ли службы на этих портах. (Обычно эту операцию выполняют с внешнего компьютера.)

10. Подключитесь средствами Telnet к одному из определенных на шаге 9 внешних портов следующим образом. В командной строке выполните команду **telnet** *<внешний_IP-адрес>* *<номер порта>* (например **telnet 64.43.113.110 10123),** где *<внешний_IP-адрес>* – это назначенный ISA-серверу внешний IP-адрес, а *<номер порта>* — один из определенных в пункте 9 локальных портов.

    Появится сообщение об ошибке подключения к порту. Порт не прослушивается. Если порт принимает внешние подключения, операция пройдет без ошибки, и в окне отобразится пустая строка или сообщение о работающей на указанном порте службе.

П. Средствами Telnet попытайтесь подключиться к каждому из перечисленных в левой колонке приведенной ниже таблицы портов. Например, чтобы подключится к порту 25 IP-адреса 64,43.113.110, выполняется команда **telnet 64.43.113.110** 25. Отметьте состояние (**Открыт** или **Закрыт)** портов в правой колонке таблицы.

Номер порта	Состояние порта
25	
7	
389	
443	
21	
8080	
1030	

Отрытое состояние порта в общем случае не говорит о слабой защите, но некоторые порты по соображениям безопасности лучше не оставлять статически открытыми, в частности порты 15 (Net-stat), 21 (FTP), 23 (Telnet), 25 (SMTP), 79 (Finger) и 80 (HTTP).

12. Закройте окно командной строки.

Резюме

ISA-сервер поставляется со многими утилитами устранения неполадок. Для первичной диагностики используются отчеты ISA-сервера, которые помогают выявлять причины низкой производительности. В Event Viewer (Просмотр событий) вы найдете все сообщения о событиях служб ISA-сервера. Оснастка Performance Monitor применяется для устранения неполадок, связанных с конфигурацией и работой сети, а также оборудования. Утилита командной строки Netstat позволяет получить информацию обо всех активных TCP- и/или UDP-подключениях и используется для выявления неполадок подключений и подсистемы безопасности. Средствами Telnet определяют доступность конкретных портов сервера. Network Monitor (Сетевой монитор) применяется для перехвата и отображения содержимого кадров, поступающих на компьютер с локальной сети. И, наконец, команда Route необходима для проверки и настройки таблиц маршрутизации, а также обеспечения корректности маршрутов во всех сегментах сети.

Занятие 2. Методики выявления неполадок в работе ISA-сервера

Чтобы успешно выявлять и устранять неполадки, нужно соблюдать определенную последовательность действий. После выявления необычного поведения ISA-сервера прежде всего следует определить, на каком уровне происходит сбой — на уровне пользователя или пакетов. В этом занятии обсуждаются методики устранения неполадок обоих типов.

Изучив материал этого занятия, вы сможете:

- ✓ устранять неполадки пользовательского доступа;
- ✓ устранять неполадки на уровне пакетов;
- ✓ устранять неполадки VPN-подключений на ISA-сервере.

Продолжительность занятия — около 30 минут.

Устранение неполадок пользовательского доступа

Если доступ для определенной учетной записи пользователя нестабилен или невозможен, вероятно, причина в излишне строгих мерах безопасности, неправильно сконфигурированных правилах или неверном методе аутентификации. Утилиты Ping и Tracert работают корректно даже в таких условиях.

Для устранения ошибки пользовательского уровня в первую очередь необходимо проверить правила политики доступа. Необходимо убедиться, что в соответствии с правилами политики доступа пользователям, которые испытывают трудности при создании сетевого подключения, предоставлены необходимые права доступа на подключение к нужным узлам, на работу с нужными группами содержимого и по соответствующих протоколами.

Если настроенные вами правила не позволяют корректно управлять пользовательскими сеансами, необходимо удостовериться в правильности настройки массива для запроса идентификационных реквизитов у пользователей, не проходящих аутентификацию. Имейте в виду, что после создания разрешающих правил политики доступа для определенного пользователя или группы ISA-сервер принудительно выполняет аутентификацию пользовательских сеансов. С другой стороны, если вы хотите оставить все Web-сеансы анонимными, но анонимный доступ невозможен, проверьте, не сконфигурирован ли массив на принудительную аутентификацию анонимных пользователей. Удалите все правила протоколов, Web-узлов и содержимого, применяемые к конкретным группам или пользователям Windows 2000,

Аутентификация

Выбор метода аутентификации для массива ISA-сервера влияет на способность подключения пользователей. Различные методы аутентификации годятся для разных сетевых окружений. Если для данной сетевой конфигурации выбран несовместимый метод аутентификации или он неправильно настроен, пользователю не удастся получить доступ к ISA-серверу и сети.

Например, режимом аутентификации по умолчанию является стандартная проверка подлинности Windows (Integrated Windows), но в этом режиме не поддерживается идентификация клиентов под управлением операционных систем, отличных от Windows. Чтобы обеспечить доступ таких клиентов к ISA-серверу, необходимо настроить массив для использования другого, совместимого метода аутентификации. Браузер Netscape не поддер-

живает работу с реквизитами пользователя в формате NTLM, поэтому при его применении не следует устанавливать режим идентификации Integrated Windows. Этот режим работает либо по протоколу Kerberos V5, либо по собственному протоколу типа «запрос — ответ», что также налагает дополнительные ограничения. Однако в схеме сквозной аутентификации (рис. 10-3) ISA-сервер не поддерживает аутентификацию по протоколу Kerberos V5, так как Kerberos V5 требует, чтобы клиент мог идентифицировать сервер, выполняющий проверку подлинности.

Рис. 10-3. Сквозная аутентификация не совместима с аутентификацией по протоколу Kerberos V5

ISA-сервер поддерживает и другие методы аутентификации — базовый (Basic), на основе хеша (Digest) и клиентских сертификатов (Client Certificate). Базовая аутентификация совместима с клиентами всех типов. Однако она предусматривает передачу по сети имени пользователя и пароля в открытом, незашифрованном виде, поэтому сама по себе она не обеспечивает должной безопасности. Аутентификация на основе хеша поддерживается только в доменах Windows 2000, пароли пересылаются по открытым сетям, но в зашифрованном виде. При аутентификации на основании клиентских сертификатов используется протокол SSL, и необходимо наличие предустановленного сертификата клиента в хранилище Web-прокси на ISA-сервере, кроме того, сертификат следует сопоставить соответствующей учетной записи пользователя. ISA-сервер представляет клиентские сертификаты только в конфигурации *SSL-сопряжения* (SSL bridging).

Устранение неполадок пакетного уровня

Когда сеть недоступна ни одному из пользователей или утилиты Ping и Tracert не работают, вероятнее всего причина неполадки — на уровне пакетов.

В процессе устранения неполадок пакетного уровня ISA-сервера прежде всего максимально упростите конфигурацию сети.

► **Упрощение конфигурации для устранения неполадок сети**

1. Включите фильтрацию пакетов (если это уже не сделано) и создайте специальный фильтр пакетов, разрешающий трафик любых IP-протоколов в обе стороны.
2. Создайте правило протокола, разрешающее прохождение любых запросов по протоколу IP. Позаботьтесь, чтобы правила узлов и содержания разрешали доступ ко всем узлам и группам содержания.
3. Верните в исходное состояние (по умолчанию) параметры всех фильтров приложений и правил маршрутизации.
4. Проверьте корректность определения в таблице локальных адресов (LAT) всех внутренних клиентов ISA-сервера.

5. Разрешите IP-маршрутизацию (установите флажок **Enable IP routing)** в диалоговом окне свойств фильтрации пакетов **IP Packet Filters Properties.**

Примечание Установка флажка **Enable IP routing** обеспечивает возможность маршрутизации для протоколов с дополнительными подключениями. Этот параметр особенно важен при конфигурировании сетей периметра. IP-маршрутизацию активизируют либо в диалоговом окне свойств фильтрации пакетов **IP Packet Filters Properties** в оснастке ISA Management, либо в оснастке **Routing and Remote** Access (Маршрутизация и удаленный доступ).

---

6. Убедитесь, что на внутреннем интерфейсе ISA-сервера не определен основной шлюз, а основной шлюз внешнего интерфейса определен корректно.
7. Отключите клиент брандмауэра и определите ISA-сервер в качестве основного шлюза на клиентских компьютерах.

Упростив конфигурацию ISA-сервера, перезапустите его службы. Если доступ все равно невозможен, перезагрузите компьютер ISA-сервера. Если и это не помогает — следовательно, неполадка не связана с конфигурацией ISA-сервера. В таком случае необходимо устранять неполадки сети обычным образом: изучать трафик средствами Network Monitor, проверять корректность DNS, таблиц маршрутизации, оповещений, отчетов и журналов.

Если в упрощенной конфигурации Интернет доступен, источник неполадки обычно определяют путем последовательного подключения сетевых элементов. Например, если при наличии доступа в Интернет на определенном компьютере после запуска интернет-приложения возникают ошибки, предполагается, что либо приложение неправильно настроено для использования ISA-сервера в качестве прокси-сервера, либо оно вообще не поддерживает работу с прокси-сервером. Для таких приложений нужно настроить клиент SecureNAT или запустить клиент брандмауэра. После исправления конфигурации клиента снова попытайтесь запустить приложение. Если при включенном обнаружении сервера клиенту брандмауэра не удается получить доступ, следовательно, автоматическое обнаружение настроено неправильно. Последовательно устраняя неполадки по мере их возникновения, добавьте все необходимые в данной конфигурации элементы сети.

VPN-сети

В виртуальных частных сетях устранение неполадок также начинается с упрощения сетевой конфигурации, как описано выше. Если вы уже установили VPN с помощью мастеров, первым делом проверьте, работает ли служба Routing and Remote Access (Маршрутизация и удаленный доступ). Далее позаботьтесь, чтобы клиентский компьютер работал как клиент SecureNAT, а не как клиент брандмауэра.

Также необходимо проверить, корректно ли мастер конфигурировал VPN локального ISA-сервера и создал интерфейс вызова по требованию службы Routing and Remote Access в узле **Routing Interfaces** (Интерфейсы маршрутизации) (рис. 10-4).

После этого выясните, созданы ли два фильтра IP-пакетов для каждого выбранного протокола аутентификации VPN-подключений. Например, при использовании в VPN-подключении протоколов L2TP и PPTP мастер VPN-конфигурации локального ISA-сервера должен создать и активизировать четыре фильтра IP-пакетов. [Для L2TP мастер создает специальные фильтры на портах 500 и 1701, а для PPTP — предопределенные фильтры вызова (PPTP Call) и приема (PPTP Receive).]

Если при правильно созданных интерфейсах и фильтрах IP-пакетов после перезагрузки компьютера нормальная работа невозможна, рекомендуется удалить все созданные мастерами фильтры IP-пакетов, отключить службу **RRAS** и снова выполнить мастер.

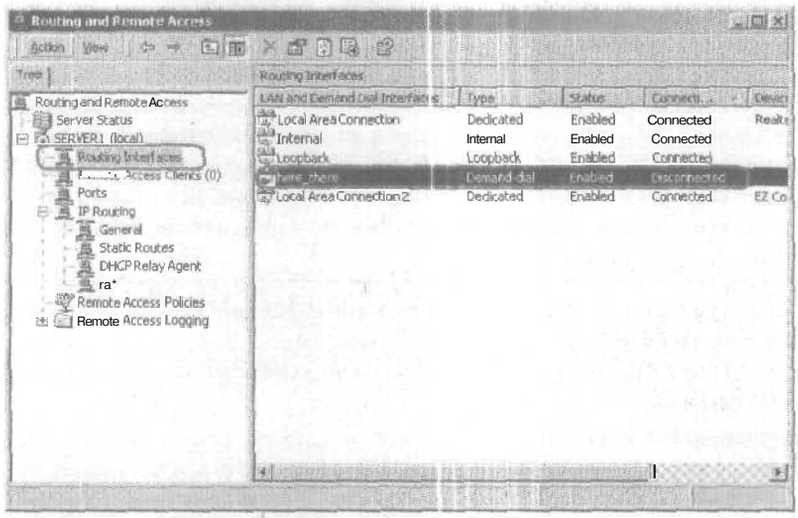


Рис. 10-4. Интерфейс вызова по требованию службы RRAS

Перечень типичных неполадок и способы их устранения

Устраняя неполадки ISA-сервера, воспользуйтесь информацией из приведенных далее таблиц. В них собраны сведения о стандартных неполадках ISA-сервера и предлагаются варианты их устранения.

Таблица 10-1. Устранение неполадок политики доступа

Неполадка	Возможные причины	Решение
Клиентам недоступны внешние Web-узлы	После установки ISA-сервер блокирует весь трафик Интернета в обеих направлениях. Вы вправе создать разрешающие правила, если это не противоречит корпоративной политике безопасности	Создайте правила протоколов, разрешающие определенным пользователям применять протоколы. Далее создайте правила узлов и содержания, предоставляющие пользователям доступ к определенным Web-узлам по протоколам, предусмотренным в правилах протоколов. Проверьте, правильно ли настроен порт прокси на клиентских браузерах. По умолчанию для взаимодействия с ISA-сервером используется порт 8080
При просмотре Web-узлов клиенты получают сообщение об ошибке 502	После установки ISA-сервер блокирует весь трафик Интернета в обоих направлениях. Вы вправе создать разрешающие правила, если это не противоречит корпоративной политике безопасности. Для некоторых правил политики доступа необходима аутентификация; возможно, не настроено прослушивание запросов аутентификации	Создайте правила протоколов, разрешающие определенным пользователям применять протоколы. Далее создайте правила узлов и содержания, предоставляющие пользователям доступ к определенным Web-узлам по протоколам, предусмотренным в правилах протоколов. Выберите метод аутентификации для прослушивания. Клиенты получат доступ согласно сконфигурированным правилам по определенному методу аутентификации

Таблица 10-1. (*окончание*)

Неполадка	Возможные причины	Решение
Клиентам недоступны отдельные протоколы, например HTTP, RealAudio и др.	После установки ISA-сервер блокирует весь трафик Интернета в обоих направлениях. Вы вправе создать разрешающие правила, если это не противоречит корпоративной политике безопасности	Создайте правила протоколов, которые разрешают обмениваться информацией по нужным протоколам. Проверьте, не заблокированы ли эти протоколы фильтрами приложений
После отключения правила протокола, клиенты продолжают работать по протоколу, который данное правило разрешало	При отключении правила протокола существующие клиентские сеансы не закрываются — просто дополнительные сеансы создать не удастся. Например, если клиент в соответствии с правилом использует протокол RealAudio, сеанс будет продолжать работу, невзирая на активизацию правила, запрещающего доступ	Отключите пользовательский сеанс
Клиенты не в состоянии использовать отдельные определения протоколов, хотя создано правило, разрешающее работу по данным протоколам	Если отключить фильтр приложения, весь трафик, связанный с определениями указанных протоколов, блокируется, хотя вроде бы правила протокола трафик разрешают	Включите фильтр приложения

Таблица 10-2. Неполадки аутентификации

Неполадка	Возможные причины	Решение
ISA-сервер не выполняет аутентификацию пользователей Netscape	Возможно, ISA-сервер сконфигурирован только на использование встроенной аутентификации Windows. Браузер Netscape не поддерживает работу с реквизитами пользователя в формате NTLM	Настройте ISA-сервер на применение других методов аутентификации — базового (Basic) или на основе хеша (Digest)

Таблица 10-3. Неполадки кэширования

Неполадка	Возможные причины	Решение
ISA-сервер кэширует не весь трафик	ISA-сервера кэширует лишь данные, которые соответствуют критериям кэширования	Рекомендуется расширить перечень кэшируемых объектов путем корректировки свойств кэширования и правил маршрутизации, разрешив активное кэширование и кэширование динамического содержимого. Для этого увеличьте TTL кэшируемых объектов, а также позвольте возвращать из кэша просроченные объекты
Не запускается служба Web-прокси	Поврежден файл кэша	Служба Web-прокси не запускается, если нарушена целостность файла кэша. Чтобы устранить неполадку, переконфигурируйте выделенные под кэш дисковое пространство

Таблица 10-4. Неполадки при входе в систему

Неполадка	Возможные причины	Решение
В журнале не регистрируется информация о клиенте (имя пользователя)	ISA-сервер не всегда выполняет аутентификацию клиентов- В этом случае клиенты получают анонимный доступ и их данные не регистрируются	Сконфигурируйте ISA-сервер на принудительную аутентификацию клиентов службой Web-прокси, настроив соответствующим образом свойства входящих и исходящих Web-запросов

Таблица 10-5. Неполадки публикации серверов

Неполадка	Возможные причины	Решение
При обращении к опубликованному Web-серверу клиенты получают сообщение об ошибке 403	Для некоторых правил политики доступа необходима аутентификация; возможно, не настроено прослушивание запросов аутентификации	Выберите метод аутентификации для прослушивания. Клиенты получат доступ согласно сконфигурированным правилам по определенному методу аутентификации
	Имеет место конфликт портов между правилом публикации серверов и файлом конфигурации клиента брандмауэра	В среде Microsoft Proxy Server 2.0 почтовый сервер рекомендуется публиковать как клиент Winsock-прокси. В этом случае на почтовом сервере создается файл Wspclnt.ini. При использовании ISA-сервера опубликованные серверы не нуждаются в специальной конфигурации, так как публикуются как клиенты SecureNAT. Удалите с опубликованного сервера файл Wspclnt.ini. Затем в оснастке ISA Management выполните мастер Mail Server Security

Таблица 10-5. *(окончание)*

Неполадка	Возможные причины	Решение
	Microsoft Exchange Server не в состоянии создать привязку к SMTP-порту ISA-сервера	Проверьте, нет ли другой службы или приложения, создающего привязку к порту *25* до сервера Exchange
	Microsoft Exchange Server теряет связь с ISA-сервером	Если связь между ISA-сервером и Exchange Server временно нарушена, необходимо перезапустить службы Exchange Server для восстановления привязки к портами ISA-сервера
Внешние пользователи не в состоянии отправлять почту на Microsoft Exchange Server, который работает как клиент Secure-NAT в сети, защищенной ISA-сервером	Неправильно сконфигурированы правила публикации сервера	Проверьте, настроены ли правила публикации серверов на пересылку всего SMTP-трафика внешнего интерфейса на порт *25,* а POP3-трафика — на порт 110 по правильному IP-адресу и порту внутреннего Exchange

Таблица 10-6. Устранение неполадок служб

Неполадка	Возможные причины	Решение
После успешной установки службы не запускаются	ISA-сервер не запускается, если неправильно сконфигурирована LAT, то есть когда она не содержит внутреннего сетевого адаптера, взаимодействующего со службой Active Directory	Чтобы добавить необходимые пункты в LAT, выполните следующие операции: • остановите службы ISA-сервера и фильтрацию пакетов. Для этого выполните в командной строке команду net stop **mspfltext**; • правильно настройте LAT. Так как запустить оснастку ISA Management нельзя, настройку LAT выполните средствами COM-объектов ISA Server Administration. Подробнее о создании LAT — в главе «Constructing the Local Address Table» комплекта ресурсов «ISA Server Software Development Kit»; • перезагрузите компьютер

Резюме

При устранении неполадок доступа на ISA-сервере прежде всего следует определить, на каком уровне происходит сбой — на уровне пользователей или пакетов. Неполадки на пользовательском уровне проявляются в том, что сетевое окружение ведет себя неодинаково по отношению к разным пользователям. При неполадках на уровне пользователей сохраняется доступ к сети утилит Ping или Tracert, но не для всех пользовательских учетных записей. При сбоях на уровне пакетов неполадки проявляются одинаково для всех пользователей, а сеть недоступна утилитам Ping или Tracert.

Для устранения неполадок пользовательского уровня необходимо проверить правила политики доступа и корректность настройки доступа разных пользователей к выделенным им ресурсам, группам содержания и протоколам. Кроме того, при настройке правил политики доступа конкретных пользователей и групп к Web-сеансам необходимо позаботиться о конфигурировании свойств массива на аутентификацию исходящих Web-запросов. Наконец, надо проверить правильность настройки метода аутентификации в массиве.

Устранение неполадок на уровне пакетов начинается с максимально возможного упрощения сетевой конфигурации и последующей проверки возможности доступа. Если упрощением сетевой конфигурации неполадку устранить не удается, следовательно, она не связана с конфигурацией ISA-сервера. В таком случае неполадки сети устраняют другими методами. Если в упрощенной конфигурации доступ в Интернет возможен, то источник неполадки определяют путем последовательного подключения сетевых элементов. При устранении неполадок VPN-подключений проверяют конфигурацию VPN-клиентов как клиентов SecureNAT, наличие и работоспособность службы Routing and Remote Access (Маршрутизация и удаленный доступ), правильность создания интерфейса вызова по требованию для VPN, а также наличие и работоспособность двух фильтров IP-пакетов для каждого протокола VPN-подключения.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Ответы для самопроверки — в приложении А «Вопросы и ответы» в конце книги.

1. ISA-сервер установлен в сети периметра (DMZ). Адресное пространство в защищенной ISA-сервером сети состоит из подсети 192.168.0.0/24, а сеть периметра перед ISA-сервером сконфигурирована как подсеть 192.168.1.0/24. Внутренний адрес ISA-сервера - 192.168.0.1, а внешний — 192.168.1.99. Адрес внешнего шлюза — 192.168.1.1. Ни с одного из клиентских компьютеров, расположенных за ISA-сервером, нет доступа в Интернет. При выполнении команды Route print на ISA-сервере получена информация, показанная на рис. 10-5. Где допущена ошибка в таблице маршрутизации? Как исправить неполадку с помошью команды Route.

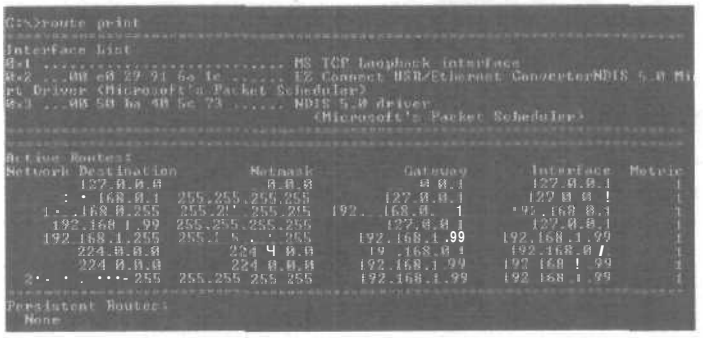


Рис. 10-5. Таблица маршрутизации (к вопросу 1)

2. После перезагрузки сервера, описанного в вопросе 1, неполадка осталась. Как избежать изменений в таблице маршрутизации после каждой перезагрузки?

3. Какая утилита применяется для выявления атаки синхронизации (SYN)? Опишите характерный признак такой атаки?

4. Зачем применяют утилиту Telnet при проверке конкретных TCP- иди UDP-портов?

5. Вы запустили мастер VPN Configuration и в качестве протокола аутентификации указали L2TP. Сколько фильтров пакетов должен создать мастер? Какие порты статически откроют эти фильтры?

Приложение А

Вопросы и ответы

Глава 1

Закрепление материала

1. Какой протокол позволяет браузерам автоматически подключаться к ISA-серверу?
   Протокол Web Proxy Autodiscovery Protocol (WPAD).
2. Какие функции выполняет фильтр редиректора HTTP?
   Фильтры редиректора HTTP пересылают HTTP-запросы от клиентов брандмауэра и клиентов SecureNAT в службу Web-прокси. Это обеспечивает автоматическое («прозрачное») кэширование для клиентов, браузеры которых не сконфигурированы для перенаправления в службу Web-прокси.
3. Как и когда в конфигурации ISA-сервер применяется служба каталогов Active Directory?
   Информация обо всех пользователях, правилах и о конфигурации обычно централизованно хранятся и управляются в службе каталогов Active Directory. В версии Enterprise Edition ISA-сервера служба каталогов Active Directory обеспечивает в организациях совместное использование схемы, создание кэширующих массивов и автоматическое применение на всем предприятии конфигурации, политик доступа и публикации, а также управление конфигурациями.
4. Каковы преимущества протокола CARP по сравнению с протоколом ICP?
   Прежде всего, ICP-массивы характеризуются «отрицательной масштабируемостью», то есть по мере роста числа серверов растет количество запросов, необходимых для определения их местоположения. В протоколе CARP обмен сообщениями не нужен, так как в нем путь при разрешении запроса определяется автоматически, что устраняет обмен сообщениями между серверами. Кроме того, в ICP-массивах возможно дублирование информации в кэше, получаемой с наиболее популярных URL-адресов. Основанная на хеше маршрутизация в протоколе CARP предотвращает такое дублирование и поддерживает единый логический кэш, распределенный между всеми серверами — членами массива.
5. Зачем применяются многоуровневые политики в версии Enterprise Edition ISA-сервера?
   Одновременное использование политик предприятия и массива позволяет обеспечить единство политики во всей организации и при этом предоставить администраторам отдельных подразделений или филиалов право определять свои политики в соответствии с локальными требованиями, создавая дополнительные правила.

6. Какая возможность в Windows 2000 Advanced Server или Windows 2000 Datacenter Server позволяет повысить производительность массива ISA-серверов версии Enterprise Edition?

   В версии Enterprise Edition ISA-сервера для обеспечения отказоустойчивости, высокой доступности, эффективности и повышенной производительности создаются кластеры из нескольких ISA-серверов под управлением службы балансировки сетевой нагрузки (Network Load Balancing, NLB) операционной системы Microsoft Windows 2000 Advanced Server.

Глава 2

Закрепление материала

1. Какую аппаратную конфигурацию (частоту процессора, объем оперативной и дисковой памяти) вы порекомендуете для компьютера, где предполагается установить ISA-сервер, который будет работать в смешанном режиме, обрабатывать 500—900 запросов в секунду и обслуживать менее 2000 пользователей?

   Процессор Pentium III 550 МГц, 256 Мбайт оперативной памяти, 10 Гбайт свободного пространства на жестком диске.

2. Каковы требования к установке ISA-сервера в массив?

   Компьютер ISA-сервер должен быть членом домена Windows 2000, и перед установкой следует выполнить процедуру инициализации предприятия.

3. Каковы преимущества сети периметра?

   Она позволяет предоставлять внешним клиентам доступ к опубликованным серверам внутренней сети, не открывая доступ к самой внутренней сети.

4. Что следует предпринять для совмещения на одном компьютере ISA-сервера и Web-сервера?

   Так же как Web-сервер, ISA-сервер ожидает входящие запросы на порту 80. Чтобы избежать конфликта, Web-сервер обычно конфигурируют для прослушивания другого порта. Далее соответствующее правило Web-публикации ISA-сервера перенастраивают на пересылку Web-запросов на соответствующий порт Web-сервера. Другой способ заключается в настройке сервера IIS (Internet Information Services) для прослушивания другого IP-адреса. Например, настройка IIS на прослушивание адреса 127.0.0.1 заставит его принимать запросы только от ISA-сервера.

5. Каково назначение таблицы LAT?

   Таблица локальных адресов (LAT) применяется на ISA-сервере для определения адаптера, который используется для доступа во внутреннюю сеть.

6. Что следует предпринять, чтобы после перехода от Proxy Server к ISA-серверу браузеры клиентов кэширующего сервера подключались к ISA-серверу?

   Существует два способа решения поставленной задачи. Во-первых, можно сконфигурировать все подчиненные члены цепочки (или браузеры) для подключения к порту 8080 на ISA-сервере. Второй способ заключается в конфигурировании ISA-сервера для прослушивания порта 80. Эту операцию необходимо выполнить, так как Proxy 2.0 ожидает клиентские HTTP-запросы на порту 80, а вновь установленный ISA-сервер прослушивает порт 8080.

Глава 3

Закрепление материала

1. Вы устанавливаете ISA-сервер и настраиваете его службы брандмауэра и Web-кэширования в двух филиалах компании. Требуется изучить потребности пользователей и дать рекомендации по настройке клиентских компьютеров. В каждом из филиалов работает по 20 сотрудников, кроме того, в штате предусмотрены 10 специалистов по обслуживанию, которые курсируют между филиалами и подключают свои портативные компьютеры к любому доступному порту Ethernet. Расположение офисных компьютеров в филиалах более или менее постоянное, и нет необходимости определять для них особые правила доступа. Требуется добиться максимальной эффективности установки и последующего сопровождения ISA-сервера. Какие компьютеры вы порекомендуете сконфигурировать как клиенты брандмауэра (если таковые вообще нужны), а какие — как клиенты SecureNAT?

   Так как офисные компьютеры установлены стационарно, а правила доступа на них конфигурируются для машины, а не для конкретных пользовательских учетных записей, такие компьютеры следует настроить как клиенты SecureNAT — таким образом максимально упростится установка и обслуживание. С другой стороны, портативные компьютеры следует конфигурировать как клиенты брандмауэра, тогда на них будет работать функция автоматического обнаружения сервера — ее поддерживают лишь клиенты брандмауэра.

2. **Чем отличаются файлы Mspclnt.ini и Wspcfg.ini на компьютерах — клиентах брандмауэра?**

   Оба файла содержат параметры конфигурации клиентов Winsock, однако при обработке запросов Winsock клиент брандмауэра отдает приоритет файлу Wspcfg.ini. Файл Wspcfg.ini, хранящийся в папке соответствующего Winsock-приложения, содержит параметры конфигурации конкретного клиента. Если файл Wspcfg.ini найти не удается, или если в нем нет никаких параметров, клиент брандмауэра пытается найти сведения о конфигурации в файле Mspclnt.ini, который расположен в установочной папке клиента брандмауэра. В этом файле хранятся стандартные параметры Winsock, не учитывающие особенности того или иного приложения.

3. Какие действия выполняются в процессе обслуживания запроса клиента при активном механизме автоматического обнаружения?

   Сначала клиент обращается к серверу DNS (Domain Name System) или DHCP (Dynamic Host Configuration Protocol), где должна храниться запись WPAD, указывающая на сервер Web-прокси с поддержкой автоматического обнаружения (Web Proxy Autodiscovery, WPAD), который подскажет местоположение ISA-сервера. Далее клиентские запросы выполняются ISA-сервером, как описано в WPAD-записи на сервере DNS или DHCP.

4. Можно ли путем настройки записей подключений ISA-сервера по телефонной линии обеспечить совместное использование клиентами Web-прокси безопасного подключения к Интернету по телефонной линии?

   Нет. Клиенты Web-прокси могут совместно использовать безопасное подключение по телефонной линии при отсутствии на ISA-сервере записи подключения по телефонной линии. Конфигурирование записи подключения по телефонной линии позволяет клиентам SecureNAT совместно использовать безопасное подключение через модем.

5. Ваша организация недавно перешла с выделенного подключения к Интернету на подключение по телефонной линии. При этом вы отключили внешний сетевой адаптер и настроили запись подключения по телефонной линии на существующее подключение по телефонной линии. Однако когда ISA-сервер дозванивается до провайдера через это подключение, никто из клиентов не в состоянии установить связь с Интернетом. Что вы порекомендуете предпринять в первую очередь для устранения этой неполадки?

   После каждого включения или отключения сетевого адаптера и до восстановления связи с клиентами ISA-сервера необходимо перезапустить службы брандмауэра и Web-прокси.

Глава 4

Закрепление материала

1. В каких из перечисленных далее условиях пользователь John получит доступ в Интернет через ISA-сервер? Предполагается, что существует только разрешающее (Allow) правило узлов и содержимого по умолчанию.

   • Вы создали правило протоколов, разрешающее доступ любому IP-трафику по любым запросам, а затем — еще одно правило протоколов, запрещающее пользователю John доступ к любому IP-трафику. Свойства исходящих Web-запросов массива по умолчанию не изменялись. Получит ли John доступ в Интернет через Web-браузер с клиента SecureNAT?

   John получит доступ в Интернет со своего Web-браузера. Так как заданные по умолчанию свойства массива для исходящих Web-запросов не изменились и не требуют идентификации пользователей, а также потому, что не сконфигурировано разрешающее правило, требующее аутентификации, Web-сеанс пользователя John останется анонимным, и запрещающее правило его не затронет.

   • Вы создали правило протоколов, разрешающее доступ к любому IP-трафику всем членам группы Domain Users (Пользователи домена). John является членом группы Domain Guests (Гости домена), но не входит в группу Domain Users. Свойства исходящих Web-запросов массива умолчанию не изменялись. Получит ли John доступ в Интернет через Web-браузер с клиента SecureNAT?

   John не получит доступ в Интернет из своего Web-браузера. Создано разрешающее правило протокола для группы Domain Users, которое требует от всех клиентов Web-прокси проходить аутентификацию. John не является членом этой группы и, следовательно, не получит доступа в Web.

   • Вы создали правило протоколов, разрешающее доступ любому IP-трафику по любым запросам, а затем — еще одно правило протоколов, запрещающее доступ к любому IP-трафику членам группы Domain Guests. John входит только в группу Domain Guests. Свойства исходящих Web-запросов массива изменены: требуется идентификация пользователей, не прошедших аутентификацию. Получит ли John доступ в Интернет через Web-браузер с клиента брандмауэра?

   John не получит доступ в Интернет, так как анонимный доступ заблокирован. Его сеанс должен проходить проверку подлинности службой Web-прокси, и так как он является членом группы Domain Guests, то доступ не получит.

   • Вы создали правило протоколов, разрешающие доступ к любому IP-трафику членам группы Domain Users. John входит в группу Domain Users. Сможет ли он установить подключение к Интернету по протоколу FTP из командной строки с компьютера, на котором нет ПО клиента брандмауэра?

   John не получит доступ в Интернет со своего FTP-клиента, так как его компьютер не сконфигурирован как клиент брандмауэра. Только клиентам брандмауэра разрешается пересы-

лать на ISA-сервер реквизиты учетной записи для не связанных с Web запросов. John не сможет пройти аутентификацию, и его запрос отклонят.

2. Какие защитные меры следует предпринять, если обнаружена атака «IP half scan» с определенного сетевого адреса?

   Рекомендуется создать правило узлов н содержимого или фильтр IP-пакетов, которые блокируют весь трафик для диапазона IP-адресов, откуда выполняется атака.

3. В каких трех ситуациях для разрешения доступа в Интернет нужно создавать фильтры IP-пакетов вместо правил протоколов и правил узлов и содержимого?

   Фильтры IP-пакетов следует создавать при публикации серверов, расположенных в сети периметра (DMZ), когда на компьютере ISA-сервера выполняются приложения или другие службы, которым необходим доступ в Интернет, а также когда требуется предоставить доступ к протоколам, которые не базируются на протоколах UDP или TCP.

4. Вы создали правило узлов и содержимого, запрещающее доступ к двум адресатам: *ftp://movies.acme.com/clips* и *ftp://radio.acme.com*. Пользователи имеют разрешения на загрузку файлов с FTP-узлов. Смогут ли они загрузить средствами FTP-клиента содержимое с узла *ftp://movies.acme.com?* Смогут ли они загрузить содержимое с папки *ftp://radio.acme.com/songs?*

   Пользователи получат доступ к *ftp://movies.acme.com* потому что правило запрещает доступ лишь к подпапке. Однако они не получат доступ к *ftp://radio.acme.com/songs* потому что доступ к этой подпапке неявно запрещен правилом, запрещающим доступ к *//radio.acme.com*.

5. Вы хотите запретить группе пользователей Windows 2000 загрузку любых аудиоданных с 10 до 16 часов по будним дням. Сколько потребуется создать элементов политики?

   Достаточно создать один элемент политики — расписание для периода времени между 10 и 16 часами. Звуковое информационное наполнение является предопределенным элементом групповой политики содержания, а пользователи и группы Windows 2000 конфигурируются в домене, а не на ISA-сервере. После создания расписания достаточно сформировать правило узлов и содержимого, которое запретит доступ группы к аудиоданным с любых адресатов в течение заданного периода времени.

Глава 5

Закрепление материала

1. Клиент Web-прокси запрашивает Web-объект, и ISA-сервер ищет копию этого объекта в своем кэше и обнаруживает, что копия просрочена. Согласно правилу маршрутизации, ISA-сервер обращается за объектом к узлу в Интернете, который оказывается недоступным. Каковы дальнейшие действия ISA-сервера?

   ISA-сервер выясняет, разрешает ли конфигурация возвращать из кэша просроченные копии объектов. Этот параметр определяется на вкладке Advanced диалогового окна страницы свойств Cache Configuration Properties. Если выбран переключатель Return the expired object only if expiration was, копия объекта из кэша возвращается лишь при условии, что не истекло ее время жизни.

2. Как ISA-сервер определяет, нужно ли кэшировать полученный из оригинального источника Web-объект?

   Определяя, следует ли кэшировать объект, ISA-сервер проверяет параметры на странице свойств механизма кэширования Cache Configuration Properties. Например, выясняет, не превышает ли размер объекта максимальный разрешенный на вкладке Advanced, а также, если адрес объекта содержит вопросительный знак (?), выясняет, включено ли кэширование динамического содержания. Если объект не нарушает никаких ограничений, а также если правила маршрутизации настроены для кэширования ответов, ISA-сервер размещает копию объекта в кэше и возвращает объект пользователю.

3. При каких условиях ISA-сервер кэширует динамическое содержимое?

   ISA-сервер кэширует динамическое содержимое, если такое кэширование включено (на вкладке Advanced диалогового окна свойств механизма кэширования Cache Configuration Properties) и если применимое к запросу правило маршрутизации требует кэширования содержимого (на вкладке Cache страницы свойств соответствующего правила маршрутизации). Кэширование динамического содержимого при выполнении заданий загрузки по расписанию настраивается в свойствах задания.

4. **Что такое кэширование отрицательных ответов и как оно включается?**

   Кэширование отрицательных ответов — это кэширование возвращенных ISA-серверу удаленными серверами сообщений о недоступности Web-объектов. Чтобы разрешить кэширование отрицательных ответов, перейдите на вкладку Advanced диалогового окна свойств кэша Cache Configuration Properties и установите флажок Cache objects even if they do not have an HTTP status code of 200.

5. Как ISA-сервер выполняет загрузку содержимого по расписанию, если сервер-источник требует выполнять аутентификацию клиента?

   В описанной ситуации задание загрузки содержимого по расписанию потерпит сбой.

Глава 6

Закрепление материала

1. Какие типы правил публикации доступны в режимах брандмауэра (Firewall) и сервера кэширования (Cache)? В режиме Cache?

   В режиме брандмауэра доступны лишь правила публикации серверов, а в режиме сервера кэширования — только правила Web-публикации.

2. Как вы порекомендуете опубликовать SMTP-сервер, расположенный в сети периметра, если сеть защищена ISA-сервером?

   Создайте фильтр IP-пакетов, разрешающий пересылку пакетов протокола TCP в обоих направлениях, в качестве локального укажите порт 25, а в качестве удаленного порта — Any ports. В качестве IP-адреса локального компьютера укажите адрес SMTP-сервера.

3. ISA-сервер получил HTTP-запрос. Какие протоколы ISA-сервер может использовать для пересылки запроса адресатам внутренней сети?

   Запросы можно пересылать по протоколам HTTP, Secure Sockets Layer (SSL) или FTP.

4. На каком порту служба Web-сервера IIS по умолчанию прослушивает запросы? На каком порту прослушивает запросы механизм автоматического обнаружения серверов? На каких портах ISA-сервер по умолчанию прослушивает внутренние и внешние запросы?

   По умолчанию IIS ожидает запросы на порту 80. Служба автоматического обнаружения также по умолчанию использует этот порт. По умолчанию ISA-сервер ожидает внутренние запросы на порту 8080, а внешние — на порте 80.

5. Почтовый сервер совмещен на одном компьютере с ISA-сервером. Какие четыре фильтра IP-пакетов следует создать, чтобы предоставить внутренним и внешним клиентам доступ к службам протоколов SMTP и POP3?

   Для нормальной работы SMTP сервера необходимо создать два фильтра IP-пакетов: первый должен разрешать входящие TCP-подключения на локальной порт 25 с любого удаленного порта, а второй — разрешать исходящие TCP-подключения на всех локальных портах с удаленного порта 25. Для поддержки протокола POP3 также требуется два фильтра IP-пакетов: первый должен разрешать TCP-подключения на локальный порт 100 с любого удаленного порта, а второй — исходящие TCP-подключения на всех локальных портах с удаленного порта 110.

Глава 7

Закрепление материала

1. Вы создали политику предприятия и хотите применить ее к массиву Branch1. Какие возможны варианты применения политики предприятия к массиву? При каких условиях удаляются политики уровня массива? В каких случаях применить политику предприятия к массиву невозможно?

   Политику предприятия применяют к массиву в следующем порядке: открывают страницу свойств политики предприятия и выбирают массив, к которому требуется применить политику. Правила протоколов и узлов и содержимого на уровне массива, несовместимые с политикой предприятия, удаляются. Вам не удастся применить политику предприятия, если массив сконфигурирован для использования лишь политики массива.

2. Как изменить политику предприятия по умолчанию, если она уже действует в существующих массивах?

   Чтобы изменить действующую заданную по умолчанию политику предприятия, нужно перенастроить каждый из массивов на использование нестандартных (пользовательских) параметров конфигурации предприятия.

3. Как разрешить компьютеру — члену массива обрабатывать больше сетевых запросов, чем другие компьютеры массива?

   Чтобы разрешить компьютеру — члену массива обрабатывать больше сетевых запросов, чем разрешено по умолчанию, следует изменить коэффициент нагрузки для данного компьютера. Она доступна на вкладке Array Membership страницы свойств компьютера в папке Computers оснастки ISA Management.

4. Обязательно ли устанавливать изолированные ISA-серверы в домене? Можно ли применить политику предприятия к изолированному ISA-серверу?

   В домене необходимо устанавливать изолированные серверы, но только при условии, что это не домен Windows 2000. Это обусловлено тем, что информация о конфигурации изолированного сервера хранится в реестре, а не в хранилище службы каталогов Active Directory. К изолированным ISA-серверам невозможно применить политику предприятия.

5. В составе ISA-сервера поставляются три мастера, упрощающие настройку VPN. Расскажите, для чего используется каждый из них.

   Мастер Local ISA Server VPN Configuration позволяет настроить локальный ISA-сервер для инициации и приема подключений. Мастер Remote ISA Server VPN Configuration позволяет сконфигурировать удаленный ISA-сервер для инициации и приема подключений. Мастер ISA Virtual Private Network Configuration применяется для настройки доступа мобильных пользователей по VPN-подключениям.

Глава 8

Закрепление материала

1. Какие четыре основных компонента определены в стандарте H.323, созданном для поддержки сетевых интерактивных видеоконференций в реальном времени?

   В стандарте H.323 предусмотрено четыре основных компонента системы проведения сетевых конференций: терминалы, шлюзы, привратники и узлы управления многосторонней связью.

2. Какие функции выполняет H.323 Gatekeeper при обслуживании клиентов видеоконференций по протоколу H.323?

   Привратник H.323 Gatekeeper выполняет преобразование адресов, которое позволяет клиентам H.323 вызывать друг друга по псевдонимам, а не IP-адресам. Привратник H.323 Gatekeeper также обеспечивает автоматическую регистрацию клиентов по протоколу RAS. Кроме того, он позволяет применять правила управления вызовами и правила маршрутизации, которые определяют, куда направлять вызовы. Наконец, привратник необходим для проведения видеоконференций, когда вызовы направляются через брандмауэры или через общедоступную телефонную сеть с применением шлюзов H.323.

3. Опишите, что происходит, когда клиент H.323, зарегистрированный на привратнике H.323 Gatekeeper одной сети, вызывает по псевдониму на основе адреса электронной почты клиент H.323, зарегистрированный на H.323 Gatekeeper другой сети.

   Клиент H.323 подключается к локальному привратнику H.323 Gatekeeper. Если последний определяет, что имя домена, указанное в псевдониме — электронной почте, не является внутренним адресом, привратник пересылает вызов на корпоративный ISA-сервер. ISA-сервер выделяет имя домена и запрашивает соответствующий ему IP-адрес в Интернете, пытаясь выполнить разрешение имен. Получив вызов псевдонима клиента H.323, удаленный ISA-сервер запрашивает корректный внутренний адрес у внутреннего привратника H.323 Gatekeeper, который в свою очередь преобразует псевдоним в сетевой адрес и возвращает ISA-серверу. Далее удаленный ISA-сервер направляет подтверждение локальному ISA-серверу и устанавливает подключение. С этого момента и до завершения сеанса оба ISA-сервера поддерживают открытым подключение, созданное привратниками H.323 Gatekeeper.

4. Клиент H.323 пытается вызвать другой клиент по псевдониму *someone@microsoft.com*. Этому псевдониму соответствует два правила адресов электронной почты. Первое правило предусматривает режим сопоставления Suffix, содержит строку сопоставления «microsoft.com» и значение его параметра Metric — 4. Второе правило предусматривает режим сопоставления Exact, содержит строку microsoft.com, а его параметр Metric равен 5. Какое из этих правил будет использовано для обработки вызова?

   Будет применяться второе правило, так как точное соответствие строки сопоставления более приоритетно, чем соответствие по суффиксу.

5. Каковы преимущества правила маршрутизации с типом адресата Gateway?

   При пересылке вызовов на шлюз H.323 существует возможность пересылать их в общедоступную телефонную сеть.

Глава 9

Занятие 2. Задание 1

1. Какой из двух трафиков данных — от клиента к серверу или от сервера к клиенту — в первом подключении, зарегистрированном в журнале в 02:31:35, больше? Совет: по таблице 9-2 определите имена полей, в которых регистрируется информация о количестве отправленных (Bytes Sent) и принятых (Bytes Received) байт и сравните эти значения в первой записи журнала.

   Трафик от сервера к клиенту существенно больше. Значение поля cs-bytes равно 259, а sc-bytes — 2200.

2. Откуда возвращены данные в ответ на запрос — из Интернета или из кэша? Совет: по таблице 9-2 определите имя поля, в котором указывается источник получения объекта (Object Source). Затем сравните значение соответствующего поля журнала со значениями, приведенными в таблице 9-4.

Запрос выполнен с использованием кэша, о чем говорит значение Cache в поле s-object-source.

3. Когда (в какое время) удаленный узел сбросил подключение? Совет: по таблице 9-5 определите код результата, соответствующего этому событию. Затем найдите в журнале запись с таким кодом и посмотрите время события.

   В 02:34:47. Это момент, когда служба Web-прокси перешла в состояние (поле sc-status) с кодом 10054.

4. Найден ли запрошенный в 02:31:45 объект в кэше? Был ли он изменен? Из какого источника в конечном счете объект возвращен клиенту? Совет: найдите в журнале запись о событии произошедшем в указанное время. По таблице 9-2 определите имя поля, в котором регистрируется код результата. Затем сравните значение соответствующего поля журнала со значениями, приведенными в таблице 9-5.

   Объект расположен в кэше, но он изменился. Запрос перенаправлен, и объект получен из Интернета. Такой вывод сделан на основании того, что значение поля s-object-source равно VFINET.

5. Какая операция выполнена в 04:55:14? Удалось ли обратиться к адресату? Совет: найдите в журнале запись о событии, произошедшем в указанное время. По таблице 9-2 определите имя поля, в котором ссдержится информация о выполненной операции, и найдите соответствующее поле в данной записи. Затем определите результат операции, используя значения из таблицы 9-5.

   Выполнена операция POST, но адресат не найден, потому что значение поля s-operation равно POST, а поля sc-status — 404.

Закрепление материала

1. Какие четыре типа ответных действий выполняются в ответ на оповещение? Какие из них настроены и выполняются по умолчанию?

   Существует четыре ответных действия для оповещения: отправка сообщения по электронной почте, запуск определенной программы, регистрация события в журнале событий Windows (Windows Event Log), остановка или запуск любой службы ISA-сервера, По умолчанию оповещения сконфигурированы для регистрации события в журнале событий Windows 2000.

2. Какое имя получит файл журнала брандмауэра, созданный в формате ISA-сервера 23 октября 2002 года?

   Имя файла журнала — FWSD20021023.

3. Какие права необходимы пользователю, чтобы конфигурировать задания для создания отчета?

   Пользователь должен обладать привилегиями локального администратора и правом запуска DCOM-объектов на всех ISA-серверах массива.

4. Опишите недостаток назначения подключению приоритета пропускной способности, отличного от приоритета по умолчанию?

   Для обслуживания новых приоритетов пропускной способности требуется больше вычислительных мощностей, чем для приоритетов по умолчанию.

5. Каковы преимущества применения консоли ISA-сервер Performance Monitor для просмотра показаний счетчиков производительности ISA-сервера?

   Оснастка ISA Server Performance Monitor позволяет наблюдать за данными только ISA-сервера — отдельно от других системных данных. Она содержит 21 счетчик производительности ISA-сервера, предустановленный в системный монитор, средство наблюдения в реальном масштабе времени.

Глава 10

Занятие 1. Практикум

5. Сколько активных подключений указано для внешнего интерфейса ISA-сервера в колонке Local Address? Посмотрите на внешние адреса подключений: действительно ли они внешние, или лишь представляют другой порт локального адреса? Какие порты этих внешних адресов используются для отправки информации на локальные адреса ISA-сервера.

   Ответы определяются конкретной системой и ее состоянием.

8. Взгляните в коней списка вывода, Сколько дополнительных активных подключений (по сравнению с данными, полученными в результате выполнения пункта 5) появилось на внешнем интерфейсе ISA-сервера в колонке Local Address? Есть ли новые активные порты на внешних адресах? После просмотра данных скажите, какой внешний порт используется для отправки Web-данных на локальный внешний IP-адрес?

   Для пересылки Web-данных па локальный компьютер применяется порт 80.

9. На какие локальные порты внешнего интерфейса ISA-сервера отправляются Web-данные? Эти динамические порты обычно изменяются от подключения к подключению. Укажите номера этих портов.

   Ответы определяются конкретной системой и ее состоянием. На внешнем интерфейсе обычно активно несколько динамических портов.

Закрепление материала

1. ISA-сервер установлен в сети периметра (DMZ). Адресное пространство в защищенной ISA-сервером сети состоит из подсети 192.168.0.0/24, а сеть периметра перед ISA-сервером сконфигурирована как подсеть 192.168.1.0/24. Внутренний адрес ISA-сервера — 192.168.0.1, а внешний — 192.168.1.99. Адрес внешнего шлюза — 192.168.1.1. Ни с одного из клиентских компьютеров, расположенных за ISA-сервером, нет доступа в Интернет, При выполнении команды Route print на ISA-сервере получена информация, показанная на рис. 10-5. Где допущена ошибка в таблице маршрутизации? Как исправить неполадку с помощью команды Route.

   Проблема с таблицей маршрутизации в том, что в ней не определен маршрут по умолчанию, указывающий на внешний шлюз. Чтобы устранить неполадку, выполните в командной строке следующую команду:

   ```
   route add 0.0.0.0 mask 0.0.0.0 192.168.1/1
   ```

2. После перезагрузки сервера, описанного в вопросе 1, неполадка осталась. Как избежать изменений в таблице маршрутизации после каждой перезагрузки?

   Вы можете устранить неполадку, добавив постоянный маршрут. Для этого нужно либо добавить статический маршрут в оснастке Routing and Remote Access (Маршрутизация и удаленный доступ), либо воспользоваться ключом –p в утилите Route следующим образом:

   ```
   route add 0,0.0.0 mask 0.0.0.0 192.168.1.1
   ```

3. Какая утилита применяется для выявления атаки синхронизации (SYN)? Опишите характерный признак такой атаки?

   Для обнаружения атаки синхронизации (SYN) иногда применяют утилиту Netstat. Такие атаки характеризуются потоком полуоткрытых подключений, исходящих из *ложного* (spoofed) адреса-источника, причем номера портов в них последовательны.

4. Зачем применяют утилиту Telnet при проверке конкретных TCP- или UDP-портов?

   Успешное подключение Telnet к определенным портам TCP или UDP означает, что работающие на этих портах службы принимают команды от внешних пользователей. Это может быть как нормальным состоянием (например при публикации службы), так и существенной «дырой» в защите, когда некоторые потенциально уязвимые службы оставлены открытыми, чем может воспользоваться злоумышленник.

5. Вы запустили мастер VPN Configuration и в качестве протокола аутентификации указали L2TP. Сколько фильтров пакетов должен создать мастер? Какие порты статически откроют эти фильтры?

   Создаются два фильтра IP-пакетов, которые разрешают трафик протокола L2TP на портах 500 и 1701.

Приложение Б

Вопросы

1. Что следует предпринять, чтобы успешно обновить серверы Proxy Server до ISA-серверов в действующей сетевой среде?

   Удалите два сервера Proxy Server 2.0 из массива, после чего обновите операционную систему до Windows 2000 Server с пакетом обновлений Service Pack I. Мастер установки Windows 2000 предупредит вас, что Proxy Server 2.0 не совместим с новой ОС, но продолжит обновление. По завершении установки Windows 2000 Server обновите схему Active Directory в домене, выполнив процедуру инициализации предприятия. Установите ISA-сервер *на* первом компьютере и создайте политики предприятия и массива. Установите ISA-сервер на другом компьютере, присоединив его к новому массиву. Мастер установки удалит кэш Proxy Server 2.0 и создаст новый кэш для ISA-сервера. Параметры конфигурации сервера Proxy Server переносятся в новый массив, причем порядок переноса определяется конфигурацией политики предприятия. Подробнее о порядке переноса правил Proxy Server 2.0 на ISA-сервер при обновлении — в разделе «Microsoft Proxy Server 2.0 array considerations» справочной системы ISA-сервера.

2. После перехода на ISA-серверы сервер Exchange Server в Сиэтле утратил способность поддерживать обмен электронной почтой через Интернет. Что следует сделать для устранения неполадки?

   Для публикации сервера Exchange в среде Proxy Server 2.0 необходимо наличие на сервере Winsock-клиента, особая конфигурация которого указана в файле WspClnt.ini. ISA-сервер эту конфигурацию не поддерживает.

   На компьютере сервера Exchange переименовывают или удаляют WspClnt.ini и конфигурируют его как клиент SecureNAT, определяя в качестве основного шлюза внутреннего сетевого адаптера IP-адрес внутреннего сетевого адаптера ISA-сервера. Проверите настройку шлюза и других параметров сетевого адаптера, выполнив команду ipconfig /all. Не устанавливайте на сервере Exchange клиент брандмауэра. Почтовый сервер следует опубликовать на ISA-сервере, чтобы SMTP-трафик пересылался на сервер Exchange. Запустите Мастер Secure Mail Server, который поможет вам опубликовать протоколы SMTP и POP3 и порты удаленного вызова процедур (RPC) сервера Exchange. Публикация протокола SMTP позволит серверу Exchange Server получать почту из Интернета, а протоколы POP3 и RPC обеспечат внешним клиентам доступ к серверу Exchange для получения почты.

   Вы вправе не прибегать к услугам мастера и вручную создать серверное правило публикации для определения протокола SMTP, а также другие необходимые правила. Сервер Exchange создает собственные исходящие подключения независимо от любых опубликованных (входящих) сессий и подключений протокола TCP/IP. Поэтому вы должны со-

здать правило протоколов, которое разрешает исходящий SMTP-трафик (порт 25) с сервера Exchange к внешним клиентам (в Интернет) для получения почты.

3. Как вы предполагаете развернуть ISA-серверы в указанных филиалах, чтобы обеспечить централизованное управление?

   Установите ISA-сервер в указанных двух филиалах в смешанном режиме (Integrated), чтобы обеспечить кэширование и резервные подключения к Интернету, Сконфигурируйте ISA-серверы в филиалах как отдельные массивы, которым соответственно присвойте имена «Paris» и «Orlando». Присоедините новые массивы к политике предприятия, определенной в массиве «Seattle». Политика предприятия обеспечит централизованное управление протоколами, правилами узлов и содержимого и многими другими элементами политики массива.

4. Расскажите, каким образом повысить производительность работы Web и протокола FTP в трех указанных офисах.

   Сконфигурируйте кэширование для всех трех массивов, чтобы обеспечить оптимальную производительность Web и FTP. Объедините массивы филиалов в Париже и Орландо в цепочку с массивом штаб-квартиры в Сиэтле (эта операция выполняется на странице свойств узла Network Configuration в оснастке ISA Management). В каждом массиве сконфигурируйте все исходящие Web-запросы на «разрешение запросов в массиве до выполнения маршрутизации» (флажок Resolve requests within array before routing на вкладке Outgoing Web Requests диалогового окна свойств массива). Таким образом, вы создадите иерархический кэш, и все исходящие запросы станут обслуживаться по протоколу CARP (Cache Array Routing Protocol); это позволит эффективно определять массив, в котором содержится кэшируемый объект до пересылки запроса в Интернет. В каждом массиве включите фильтр приложений HTTP Redirector Filter (он расположен в папке Application Filters), чтобы клиенты SecureNAT и брандмауэра могли пользоваться преимуществами кэширования. Чтобы предотвратить перегрузку интернет-трафика в рабочие часы, сконфигурируйте кэширование по расписанию на загрузку содержимого в непиковое время. Включите и сконфигурируйте активное кэширование — в результате популярное содержимое в кэше будет обновляться до истечения срока его устаревания. Для настройки кэширования по расписанию и активного кэширования используется узел Cache Configuration в оснастке ISA Management.

5. После настройки механизма кэширования в массивах вы обнаружили с помощью оснастки Performance Monitor, что показания счетчика Cache Hit Ratio малы. Что можно предпринять, чтобы повысить частоту попаданий кэша?

   Счетчик попаданий кэша Cache Hit Ratio позволяет быстро выяснить эффективность действующей конфигурации кэширования. Нулевые показания свидетельствуют о неработающем кэше, а низкие показания — о низком уровне попаданий кэша, то есть о том, что большинство запросов обслуживается из Интернета, а содержимое либо не подлежит кэшированию, либо кэш слишком мал. Увеличьте размер кэша или время жизни (TTL) кэшируемых объектов.

6. Расскажите, как настроить маршрутизацию всего интернет-трафика филиалов через массив ISA-серверов в Сиэтле и обеспечить поддержку резервных подключений на случай сбоев основных.

   Создайте подмножество адресатов, состоящее из компьютеров внутренней сети в каждом филиале. Для каждого массива в филиалах (в Париже и Орландо) создайте правило маршрутизации, которое перенаправляет все запросы, не относящиеся к данному подмножеству адресатов, на вышестоящий сервер в штаб-квартире в Сиэтле. В этом же правиле маршрутизации укажите, что при сбое основного маршрута запросы обслуживаются по резервному маршруту — через выделенное подключение к Интернету в филиале в Орландо и по ISDN-линии — в парижском филиале.

7. Анализируя журналы Web-прокси, вы обнаружили, что все пользователи получают анонимный доступ. Что следует изменить, чтобы регистрировались имена пользователей?

   Клиенты под управлением Windows 2000 Professional с Microsoft Internet Explorer поддерживают аутентификацию пользователей Web-прокси. На компьютерах под управлением UNIX сконфигурируйте клиенты с поддерживающими стандарты CERN браузерами для аутентификации пользователей Web-прокси. В диалоговом окне свойств каждого из массивов перейдите на вкладку Outgoing Web Requests и установите флажок Ask unauthenticated users for identification, чтобы выполнялась аутентификация и регистрация журналах событий на уровне пользователей. В этом же диалоговом окне укажите встроенный метод аутентификации Windows NT (флажок Integrated) или аутентификации на основе хеша (флажок Digest with this domain) для безопасной проверки подлинности. Для совместимости с протоколом HTTP выберите базовую аутентификацию (флажок Basic with this domain). Последняя операция позволит клиентам браузера, которые не поддерживают проверку подлинности по механизму «запрос — ответ» в Windows NT, проходить проверку подлинности на основе только текстовых реквизитов учетной записи. Если браузеру клиента не удается «прозрачно» передать на ISA-сервер информацию аутентификации, он запросит ее у пользователя. Выполненная проверка подлинности действительна лишь для текущего сеанса и выполняется независимо от запросов проверки подлинности на сервере Web-узла.

8. Как вы предполагаете обеспечить пересылку всего локального трафика (то есть трафика к узлами в домене верхнего уровня .fr), инициированного в парижском филиале, в Интернет через ISDN-линию, а остального трафика, как и прежде, — через штаб-квартиру в Сиэтле?

   Следует создать подмножество адресатов, состоящее из доменов *.fr, и правило маршрутизации, которое предусматривает выполнение запросов на адреса этого подмножества непосредственно из Интернета. Кроме того, необходимо позаботиться о корректном расположении созданного правила в оби ем наборе правил, то есть оно должно обрабатываться до других правил маршрутизации, которые перенаправляют трафик в штаб-квартиру.

9. Как вы предполагаете сконфигурировать сеть периметра и опубликовать указанные три Web-сервера, чтобы обеспечить требуемый доступ?

   Сконфигурируйте ISA-сервер для подключения к сети периметра через третий сетевой адаптер (172.16.0.1/24), который в этом случае следует определить как внешнюю сеть по отношению к ISA-серверу. Позаботьтесь о том, чтобы в таблице локальных адресов (LAT) массива в Сиэтле не указывалась сеть периметра (172.16.0.0/24). Обмен данными между двумя внешними сетями (например из Интернета в сеть периметра) через ISA-сервер обрабатывается механизмом IP-маршрутизации (IP Routing) и ограничивается фильтрами IP-пакетов. Операция включения фильтрации IP-пакетов (флажок IP Packet Fitters) и IP-маршрутизации (флажок IP Routing) в массиве в Сиэтле выполняется в диалоговом окне свойств узла IP Packet Filters, расположенного в папке Access Policy оснастки ISA Management. Сконфигурируйте массив в Сиэтле, разрешив доступ в сеть периметра из Интернета. Для этого создайте фильтры IP-пакетов для протокола HTTP на портах 80 и 443, которые разрешают всем удаленным пользователям доступ в локальную сеть периметра.

   Для успешного взаимодействия Web-серверов с сервером SQL Server во внутренней сети следует опубликовать последний. В стандартной установочной конфигурации ISA-сервера протокол SQL Sockets не предусмотрен — вы должны создать его определение самостоятельно. Для этого создайте определение протокола с именем SQL Sockets, указав следующие параметры: направление — входящее (Inbound), порт — 1433 и протокол — TCP. Требуется закрыть прямой доступ внешних пользователей к серверу SQL Server — они должны обращаться к нему только через Web-серверы. Ограничьте доступ лишь Web-серверами, создав в папке Client Address Set (подпапка папки Policy Elements) подмножество адресов клиентов, состоящее из IP-адресов всех Web-серверов (172.16.2—4). Убедитесь в том, что включена фильтрация IP-пакетов. Если не включить фильтрацию IP-пакетов, правило

публикации сервера будет применяться ко всем клиентам, независимо от наличия или отсутствия отдельных подмножеств клиентских адресов. Далее опубликуйте сервер, воспользовавшись созданным определением протокола и подмножеством клиентов. Правило публикации определите следующим образом: в качестве адреса внешнего интерфейса определите IP-адрес адаптера, подключенного к сети периметра, (172.16.0.1), а в качестве внутреннего адреса — IP-адрес сервера SQL Server (192.168.0.10). Сконфигурируйте SQL Server как клиент SecureNAT, определив в качестве основного шлюза его сетевого адаптера IP-адрес адаптера внутренней сети на ISA-сервере (192.168.0.1).

10. Объясните, как опубликовать частное серверное приложение.

    Служба публикации Web-серверов управляет ограничениями, применяемыми как к подмножествам клиентских адресов, так к пользователям и группам. Однако правила публикации серверов поддерживают лишь подмножества клиентских адресов (IP-адресов), поэтому вам придется определять и регулировать доступ, указывая интервалы IP-адресов. Создайте подмножество клиентских адресов или наборы, которые содержат всех ваших удаленных пользователей, например интервал IP-адресов Интернет-провайдера компании Contoso.

    Далее создайте определение протокола входящего направления через TCP-порт 2122. Протокол обязательно определите как входящий, чтобы он стал доступным для выбора в правиле публикации серверов. Опубликуйте сервер, указав в правиле внешний IP-адрес ISA-сервера и внутренний IP-адрес частного серверного приложения. Ограничьте доступ лишь ранее определенному подмножеству клиентских адресов.

11. Как следует переконфигурировать ISA-сервер и клиенты в рассматриваемых подсетях, чтобы восстановить доступ в Интернет?

    Изучите таблицу маршрутизации ISA-сервера и добавьте в нее адресата и шлюз, соответствующие компьютеру-лаборатории отдела контроля качества, назначив их внутреннему интерфейсу ISA-сервера. В этом примере компьютер ISA-сервер следует сконфигурировать для пересылки пакетов, направленных в подсети 192.168.1.0/24 и 192.168.2.0/24, на шлюз 192.168.0.2 через интерфейс 192,168.0.1. Воспользуйтесь командой route, чтобы проверить и при необходимости устранить неполадки маршрутизации. Настройте основной шлюз промежуточных маршрутизаторов на перенаправление на вышестоящие маршрутизаторы, и, в конечном счете, — на внутренний интерфейс ISA-сервера.

    Позаботьтесь о правильной настройке основных шлюзов клиентов SecureNAT, то есть в качестве шлюза на каждом клиенте следует указать IP-адрес соответствующего промежуточного маршрутизатора. В рассматриваемом примере основной шлюз компьютера-лаборатории в отделе контроля качества следует настроить на адрес 192.168.2.1. Кроме того, убедитесь, что адрес прокси на клиентах брандмауэра и Web-прокси настроен на внутренний IP-адрес ISA-сервера (192.168.0.1). После правильной настройки промежуточных маршрутизаторов и клиентов о корректной работе клиентских подключений «позаботится» стандартный механизм маршрутизации протокола TCP/IP.

12. Какие операции по переконфигурированию ISA-сервера следует предпринять, чтобы обеспечить поддержку новой топологии сети?

    Удалите парижский массив ISA-серверов из политики предприятия и затем — программное обеспечение ISA-сервера, чтобы вывести компьютер из массива. Присоедините этот компьютер к домену в Париже и выполните процедуру инициализации предприятия, обновив схему Active Directory нового домена. Снова установите ISA-сервер, создав новый массив ISA-серверов в парижском домене. Создайте правила протоколов и правила узлов и содержимого так, чтобы предоставить доступ в Интернет сотрудникам парижского филиала.

    В Сиэтле настройте VPN-подключение с филиалом в Париже, выполнив инструкции мастера локальной конфигурации Local ISA Server VPN Configuration. На парижском ISA-сервере запустите мастер Remote ISA Server VPN Configuration и воспользуйтесь файлом

данных, ранее созданным мастером Local ISA Server VPN Configuration, чтобы настроить парижский филиал в качестве конечной точки VPN-туннеля.

13. **Вы** сконфигурировали VPN в филиале в Сиэтле, но установить связь с парижским филиалом не удается. Конфигурации каких компонентов следует просмотреть в процессе устранения неполадок подключения?

    Прежде всего выясните правильность определения протоколов. ISA-сервер поддерживает оба протокола — L2TP (Layer Two Tunneling Protocol) и PPTP (Point-to-Point Tunneling Protocol). L2TP работает в паре с протоколом IPSec. Кроме того, проверьте правильность настройки удаленной конечной точки — при ее установке требуется использовать корректный VPC-файл, созданный мастером настройки VTN. По умолчанию мастер настройки VPN не конфигурирует двустороннюю инициацию подключений — ее следует настраивать особо. Далее откройте окно оснастки Routing and Remote Access (Маршрутизация и удаленный доступ) и проверьте корректность конфигурации статических маршрутов, а также работоспособность интерфейса обратного вызова, значок которого расположен в папке General.

14. Расскажите, как перевести пользователей с существующего частного подключения по телефонной линии на VPN-подключение, развернув ISA-сервер,

    Воспользуйтесь мастером Virtual Private Network Configuration (вызывается из контекстного меню папки Network Configuration в оснастке ISA Management) в массиве в Сиэтле, который сконфигурирует сервер маршрутизации и удаленного доступа (Routing and Remote Access Server) и настроит на нем VPN-порты для туннелей L2TP и PPTP. Мастер также создаст четыре правила фильтров IP-пакетов, чтобы открыть пакетам протоколов PPTP и L2TP доступ к ISA-серверу. Для каждого клиента создайте учетную запись подключения к Интернету по телефонной линии и дополнительное (вторичное) VPN-подключение. На клиентах под управлением Windows 2000 воспользуйтесь мастером сетевого подключения Network Connection и настройте новое подключение к частной сети через Интернет. В качестве имени VPN-хоста укажите IP-адрес или полное доменное имя (Fully Qualified Domain Name, FQDN) внешнего адаптера ISA-сервера.

15. Почему пользователи не могут получить доступ в Интернет из ЛВС удаленных офисов? Расскажите, как администратору устранить проблему, не прибегая к ручному переконфигурированию каждого портативного компьютера.

    Возможно, клиент брандмауэра или клиент Web-прокси и ISA-сервер не настроены для автоматического обнаружения. В Control Panel (Панель управления) клиентского компьютера дважды щелкните значок Firewall Client и установите флажок Automatically detect ISA Server. Автоматическое обнаружение на клиентах Web-прокси выполняется через браузер. Когда автоматическое обнаружение отключено, клиенты не в состоянии автоматически обновлять свои подключения к другим ISA-серверам, например при обращении в другие филиалы.

    ISA-сервер предоставляет клиентам информацию обновления по протоколу WPAD (Web Proxy Auto Discovery Protocol — «протокол автоматического обнаружения Web-прокси»). В диалоговом окне свойств массива перейдите на вкладку Auto Discovery, установите флажок Publish automatic discovery information и укажите порт для выполнения автоматических запросов обнаружения — по умолчанию порт 80. Это стандартный порт Web-сервера, поэтому, если на компьютере с ISA-сервером установлен IIS, позаботьтесь, чтобы другие Web-узлы не использовали порт 80, в противном случае возникнет конфликт со службой автоматического обнаружения. Воспользуйтесь командой netstat -na, чтобы проверить, нет ли других приложений, работающих на этом порте. Затем сконфигурируйте DNS или DHCP, чтобы создать для клиентов нужную запись WPAD. Подробные инструкции но конфигурированию записей DNS и DHCP вы найдете в настоящем курсе и в справочной системе ISA-сервера.

16. После изменения в структуре доменов обнаружилось, что сетевой трафик в Интернет существенно возрос, а также замедлился доступ пользователей в интрасеть. На компьютерах сотрудников филиала в Орландо установлен клиент брандмауэра. Какова наиболее вероятная причина задержек при доступе пользователей к сети?

Изучите логическое расположение внутренних и внешних серверов доменных имен (DNS) и убедитесь, что не все клиенты сконфигурированы для разрешения запросов внутренних компьютеров средствами внешних серверов имен. При наличии клиента брандмауэра клиентский компьютер на разрешает имена самостоятельно, а пересылает запросы на разрешение имен ISA-серверу. Поскольку на клиентах установлено ПО клиента брандмауэра, в *таблице локальных доменов* (Local Domain Table, LDT) следует указать имена всех доменов внутренней сети. В процессе определения домена адресата клиенты брандмауэра прежде всего будут запрашивать LDT и, найдя его, не станут отправлять запрос на ISA-сервер. Этот способ высокопроизводительного разрешения имен внутренних доменов пригоден только для компьютеров с клиентом брандмауэра.

Приложение Б

Развертывание и администрирование ISA-сервера в сложных сетях

В этом приложении

Здесь подробно описано несколько вариантов установки версии Enterprise Edition ISA-сервера в сложных сетях. Вам предлагается создать для них сценарии развертывания и администрирования в различных ситуациях, чтобы проверить, как вы усвоили материал курса и научились устранять неполадки. Модели сетевых конфигураций рассматриваются в процессе их развития, что позволяет изучить работу ISA-сервера с разных сторон. После небольшой вводной информации об изменениях в сети перечислены вопросы, на которые вы должны ответить. Ответы для самопроверки — в приложении А «Вопросы и ответы».

Прежде всего

Чтобы выполнить задания и ответить на вопросы данного приложения, необходимо хорошо знать:

- материал данного курса;
- особенности основных компонентов Windows 2000, в том числе службы Routing and Remote Access (Маршрутизация и удаленный доступ), типы аутентификации, строение доменов, а также средства наблюдения за производительностью и управления учетными записями безопасности;
- основы построения сетей, в том числе маршрутизацию между подсетями, строение пакетов и работу с ними [протоколов TCP (Transmission Control Protocol) и UDP (User Datagram Protocol)], порты источника и адресата, службы разрешения имен DNS и протокола DHCP (Dynamic Host Configuration Protocol);
- общие утилиты и инструментальные средства устранения неполадок Windows 2000, в том числе ipconfig, netstat, route и ping.

Исходные данные

Вы отвечаете за проектирование сети и ее безопасность в Contoso Ltd., крупной международной компании, штаб-квартира которой находится в Сиэтле (штат Вашингтон). Продажей разработанных в Contoso программ занимаются коммерческие агенты, о также сотрудники филиалов в Орландо, Флориде и Париже. В Сиэтле, в отделах продаж, маркетинга и разработки, служат около 500 сотрудников; штат филиала в Орландо составляет 100 человек, а штат в Париже — 50 человек. Вы работаете в Contoso уже пять лет, в течение которых разработали и развернули существующую сетевую инфраструктуру. Сейчас вы планируете обновить все серверы Microsoft Proxy Server 2.0 до ISA-серверов, чтобы воспользоваться такими преимуществами ISA-сервера, как более производительный механизм кэширования и мощные средства обеспечения безопасности.

Вы последовательно выполните все этапы установки и администрирования ISA-сервера и ответите на вопросы, которые помогут вам оценить, насколько полно вы изучили возможности ISA-сервера.

Вопросы

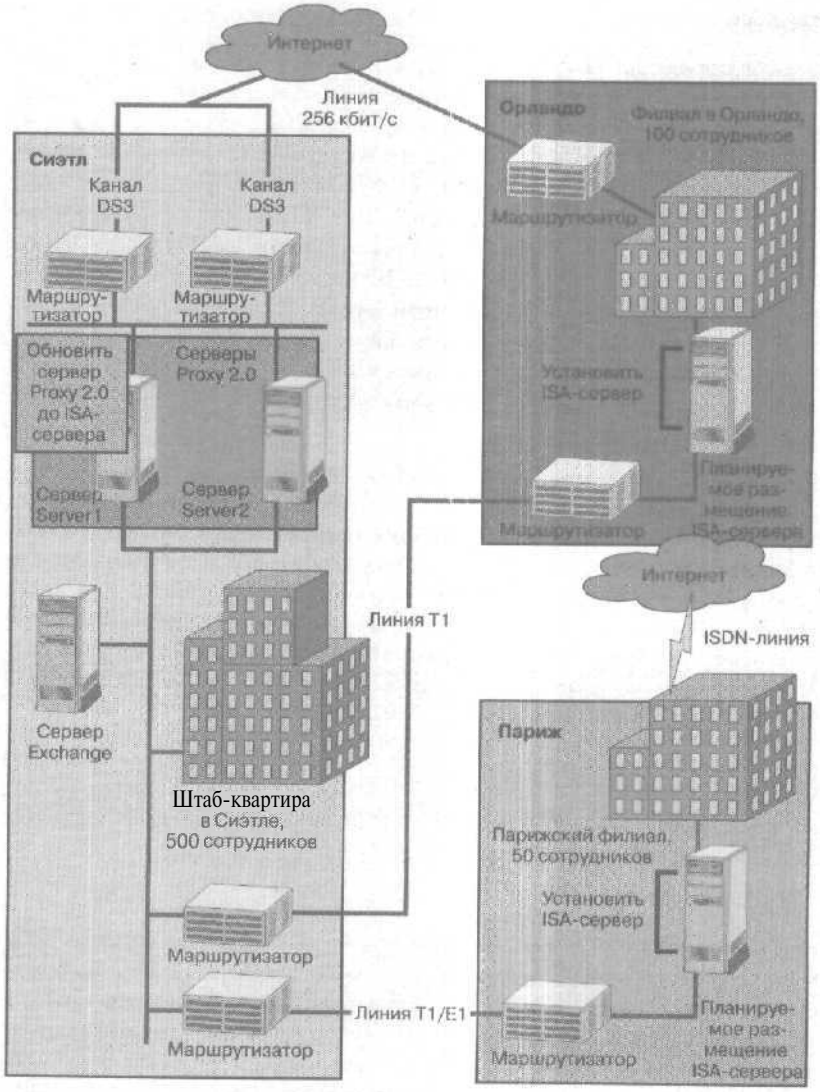
Вы планируете обновить до ISA-сервера два действующих компьютера в филиале в Сиэтле, на которых установлены Windows NT 4.0 Server и Proxy Server 2,0. Также предполагаете развернуть ISA-серверы в двух филиалах Contoso в Париже и Орландо (рис. Б-1). Сервер Microsoft Exchange Server в Contoso опубликован во внутренней сети, защищенной Proxy Server 2.0, и поддерживает почтовый обмен через Интернет для внутренних клиентов.

1. Что следует предпринять, чтобы успешно обновить серверы Proxy Server до ISA-серверов в действующей сетевой среде?

2. После перехода на ISA-серверы сервер Exchange Server в Сиэтле утратил способность поддерживать обмен электронной почтой через Интернет. Что следует сделать для устранения неполадки?

Штаб-квартира Contoso и два филиала расположены в одном домене Windows 2000. Филиалы связаны со штаб-квартирой напрямую двумя WAN-линиями T1/E1 с пропускной способностью 1,54 Мбит/с. Филиал в Орландо подключен к Интернету по каналу с пропускной способностью 256 кбит/с, а парижский филиал — по ISDN-линии с пропускной способностью 56 кбит/с. Клиенты филиалов в Сиэтле и Орландо используют Windows 2000 Professional, а в Париже клиентские компьютеры работают под управлением Windows 2000 и UNIX. Вы установили в Сиэтле два ISA-сервера в составе одного массива и планируете развернуть ISA-серверы в указанных двух филиалах, что позволит повысить производительность интернет-приложений. Требуется предусмотреть резервное (избыточное) подключение к Интернету во всех филиалах и обеспечить регистрацию в журналах активности в Web всех пользователей. Вы также хотите централизованно управлять созданной инфраструктурой из Сиэтла и маршрутизировать весь интернет-трафик средствами массива в штаб-квартире.

3. Как вы предполагаете развернуть ISA-серверы в указанных филиалах, чтобы обеспечить централизованное управление?



4. Расскажите, каким образом повысить производительность работы Web и протокола FTP в трех указанных офисах.

5. После настройки механизма кэширования в массивах вы обнаружили с помощью оснастки Performance Monitor, что показания счетчика Cache Hit Ratio малы. Что можно предпринять, чтобы повысить частоту попаданий кэша?

6. Расскажите, как настроить маршрутизацию всего интернет-трафика филиалов через массив ISA-серверов в Сиэтле и обеспечить поддержку резервных подключений на случай сбоев основных.

7. Анализируя журналы Web-прокси, вы обнаружили, что все пользователи получают анонимный доступ. Что следует изменить, чтобы регистрировались имена пользователей?

Пользователям парижского филиала не удается получить доступ к некоторым французским Web-узлам из-за того, что их фактический внешний IP-адрес является IP-адресом ISA-сервера в штаб-квартире в Сиэтле.

8. Как вы предполагаете обеспечить пересылку всего локального трафика (то есть трафика к узлами в домене верхнего уровня .fr), инициированного в парижском филиале, в Интернет через ISDN-линию, а остального трафика, как и прежде, — через штаб-квартиру в Сиэтле?

В Сиэтле руководство Contoso Ltd. планирует развернуть три Web-сервера, объединенных в Web-ферму под управлением *службы балансировки сетевой нагрузки* (Network Load Balancing, NLB). Web-ферму предполагается разместить в сети периметра и защитить посредством ISA-серверов. Внешние клиенты получают доступ к Web-ферме по протоколам HTTP и HTTPS (рис. Б-2). Указанным Web-серверам необходимо подключаться и обмениваться информацией по сокетам MS SQL Sockets (TCP-порт 1433) с сервером Microsoft SQL Server, который расположен во внутренней сети.

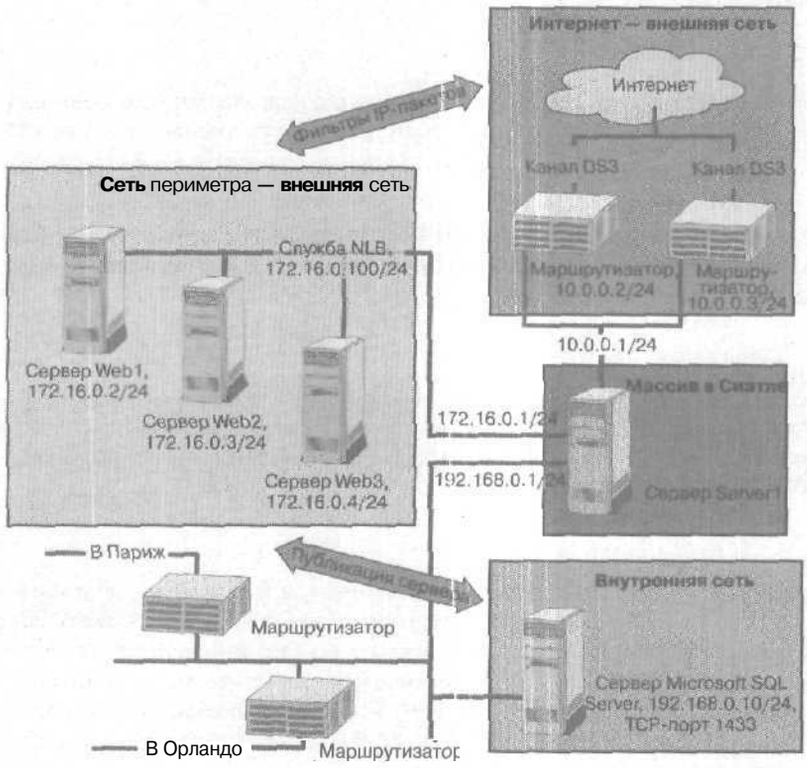
9. Как вы предполагаете сконфигурировать сеть периметра и опубликовать три указанных Web-сервера, чтобы обеспечить требуемый доступ?

Для компании Contoso Ltd. приобретено частное серверное приложение, оно установлено во внутренней сети. Вы хотите предоставить удаленный доступ к указанному приложению лишь сотрудникам компании. Предполагается, что для работы с приложением сотрудники должны сначала подключиться к Интернету, а затем запустить клиентское приложение, работающее через TCP-порт 2122.

10. Объясните, как опубликовать частное серверное приложение.

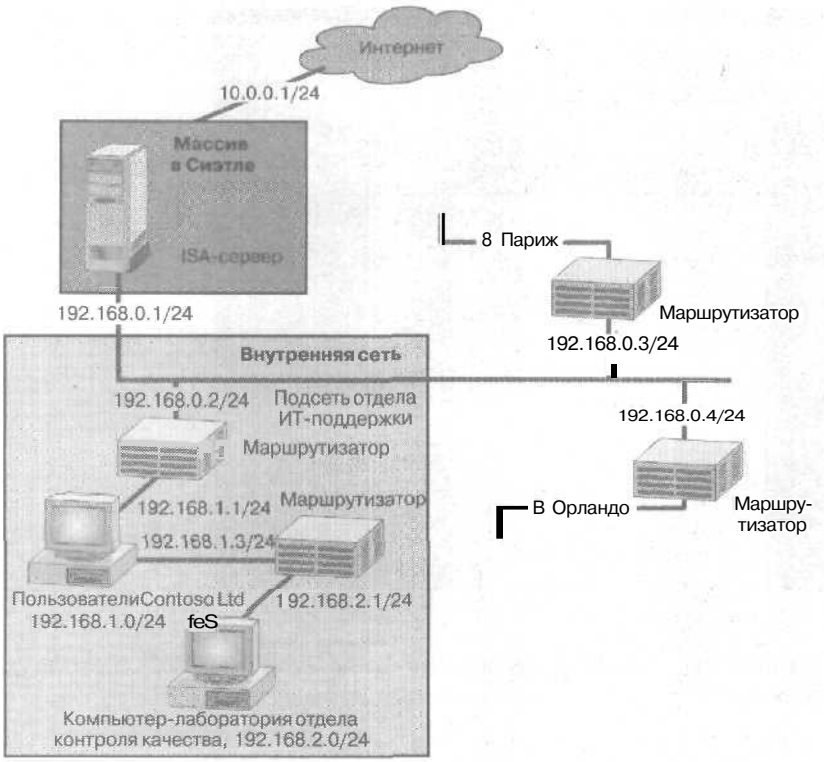
Отдел управления сетью Contoso изменил проект сети, предусмотрев подсеть для отдела ИТ-поддержки, в которой разместил тестовый компьютер-лабораторию отдела контроля качества (Quality Assurance, QA), как показано на рис. Б-3. Однако после добавления

новой подсети и маршрутизаторов сотрудники отдела не могут получить доступ в Интернет с компьютера-лаборатории.



11. Как следует переконфигурировать ISA-сервер и клиенты в рассматриваемых подсетях, чтобы восстановить доступ в Интернет?

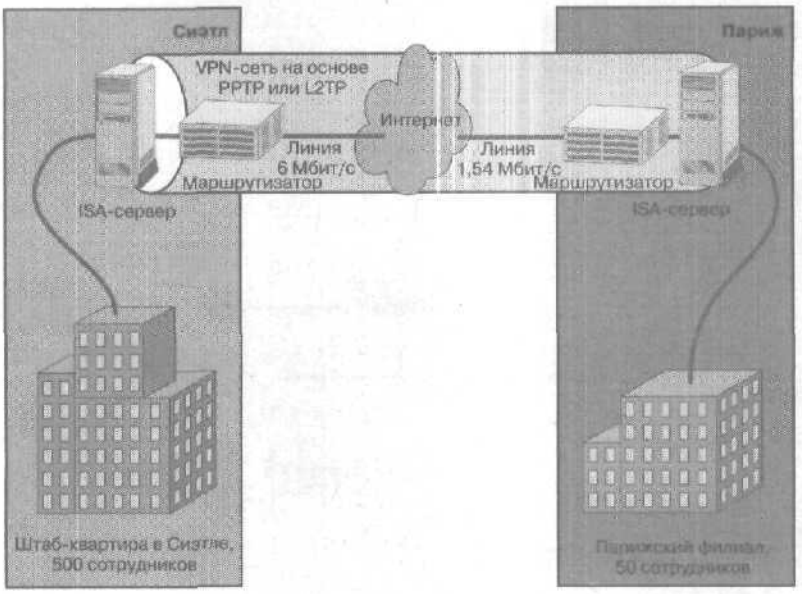
Руководство требует, чтобы вы сократили расходы своего подразделения. Вы полагаете, что для этого следует заменить WAN-подключения по выделенной линии T1/E1 между штаб-квартирой и парижским филиалом на подключение виртуальной частной сети (VPN), а также заменить (или модернизировать) ISDN-подключения парижского филиала более емким каналом связи с Интернетом. Вы планируете предоставить парижскому филиалу прямой доступ в Интернет и прекратить управление им из штаб-квартиры в Сиэтле. Предполагается, что VPN-подключения будут инициироваться сотрудниками штаб-квартиры в Сиэтле. В рамках указанной модернизации в парижском филиале создан отдельный домен и размешен контроллер этого домена. Группа поддержки сети успешно модернизировала сеть, и вы удалили ISDN-адаптер с компьютера ISA-сервера и установили внешний сетевой адаптер для подключения к Интернету, как показано на рис. Б-4.



12. Какие операции по переконфигурированию ISA-сервера следует предпринять, чтобы обеспечить поддержку новой топологии сети?

13. Вы сконфигурировали VPN в филиале в Сиэтле, но установить связь с парижским филиалом не удается. Конфигурации каких компонентов следует просмотреть в процессе устранения неполадок подключения?

Коммерческие агенты, работающие в компании Contoso Ltd., постоянно находятся в разъездах и подключаются к частному модемному пулу в штаб-квартире по бесплатному (для звонящих) телефонному номеру. Такое прямое подключение обходится компании достаточно дорого, кроме того, телефонный номер часто занят в часы интенсивного использования модемного пула. Вы полагаете, что обеспечение VPN-доступа средствами **ISA**-сервера поможет сэкономить деньги и предоставит доступ большему числу сотрудников.



14. Расскажите, как перевести пользователей с существующего частного подключения по телефонной линии на VPN-подключение, развернув ISA-сервер.

Коммерческие агенты, которые числятся в одном филиале Contoso, часто по долгу службы бывают в других филиалах компании, где им необходимо подключать свои портативные компьютеры к локальной сети. Однако доступ в Интернет у них есть лишь при подключении к ЛВС своего «родного» филиала — в двух остальных филиалах получить доступ в Интернет им не удается. На компьютерах этих пользователей установлен клиент брандмауэра.

15. Почему пользователи не могут получить доступ в Интернет из ЛВС удаленных офисов? Расскажите, как администратору устранить проблему, не прибегая к ручному переконфигурированию каждого портативного компьютера.

Филиал в Орландо реорганизовали, создан на его основе компанию с новым именем. В связи с этим весь филиал перенесли в новый домен Active Directory. Тем не менее весь сетевой трафик из Орландо все равно пересылается в Интернет через ISA-сервер, расположенный в штаб-квартире в Сиэтле.

16. После изменения в структуре доменов обнаружилось, что сетевой трафик в Интернет существенно возрос, а также замедлился доступ пользователей в интрасеть. На компьютерах сотрудников филиала в Орландо установлен клиент брандмауэра. Какова наиболее вероятная причина задержек при доступе пользователей к сети?

Предметный указатель

A

Active Directory 49
admission request *см.* запрос на доступ
Advanced *см.* оснастка MMC, расширенный вид
alias *см.* псевдоним
allow filter *см.* фильтры IP-пакетов, разрешающие
Any RPC Server 121
AOL Instant Messenger 121
Archie 121

B

block filter *см.* фильтры IP-пакетов, блокирующие
bridging *см.* сопряжение

C

Cache *см.* сервер Web-кэширования
Chargen 121
content groups *см.* группа содержимого

D

Daytime 121
demilitarized zone *см.* демилитаризованная зона
Discard 121
DNS (Domain Name System) 39
DNS Query 121
DNS Query Server 121
DNS Zone Transfer 121
DNS Zone Transfer Server 121
DNS-сервер 39
DSL (Digital Subscriber Line) 39

E

Echo 121
effective bandwidth *см.* фактическая пропускная способность
enterprise initialization *см.* инициализация предприятия
event location *см.* местоположение события
Event Viewer 321
Exchange RPC Server 121

F

Finger 121
Firewall *см.* брандмауэр
Firewall Client *см.* брандмауэр, клиент
FTP 121
FTP Download only 121
FTP Server 121
Fully Qualified Domain Name (FQDN) *см.* полное доменное имя

G

gatekeeper *см.* привратник
Gopher 121

H

H.323 121
HTTP 121
HTTPS 121
HTTPS Server 121

I

IANA (Internet Assigned Numbers Authority) 52
ICA 121
ICANN (Internet Corporation for Assigned Names) 39
ICQ 121
ICQ 2000 121
Idem 121
IKE 121
IMAP4 121
IMAP4 Server 122
IMAPS 122
IMAPS Server 122
inbound bandwidth см. пропускная способность, входящая
Integrated *см.* смешанный режим
International Telecommunications Union, ITU *см.* Международный союз телекоммуникаций
Internet Connection Sharing, ICS *см.* общий доступ для подключения к Интернету
Internet Engineering Task Force (IETF) 4
Internet Explorer *76*
Internet Service Provider, ISP *см.* интернет-провайдер
IRC 122
ISA Management 12, 180, 205, 235
ISA Server Security Configuration 105, 106
ISAPI (Internet Server Application Programming Interface) 6
ISA-сервер 2
— COM-объект администрирования 5
— Web-протокол 120
— Web-фильтр 6
— автоматическое обнаружение прокси-сервера клиентами 5
— архитектура 7-8
— аутентификация 103
— безопасная публикация серверов 3
— брандмауэр Интернета 3
— в составе массива 37
— версия
— — Enterprise Edition 2
— — Standard Edition 2
— группы содержимого 130
— журнал
— — Web-прокси 267
— — безопасности и доступа 267
— — брандмауэр 267
— — **запись** в базу данных 271
— — запись информации о пакетах 273
— — параметры ведения файлов 271
— — поля записей 274
— — фильтров IP-пакетов 267
——формат ISA 270

— - формат W3C 269
— интеграция
——аутентификация 4
— — интегрированные виртуальные частные сети 4
— — преобразование сетевых адресов 4
— интерфейс управления 5
— информация о конфигурации 39
— использование сервера Exchange 43
— исходящий запрос 101
— качество обслуживания 5
— клиент 66
— — SecureNAT 103, 111
— — Web-прокси 74, 104
— — автоматическое обнаружение 85, 86, 88
— — аутентификация 103
— — брандмауэр 70, 77, 104
— — дополнительная настройка 71
— — настройка 68, 75
— — параметры приложений 71
— — потребности 67
— кэширование 21
— — активное 23
— — иерархическое 25
— — методики 21
— — механизм 26
——обратное 22
——прямое 21
— масштабируемость 6
— — балансировка сетевой нагрузки 7
— — поддержка симметричных многопроцессорных вычислений 6
— обнаружение атаки на сеть 18
——IP-атака без создания подключения 18
— — Ping смерти 18
— — UDP-бомба 18
— — атака передачи внешних данных в Windows 18
— — атака перечисления портов 18
— — атака с обратной адресацией 18
— — сканирование всех портов 18
— — фильтры 19
— ограничение подключений 81
— оповещение 6, 258
— — DNS intrusion 265
— — Intrusion Detected 265
— — настройка 258
——порог инициирования 260
— — условия возникновения 259
— оснастка 303
— отчет
— — атаки на сеть (Security) 285
— — база данных 288
— — использование Web (Web Usage) 284
— — использование клиентских приложений (Application Usage) 285
— — конфигурирование 283, 285, 287
— — просмотр 283
— — трафика и использование Интернета (Traffic & Utilization) 285
— — учетная запись 287
—— сводный 284
— параметры 53
— перезапуск службы 95
— поддержка многопроцессорных систем 5
— подключение к Интернету
— — по телефонной линии 39
——прямое (постоянное) 39
— политика предприятия 204
— — настройка параметров 205
— — порядок применения 204
——создание 204
— пользователи и группы пользователей 111
— правила
— — механизм публикации серверов 181
——политики публикации 180
— — публикации серверов 180
— правила Web-публикации 187
— — действия 188
— — конфигурирование 187
— — создание 188
— процедуры управления 27
— публикация серверов 19, 180
— различия 2
— расписание 107
— расширения 7
— — комплект ресурсов для разработчиков 7
— режим работы 38
— сервер
——обратного Web-кэширования 4
— — прямого Web-кэширования 4
— сетевая атака 147
— — типы вторжений 147
— события 263
— совмещение с Web-сервером 42
— создание
——массива 210
——массивов 213
— типовые конфигурации сети 40
— требования
— — для брандмауэра 35
— — для обратного кэширования 36
——для прямого кэширования 35
— — для удаленного администрирования 35
— — к оборудованию 34
— уровень безопасности системы
— - Dedicated 105
— — Limited Services 105
— — Secure 105
——мастер Getting Started 105
— установка 47
— — ISA-сервера 48
— — адаптер внешней сети 47
— — выборочная 50
— — модема или адаптера ISDN 48
— — определение таблицы маршрутизации 48
——планирование 34
— — полная 50
— — создание таблицы локальных адресов 52
— — стандартная 50
— — устранение неполадок 53
— устранение неполадок 320
——Event Viewer 321
— — Netstat 322
— — Network Monitor 323
— — Performance Monitor 321
——Ping и Tracert 325

— — Telnet 323
— — аутентификация 329
— — виртуальные частные сети 331
— — методика выявления 329
— — отчет 320
— — пакетного уровня 330
— — способы устранения 332
— шаблон безопасности 4
— элемент политики 107
ISDN (Integrated Services Digital Network) 34

K

Kerberos-Adm 122
Kerberos-IV 122
Kerberos-Sec 122

L

LAT (Local Address Table) 70
LDAP (Lightweight Directory Access Protocol) 122
LDAPS 122
LDAPS GC 122
LDT (Local Domain Table) 75
Local Address Table (LAT) *см.* таблица локальных адресов
location request *см.* запрос на поиск

M

Microsoft Internet Security and Acceleration Server 2000 (ISA-сервер) 33
Microsoft ISA Server. 58
Microsoft Management Console *см.* оснастка MMC, консоли
Microsoft Proxy Server 2.0. 58
Microsoft SQL Server 122
MMS 122
Monitoring Configuration 258
MSN 122
MSN Messenger 122
multipoint control unit (MCU) *см.* узел управления многосторонней связью

N

Net2Phone 122
Net2Phone Registration 122
NetBIOS Datagram 122
NetBIOS Name Service 122
NetBIOS Session 122
Netstat 322
Network Address Translation (NAT) *CM.* ISA-сервер, интеграция, преобразование сетевых адресов
Network Load Balancing (NLB) *CM.* ISA-сервер, масштабируемость, балансировка сетевой **нагрузки**
Network Monitor 323
NNTP (Network News Transfer Protocol) 122
NNTP Server 122
NNTPS 122
NNTPS Server 122
NTP 122

O

outbound bandwidth *см.* пропускная способность, исходящая

P

Performance Monitor 321
perimeter network *см.* сеть периметра
PNM 122
POP2 122
POP3 122
POP3 Server 123
POP3S 123
POP3S Server 123
private IP-address *см.* частные IP-адреса
Proxy Server 2.0 33

Q

Quality of Service, QoS *CM.* ISA-сервер, качество обслуживания
Quote 123

R

RADIUS (Remote Authentication Dial-In User Service) 123
RDP (Remote Desktop Protocol) 123
redirector filler *см.* фильтр-перенаправитель
Request for Comments (RFC) 1918 52
RIP (Routing Information Protocol) 123
Rlogin 123
round robin *см.* циклическое обслуживание
RTSP (Real Time Streaming Protocol) 123
RTSP Server 123

S

Scheduled Content Download *см.* служба загрузка содержимого по расписанию
screened subnet *см,* экранированная подсеть
SecureNAT 7
SMTP (Simple Mail Transfer Protocol) 123
SMTP Server 123
SMTPS 123
SMTPS Server 123
SNMP (Simple Network Management Protocol) 123
SNMP Trap 123
software development kit, SDK *CM.* ISA-сервер, расширения, комплект ресурсов для разработчиков
SSH 123

T

Taskpad *см.* оснастка MMC, панель заданий
Telnet 123, 323
Telnet Server 123
TFTP (Trivial File Transfer Protocol) 123
Time 123
TTL 320

V

Virtual Private Network, VPN *см.* ISA-сервер, интеграция, интегрированные виртуальные частные сети

W

Web-запрос 193
Web-кэширования 2
Web-прокси 7, 8, 76
Web-публикация
— создание правил 194
Web-сервер 192, 193
Web-узел 39
Whois 123

А

адаптер 39
— сетевой 220
администратор 209, 241
— домена 210
— массива 210
— предприятия 210, 215
адресат
— Active Directory 251
-DNS 251
— Gatekeeper 251
— Gateway or proxy server 250
- *ILS* server 250
— Local network 251
— Multicast group 251
— None (no destination) 250
— Registration database 250
архивирование 208, 217
— конфигурации 217
архивный файл 217
аутентификация
— метод
— — базовый 330
— — на основе клиентских сертификатов 330
— — на основе хеша 330

Б

балансировка сетевой нагрузки 219
безопасное преобразование сетевых адресов 181
безопасность работы в Интернете 203
безопасный доступ 75
брандмауэр 2, 3, 31, 46, 180, 196, 219
— клиент 7
— методы фильтрации
— — IP-пакетов 13
— многоуровневый 2
— фильтрация 13
— — на уровне каналов (протоколов) 14
— — трафика приложений 15
браузер 221

В

видеоконференция 234
виртуальный адрес кластера 220
восстановление конфигурации 208
— массива 218
входящий трафик 75
вызов по требованию 225

Г

гарантированное качество обслуживания 234
группа содержимого 113–114

Д

демилитаризованная зона 137
домен 37, 39, 214
— пользователь 210

Ж

журнал пакетов 141

З

запрос
— на доступ 252
— на поиск 251

И

иерархия 25
инициализация предприятия 37, 49, 213
интернет-провайдер 39, 225
интрасеть 42

К

клиент
— SecureNAT 4
— регистрация 239, 241
код
— ошибки 278
— состояния 278
конференция 235
конфигурация 216, 242
конфигурирование 197, 205
коэффициент нагрузки 222
кэширование 79, 180
— FTP-объектов 168
— HTTP-объектов 166
— — конфигурация 167
— — настройка 167
— автоматическое обновление 173
— активное 170
— — активизация 171
— — настройка 170
— в оперативной памяти 166
— выбор порядка объектов 165
— динамическое содержимое 175
— дополнительная политика 161
— загрузка по расписанию 173
— извлечение информации 155
— конфигурация 154
— механизм работы 154
— настройка конфигурации кэша 163
— настройка объема оперативной памяти 172
— отрицательных ответов 171
— правила маршрутизации 155
— процесс 159
— размер и местоположение кэша 164

— размещение информации 155
— создание политики 154
— требования и рекомендации 163
— файл содержимого кэша 164
— фильтрация 160

Л

локальный файл 208, 217

М

маршрутизатор 41
маршрутизация 24, 79, 156, 244, 324
— Web-прокси 25
— правила 158, 16!
— создание правил 245
массив 204, 206, 213
— добавление и удаление 216
мастер
— Add Destination 250
- ISA Virtual Private Network 226
- Local ISA Server VPN 225
— Mail Server Security 196, 197
— New Alert wizard 259
- New IP Packet Filter 184
— New Routing Rule 245
- New Server Publishing Rule 180, 182
- Remote ISA Server VPN 226
— конфигурации VPN 225
масштабируемость 24
Международный союз телекоммуникаций 234
местоположение события 260
модем 34, 39, 292

О

общий доступ для подключения к Интернету 40
операционная система
- Windows 2000 2, 58, 70
- Windows NT 4.0 39, 59. 70
оснастка MMC
— консоли 2
— панель заданий 5
— расширенный вид 5
отказоустойчивость 219

П

панель заданий 2, 27
повышение производительности
— ISA-сервера 300
— кэша 301
— объекты и счетчики 302, 304
подключение
—клиент — шлюз 4
—шлюз — шлюз 4
подмножество адресатов 109–110
политика
— массива 30
— правила публикации 29
— предприятия 30
полное доменное имя 39
правила
— IP-адреса 247
— адреса электронной почты 247
— узлов 127
— — обработка путей 128
— — порядок выполнения 127
— — разрешение и запрещение действий 127
— — создание 129
привратник H.323 Gatekeeper 16, 234
— входящий вызов 252
— исходящий вызов 253
— настройка 16
— оснастка 235
— тип адресации 237
— установка 240
— — особенности 241
проверка конфигурации 210
прокси-сервер 24
пропускная способность
— входящая 295
— исходящая 295
— конфигурирование 296
— порядок применения правил 297
— приоритет 294
протокол
— AH (Authentication Header) 227
- CARP (Cache Array Routing Protocol) 24, 220, 223
— ESP (Encapsulating Security Payload) 227
— H.323 RAS (H.323 Registration, Admission, and Status protocol) 237
— ICMP (Internet Control Message Protocol) 18
— ICP (Internet Cache Protocol) 24
— IMAP4 (Internet Messaging Access Protocol 4) 197
— Kerberos **4**
- L2TP (Layer 2 Tunneling Protocol) 224
— L2TP/ IPSec (Layer 2 Tunneling Protocol / Secure Internet Protocol) 4
— MAPI (Messaging Application Programming Interface) 197
- NNTP (Network News Transfer Protocol) 197
- NNTP (Secure NNTP) 197
- NTLM (NT LAN Manager) 4
— PNA (Progressive Networks Audio) 16
- POP (Post Office Protocol) 16
- POP3 (Post Office Protocol 3) 197
— PPTP (Point to Point Tunneling Protocol) 4
- PPTP (Point-to-Point Tunneling Protocol) 224
- Real-Time Streaming Protocol (RTSP) 16
- SMTP (Simple Mail Transfer Protocol) 43
— SSL (Secure Sockets Layer) 189
— TCP/IP (Transmission Control Protocol/Inlernet Protocol) 37
— Web Proxy Autodiscovery Protocol 5
- WPAD (Web Proxy Autodiscovery Protocol) 85
— настройка определения 112
— поддержка 16
— правила 29, 75, 117
— — изменение 117
— — настройка 118
— — порядок выполнения 120
— — **применение** 123
— — создание 117, 125

— правило 101
— создание определения 112
псевдоним 235, 238, 244
публикация серверов 184

Р

редиректор HTTP 7

С

сайт 214
сервер
— изолированный 223
— кэширующий 3
— почтовый 196
— удаленного доступа 40
—изолированный 214
сеть
— виртуальная частная 17, 41
— глобальная 40
— корпоративная 227
- локальная 18, 40, 69, 184, 191
— настройка 225
— периметра 44, 137
— — с одним ISA-сервером с тремя адаптерами 45
— — со сдвоенными ISA-серверами 44
— телефонная 236
служба
- ILS (Internet Locator Service) 250
— NLB 7
— Routing and **Remote** Access 331
— SMTP 198
— — конфигурирование 198
— загрузка содержимого по расписанию 23
смещанный режим 2, 3, 180
создание Web-узела 194
сопряжение 190, 195

Т

таблица
— локальных адресов 33, 47
— маршрутизации 53
телефонная линия 78, 292
телефонные номера 245
трассировка сетевой активности 324

У

узел управления многосторонней связью 234
упорядоченный список правил 249
устранение неполадок 88, 92, 94
участник конференции 234

Ф

фактическая пропускная способность 292
фильтрация 197,207
— IP-фрагментов 141
— параметров протокола IP 141
фильтр-пере направите ль 154
фильтр
— H.323 16
- RPC 15
-SMTP 15
- SOCKS 15
— доступа по протоколу FTP 15
— обнаружения атак на DNS 16
— потоковые мультимедийные данные 16
— протокол POP 16
— редиректор HTTP 15
фильтры IP-пакетов 137, 183, 184, 192, 197
— блокирующие 137
— для Web-содержимого (HTTP) 145
— для входящей почты 142
— для исходяшей почты 143
— для протокола NNTP 144
— настройка
— — для локального компьютера 140
— — для удаленного компьютера 140
— — параметров 140
— — протокола 139
— применение к серверу 139
— разрешающие 137
— создание 137, 138

Ц

цепочка *см.* иерархия
циклическое обслуживание 219

Ч

частные IP-адреса 52
член массива
— порядок настройки параметров 215

Ш

шлюз 220

Э

экранированная подсеть 44, 137

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ MICROSOFT

прилагаемый к книге компакт-диск

ЭТО ВАЖНО — ПРОЧИТАЙТЕ ВНИМАТЕЛЬНО. Настоящее лицензионное соглашение (далее «Соглашение») является юридическим документом, оно заключается между Вами (физическим или юридическим лицом) и Microsoft Corporation (далее «корпорация Microsoft») на указанный выше продукт Microsoft, который включает программное обеспечение и может включать сопутствующие мультимедийные и печатные материалы, а также электронную документацию (далее «Программный Продукт»). Любой компонент, входящий в Программный Продукт, который сопровождается отдельным Соглашением, подпадает под действие именно того Соглашения, а не условий, изложенных ниже. Установка, копирование или иное использование данного Программного Продукта означает принятие Вами данного Соглашения. Если Вы не принимаете его условия, то не имеете права устанавливать, копировать или как-то иначе использовать этот Программный Продукт.

ЛИЦЕНЗИЯ НА ПРОГРАММНЫЙ ПРОДУКТ

Программный Продукт защищен законами Соединенных Штатов по авторскому праву и международными договорами по авторскому праву, а также другими законами и договорами по правам на интеллектуальную собственность.

1. ОБЪЕМ ЛИЦЕНЗИИ. Настоящее Соглашение дает Вам право:
   a) Программный продукт. Вы можете установить и использовать одну копию Программного Продукта на одном компьютере. Основной пользователь компьютера, на котором установлен данный Программный Продукт, может сделать только для себя вторую копию и использовать ее на портативном компьютере.
   b) Хранение или использование в сета. Вы можете также скопировать или установить экземпляр Программного Продукта на устройстве хранения, например на сетевом сервере, исключительно для установки или запуска данного Программного Продукта на других компьютерах в своей внутренней сети, но тогда Вы должны приобрести лицензии на каждый такой компьютер. Лицензию на данный Программный продукт нельзя использовать совместно или одновременно на других компьютерах.
   c) License Pak. Если Вы купили эту лицензию в составе Microsoft License Pak, можете сделать ряд дополнительных копий программного обеспечения, входящего в данный Программный Продукт, и использовать каждую копию так, как было описано выше. Кроме того, Вы получаете право сделать соответствующее число вторичных копий для портативного компьютера в целях, также оговоренных выше.
   d) Примеры кода. Это относится исключительно к отдельным частям Программного Продукта, заявленным как примеры кода (далее «Примеры»), если таковые входят в состав Программного Продукта.
      i) Использование и модификация. Microsoft дает Вам право использовать и модифицировать исходный код Примеров при условии соблюдения пункта (d)(iii) ниже. Вы не имеете права распространять в виде исходного кода ни Примеры, ни их модифицированную версию.
      ii) Распространяемые файлы. При соблюдении пункта (d)(iii) Microsoft дает Вам право на свободное от отчислений копирование и распространение в виде объектного кода Примеров или их модифицированной версии, кроме тех частей (или их модифицированных версий), которые оговорены в файле Readme, относящемся к данному Программному Продукту, как не подлежащие распространению.
      Mi) Требования к распространению файлов. Вы можете распространять файлы, разрешенные к распространению, при условии, что: а) распространяете их в виде объектного кода только в сочетании со своим приложением и как его часть; б) не используете название, эмблему или товарные знаки Microsoft для продвижения своего приложения; в) включаете имеющуюся в Программном Продукте ссылку на авторские права в состав этикетки и заставки своего приложения; г) согласны освободить от ответственности и взять на себя защиту корпорации Microsoft от любых претензий или преследований по закону, включая судебные издержки, если таковые возникнут в результате использования или распространения Вашего приложения; и д) не допускаете дальнейшего распространения конечным пользователем своего приложения. По поводу отчислений и других условий лицензии применительно к иным видам использования или распространения распространяемых файлов обращайтесь в Microsoft.

2. ПРОЧИЕ ПРАВА И ОГРАНИЧЕНИЯ
   - Ограничения на реконструкцию, декомпиляцию и дезассемблирование. Вы не имеете права реконструировать, декомпилировать или дизассемблировать данный Программный Продукт, кроме того случая, когда такая деятельность (только в той мере, которая необходима) явно разрешается соответствующим законом, несмотря на это ограничение.

- **Разделение компонентов.** Данный Программный Продукт лицензируется как единый продукт. Его компоненты нельзя отделять друг от друга для использования более чем на одном компьютере.
- **Аренда. Данный** Программный Продукт нельзя сдавать в прокат, передавать во временное пользование или уступать для **использования** в иных целях.
- **Услуги по технической поддержке.** Microsoft может (но не обязана) предоставить Вам услуги по **технической** поддержке данного Программного Продукта (далее «Услуги»). Предоставление Услуг регулируется соответствующими правилами и программами Microsoft, описанными в руководстве пользователя, электронной документации и/или других материалах, публикуемых Microsoft. Любой дополнительный программный код, предоставленный в рамках Услуг, следует считать частью данного Программного Продукта и подпадающим под действие настоящего Соглашения. Что касается технической информации, предоставляемой Вами корпорации Microsoft при использовании ее Услуг, то Microsoft **может** задействовать эту информацию в деловых целях, в том числе для технической поддержки продукта и разработки. Используя такую техническую информацию, Microsoft не будет ссылаться на **Вас.**
- **Передача прав на программное обеспечение.** Вы можете безвозвратно уступить все права, регулируемые настоящим Соглашением, при условии, что не оставите себе никаких копий, передадите все составные части данного Программного Продукта (включая компоненты, мультимедийные и печатные материалы, любые обновления, Соглашение и сертификат подлинности, если таковой **имеется) и** принимающая сторона согласится с условиями настоящего **Соглашения.**
- **Прекращение действия Соглашения.** Без ущерба для любых других прав Microsoft может прекратить действие настоящего Соглашения, если Вы нарушите его условия. В этом случае Вы должны будете уничтожить все **копии** данного **Программного** Продукта вместе со всеми его компонентами.

3. **АВТОРСКОЕ ПРАВО.** Все авторские права и право **собственности на Программный** Продукт (в том числе любые изображения, фотографии, анимации, видео, аудио, музыку, текст, **примеры** кода, распространяемые файлы и апплеты, **включенные** в состав Программного Продукта) и любые его копии принадлежат корпорации Microsoft или ее поставщикам. Программный Продукт охраняется законодательством об авторских правах и положениями международных договоров. Таким образом, Вы должны обращаться с данным **Программным** Продуктом, как с любым другим материалом, охраняемым авторскими правами, **с тем исключением**, что **Вы** можете установить **Программный Продукт** на один компьютер при **условии,** что храните оригинал исключительно как резервную или архивную копию. Копирование печатных материалов, поставляемых вместе с Программным Продуктом, запрещается

ОГРАНИЧЕНИЕ ГАРАНТИИ

ДАННЫЙ ПРОГРАММНЫЙ ПРОДУКТ (ВКЛЮЧАЯ ИНСТРУКЦИИ ПО ЕГО ИСПОЛЬЗОВАНИЮ) ПРЕДОСТАВЛЯЕТСЯ БЕЗ КАКОЙ-ЛИБО ГАРАНТИИ. КОРПОРАЦИЯ MICROSOFT СНИМАЕТ С СЕБЯ ЛЮБУЮ ВОЗМОЖНУЮ ОТВЕТСТВЕННОСТЬ, В ТОМ ЧИСЛЕ ОТВЕТСТВЕННОСТЬ ЗА КОММЕРЧЕСКУЮ ЦЕННОСТЬ ИЛИ СООТВЕТСТВИЕ ОПРЕДЕЛЕННЫМ ЦЕЛЯМ. ВЕСЬ РИСК ПО ИСПОЛЬЗОВАНИЮ ИЛИ РАБОТЕ С ПРОГРАММНЫМ ПРОДУКТОМ ЛОЖИТСЯ НА ВАС.

НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ КОРПОРАЦИЯ MICROSOFT, ЕЕ РАЗРАБОТЧИКИ, А ТАКЖЕ ВСЕ, ЗАНЯТЫЕ В СОЗДАНИИ, ПРОИЗВОДСТВЕ И РАСПРОСТРАНЕНИИ ДАННОГО ПРОГРАММНОГО ПРОДУКТА, НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КАКОЙ-ЛИБО УЩЕРБ (ВКЛЮЧАЯ ВСЕ, БЕЗ ИСКЛЮЧЕНИЯ. СЛУЧАИ УПУЩЕННОЙ ВЫГОДЫ, НАРУШЕНИЯ ХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ, ПОТЕРИ ИНФОРМАЦИИ ИЛИ ДРУГИХ УБЫТКОВ) ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ИЛИ НЕВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ДАННОГО ПРОГРАММНОГО ПРОДУКТА ИЛИ ДОКУМЕНТАЦИИ. ДАЖЕ ЕСЛИ КОРПОРАЦИЯ MICROSOFT БЫЛА ИЗВЕЩЕНА О ВОЗМОЖНОСТИ ТАКИХ ПОТЕРЬ, ТАК КАК В НЕКОТОРЫХ СТРАНАХ НЕ РАЗРЕШЕНО ИСКЛЮЧЕНИЕ ИЛИ ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ ЗА НЕПРЕДНАМЕРЕННЫЙ УЩЕРБ, УКАЗАННОЕ ОГРАНИЧЕНИЕ МОЖЕТ ВАС НЕ КОСНУТЬСЯ.

РАЗНОЕ

Настоящее Соглашение регулируется законодательством штата **Вашингтон (США),** кроме случаев (и **лишь** в той мере, насколько это необходимо) исключительной юрисдикции того государства, **на территории** которого используется Программный Продукт.

Если у **Вас** возникли **какие-либо** вопросы, касающиеся настоящего **Соглашения, или** если **Вы желаете связаться** с Microsoft по любой другой причине, пожалуйста, обращайтесь в местное представительство Microsoft или пишите по адресу: Microsoft Sales Information Center, One Microsoft Way, Redmond, WA 98052-6399.

Microsoft Corporation

Microsoft Internet Security and Acceleration Server 2000

Учебный курс MCSA/MCSE

Издание 2-е, исправленное

Перевод с английского под общей редакцией **А. Р. Врублевского**

Редакторы **Ю. П. Леонова, С. В. Дергачев**

Компьютерная верстка Е. **В. Козлова**

Технический редактор **О. В. Дергачева**

ParaType TypeMarketFontLibrary легальный пользователь

Оригинал-макет выполнен с использованием издательской системы Adobe PageMaker 6.0

Главный редактор А. **И. Козлов**

Подготовлено к печати издательством «Русская Редакция»
e-mail: info@rusedit.ru, http:// www.rusedit.ru

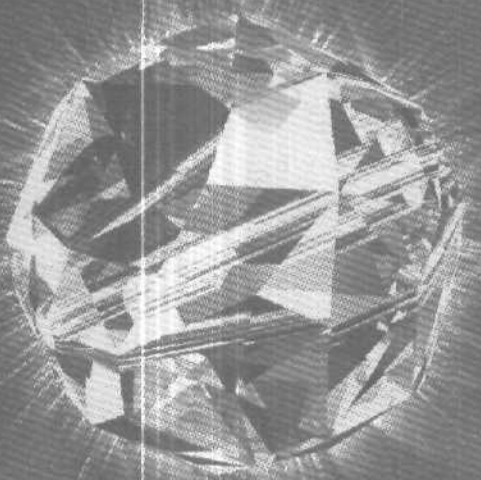
РУССКАЯ РЕДАКЦИЯ

Подписано в печать 11.11.2003 г. Тираж 2500 экз.
Формат 70x100/16. Физ. п. л. 25

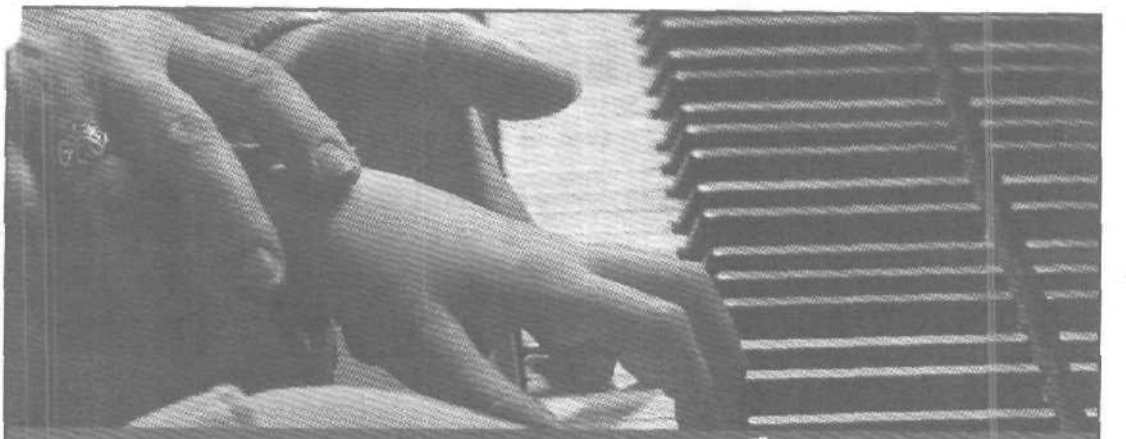
Отпечатано в ОАО «Типография "Новости"»
105005, Москва, ул. Фр. Энгельса, 46

HARD'n'SOFT

www.hardnsoft.ru



МНОГОГРАННЫЙ
КОМПЬЮТЕРНЫЙ
ЖУРНАЛ



непрерывное обучение

как повысить отдачу от вложений в информационную инфраструктуру компании?

обучить специалистов в учебном центре softline®!

Даже грамотный специалист, занятый текущей работой, не в состоянии самостоятельно повышать свою квалификацию. Для этого у него нет ни времени, ни методических материалов. Только авторизованное обучение под руководством опытного инструктора позволяет эффективно на 100% использовать все возможности как IT-инфраструктуры, так и персонала компании.

Непрерывное обучение. Информационные технологии быстро меняются. Так же бысгро устаревают знании сотрудников. Мы предлагаем экономичный и эффективный способ непрерывного обучения. Мы готовы разработать корпоративную программу обучения специальнодля сотрудников вашей компании.

Широкий набор курсов для профессионалов в области IT, которые хотят повысить свой уровень. Большое внимание уделяется вопросам построения правильной IT-инфраструктуры современной компании - вопросам безопасности, защиты данных, резервному копированию, администрированию сети и др.

Авторизованное обучение. SoftLine® является авторизованным учебным центром компаний Microsoft, Symantec, Citrix, VERITAS, и др.

Высокое качество обучения. Обучение ведут сертифицированные преподаватели по официальным методическим материалам. Высокое качество обучения подтверждается откликами крупнейших компаний, входящих в ТОП 100 Российского рынка.

Корпоративные программы обучения. SoftLine® ориентируется на долгосрочные отношения с корпоративными клиентами. Мы предлагаем разработку непрерывной программы обучения сотрудников, которая позволит экономить ресурсы, выделяемые на обучение.

Обратитесь к консультантам учебного центра **Анне Дмитраковой** иди **Нине Доминго по тел.: +7 (095) 232-0023 и закажите бесплатный каталог учебных курсов.**

Citrix · Microsoft CERTIFIED · VERITAS · symantec. · softline®

программное обеспечение - лицензирование, обучение, консалтинг

+7 (095) 232-0023 www.softline.ru

©2003 SoftLine Int. Все правазащищены. SoftLine, логотип SoftLine являются тортовым марками SoftLine tat и зарегистрированы в России и других странах.
Другие компании и названия продуктов являются торговыми марками, представленными их владельцами.

Оперативная информация
для профессионалов в журнале «MSDN Magazine/Русская Редакция»

Своей *популярностью этот* журнал обязан содержанию: *читатель* получает самую свежую *и* актуальную *информацию как от ведущих разработчиков* корпорации Microsoft, так *и от* известных специалистов в сфере *разработки* приложений. Глубокие *и* содержательные статьи *оказывают* неоценимую помощь профессиональному *разработчику,* регулярно *использующему* средства разработки *Microsoft.*

Из статьи Ольги Деруновой, главы представительства Microsoft в СНГ *(MSDN Magazine/Русская Редакция, спецвыпуск* № 1, *апрель 2002 г.)*

Журнал содержит:

постоянные рубрики

Web: вопросы и ответы — вопросы и ответы, связанные с Web-разработкой.

XML — основные спецификации XML (XML Schema, пространство имен VS-Security), Web-сервисы и т. д.). Ответы на вопросы читателей.

ASP — все аспекты программирования с использованием ASP и ASP.NET.

Доступ к данным — проблемы разработки эффективных приложений для взаимодействия с СУБД, повышение производительности и обеспечение безопасности, а также программирование с использованием ADO.NET.

На переднем крае — передовые технологии разработки (SOAP, Web-сервисы, .NET Framework и др.)

.NET — Джеффри Рихтер об основных концепциях и понятиях .NET и о приемах программирования.

Основы и тонкости — актуальные проблемы программирования, интересующие в основном начинающих программистов.

Отладка и оптимизация — эффективные приемы и подходы к решению задач отладки и оптимизации приложений.

Под капотом — особенности функционирования системных компонентов и исполняющих сред, создание эффективного программного обеспечения. Для системных программистов и разработчиков.

Изощренный код — необычные приемы, трюки программирования. Для системных программистов и разработчиков.

C++: вопросы и ответы — вопросы и ответы, связанные с программированием на языке C++.

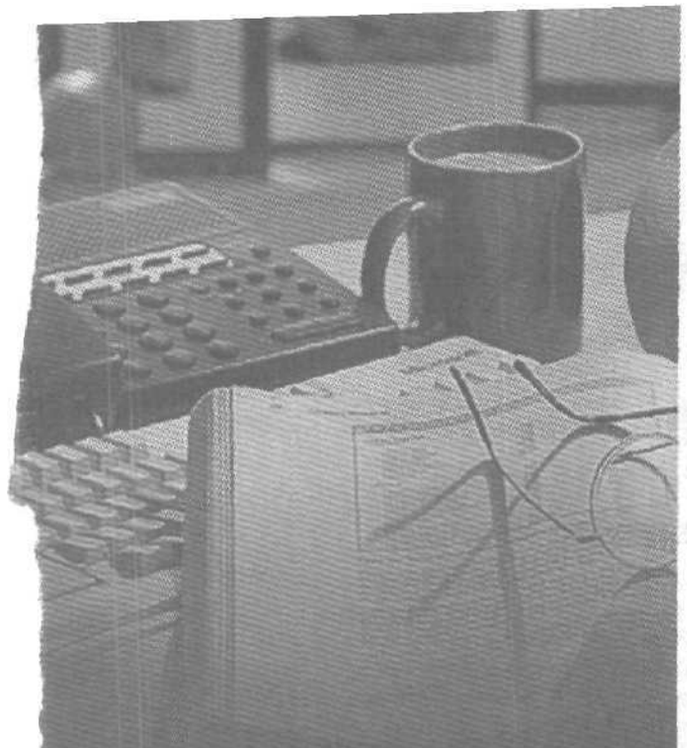
тематические статьи

— глубоко и подробно раскрывают проблемы разработки ПО.

Информационная поддержка журнала «MSDN Magazine/Русская Редакция» — www.microsoft.com/rus/msdn/magazine

Оформить подписку и приобрести журнал **можно** в Интернет-магазине

www.ITbook.ru



Издательство «Русская Редакция» — партнер Microsoft Press в России — предлагает широкий выбор литературы по современным информационным технологиям.

РУССКАЯ РЕДАКЦИЯ

тел.: (095) 256-5120; тел./факс: (095) 256-4541;
e-mail: info@rusedit.ru; http://www.rusedit.ru

Наши книги Вы можете приобрести

• • Москве:

Специализированный магазин «Компьютерная и деловая книга»
Ленинский проспект, строение 38,
тел.: (095) 778-7269

«Библио-Глобус» ул. Мясницкая, 6,
тел.: (095) 928-3567

«Московский дом книги» ул. Новый Арбат, 8,
тел.: (095) 290-4507

«Дом технической книги» Ленинский пр-т, 40,
тел.: (095) 137-0633

«Молодая **гвардия»** ул. Большая Полянка, 28,
тел.: (095) 238-5001

«Дом книги **на Соколе»** Ленинградский пр-т, 78,
тел.: (095) 152-4511

«Дом книги на **Войковской»** Ленинградское ш.. 13, стр. 1.
тел.: (095) 150-6917

"Мир **печати»** ул. 2-я Тверская-Ямская, 54,
тел.: (095) 978-5047

Торговый **дом книги «Москва»** ул. Тверская, S,
тел.: (095) 229-6483

• • Санкт-Петербурге:

СПб Дом книги, Невский пр-т., 28
тел.: (812) 318-6402

СПб Дом военной книги, Невский пр-т., 20
тел.: (812) 312-0563, 314-7184

Магазин «Подписные издания»,
Литейный пр-т., 57, тел.: (812) 273-5053

Магазин «Техническая книга», ул. Пушкинская, 2,
тел.: (812) 164-6565, 164-1413

Магазин «Буквоед», Невский пр-т., 13,
тел.: (812) 312-6734

ЗАО «Торговый Дом «Диалект»,
тел.: (812) 247-1483

Оптово-розничный магазин «Наука и **техника»**,
тел.: (812) 567-7025

• в Екатеринбурге:

Книготорговая компания «Дом книги»,
ул. Антона Валека, 12.
тел.: (3432) 59-4200. 59-4898

• в Великом Новгороде:

«Наука и **техника»**,
ул. Большая Санкт-Петербургская, 44,
Дворец Молодежи, 2-й этаж

• • Новосибирске:

ООО «Топ-книга», тел.: (3832) 36-1026

• в Алматы (Казахстан):

ЧП Болат Амреев,
моб. тел.: 8-327-908-28-57, (3272) 76-1404

• в Киеве (Украина):

ООО Издательство «Ирина-Пресс»,
тал/ (+1038044) 269-0423

«Техническая книга на Петровке»,
тел.: (+1038044) 268-5346

конкурс
«Читатель месяца»

Хотите сэкономить на обучении до $1000?

Издательство «Русская Редакция» и учебный центр компании «Инвента» проводят конкурс «Читатель месяца» и будут ежемесячно выбирать двух самых активных читателей книг серии «Учебный курс».

Просто вырежьте купон из книги, помеченной на обложке специальным значком «Читатель месяца», и пришлите нам по адресу: ***123317, Россия,* г. Москва, ул. *Антонова-Овсеенко,* д. 13. Издательство «Русская Редакция».**

Лотерея определит победителей месяца. Один купон — один голос!
Чем больше купонов вы пришлете, тем больше у вас шансов выиграть!

Призы победителям — *бесплатное* обучение в учебном центре «Инвента» в Москве!

Но это не все! Помимо выбранного вами курса по программе сертификации Microsoft, победителей ждут и другие призы — скидка на дальнейшее обучение в учебном центре и подарок от «Русской Редакции».

Подробности конкурса — на сайте издательства "Русская Редакция» (*www.rusedit.ru/bonus*) и на сайте компании «Инвента» (*www.inventa.ru*). Там же все новости о конкурсе и о победителях. Телефон для справок (095) 775-8777

КОНКУРС

Купон участника конкурса «Читатель месяца»

РУССКАЯ РЕДАКЦИЯ ***ИНВЕНТА***

Ф. И. О.:	
E-mail:	
Телефон:	
Род занятий:	

ВНИМАНИЕ! Незаполненные купоны не принимаются.

Конкурс проводится исключительно *за* счет *устроителей* и *данный купон* не может *рассматриваться как* коммерческое *предложение.*

Купон из книги **Проектирование и реализация баз данных SQL Server 2000. Учебный Курс *MCAD/MCSE/MSDBA*** ISBN 5-7502-0181-3