А.М. Голиков

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МЕТОДИКИ ВНЕДРЕНИЯ И АДМИНИСТРИРОВАНИЯ ВСТРОЕННЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ MICROSOFT ISA SECURITY 2004 (MICROSOFT INTERNET SECURITY AND ACCELERATION SERVER) УСТАНОВКА И КОНФИГУРИРОВАНИЕ БРАНДМАУЭРА ISA

Методические указания по лабораторной работе по курсу «Основы технической эксплуатации защищенных телекоммуникационных систем» для студентов специальности

090106 «Информационная безопасность

телекоммуникационных систем» и

Томск – 2009

Исследование и администрирование средств обеспечения информационной безопасности Microsoft ISA Security Server. Установка и конфигурирование брандмауэра ISA

1 Задачи и анализ действий перед установкой брандмауэра ISA

Прежде чем устанавливать программное обеспечение брандмауэра ISA, нужно рассмотреть несколько ключевых моментов:

- системные требования;
- настройка таблицы маршрутизации;
- размещение DNS-сервера;
- конфигурирование сетевых интерфейсов брандмауэра ISA;
- автоматизированная установка;
- установка с помощью режима администрирования службы терминалов.

1.1 Системные требования

Компьютер, на котором будет установлено программное обеспечение брандмауэра ISA, должен удовлетворять следующим требованиям:

- процессор Intel или AMD с частотой 550 МГц и выше;
- операционная система Windows 2000 или Windows Server 2003;
- минимум 256 Мб памяти; минимум 512 Мб памяти для систем без функции Web-кэширования и 1 000 Мб памяти для брандмауэра ISA с Web-кэшированием;
- хотя бы один сетевой адаптер; два и более сетевых адаптера необходимы для обеспечения функций фильтрации с отслеживанием соединений и проверки на уровне приложения с отслеживанием соединений;
- дополнительный сетевой адаптер для каждой сети, соединенной с компьютером ISA Server;
- один локальный жесткий диск, отформатированный с файловой системой NTFS, и хотя бы 150 Мб свободного пространства на жестком диске (за вычетом пространства на жестком диске, предназначенного для кэширования);
- дополнительное пространство на диске; в идеале, на отдельном;
- дополнительное свободное пространство на диске; *в* идеале, отдельный диск, если планируется использовать функцию Web-кэширования брандмауэра ISA.

Еще одним важным вопросом является планирование ресурсов. Приведенный ранее список отражает минимальные системные требования для установки и запуска программного обеспечения брандмауэра ISA, идеальную конфигурацию можно получить, соразмеряя возможности аппаратного обеспечения для оптимизации производительности программного обеспечения брандмауэра ISA на конкретном компьютере. В табл. 1 представлены основные требования при выборе процессора, памяти, емкости жесткого диска и сетевого адаптера на основании скорости канала связи с Интернетом.

Табл.1. Основные требования к процессору, памяти, емкости жесткого диска и сетевому адаптеру в зависимости от скорости канала связи с Интернетом

Скорость канала связи с Интернетом	До 7,5 Мбит/с	До 25 Мбит/с	До 45 Мбит/с	Примечания
Количество процессоров	1	1	2	
Тип процессора	Pentium III 550 МГц (и	Pentium IV с частотой 2,0	Xeon с частотой 2,0 –	В реализациях, требующих только

	больше)	– 3,0 ГГц	3,0 ГГц	фильтрации с отслеживанием соединений («проверка с отслеживанием соединений» означает, что не нужно обеспечивать более безопасную проверку с отслеживанием соединений на уровне приложения), использование процессоров Pentium IV и Хеоп позволяет достичь скорости кабельных ЛВС
Скорость канала связи с Интернетом	До 7,5 Мбит/с	До 25 Мбит/с	До 45 Мбит/с	Примечания
Память	256 Мб	512 Мб	1 Гб	При включенном режиме Web-кэширования указанный объем памяти нужно увеличить примерно на 256-512 Мб
Свободное пространство на жестком диске	150Мб	2,5 Гб	5 Гб	Сюда не включается пространство жесткого диска, необходимое для кэширования и ведения журналов
Сетевой адаптер	10/100 Мбит/с	10/100 Мбит/с	100/1000 Мбит/с	Это требования для сетевых адаптеров, не подключенных к Интернету
Одновременные VPN-подключения удаленного доступа	150	700	850	Standart Edition брандмауэра ISA поддерживает жестко запрограммированный максимум в 1000 одновременных VPN-подключений. Enterprise Edition поддерживает столько подключений, сколько поддерживает базовая операционная система, и не имеет жестко закодированных ограничений

1.2 Настройка таблицы маршрутизации

Таблица маршрутизации на компьютере брандмауэра ISA должна быть настроена до установки программного обеспечения брандмауэра ISA. Таблица маршрутизации должна включать маршруты ко всем сетям, которые не являются локальными для сетевых интерфейсов брандмауэра ISA. Эти записи в таблице маршрутизации необходимы, потому что у брандмауэра ISA может быть только один основной шлюз. Обычно основной шлюз настроен на сетевом интерфейсе, используемом для внешней сети. Поэтому, если имеется внутренняя сеть или другая сеть, содержащая несколько дочерних сетей, нужно настроить записи в таблице маршрутизации так, чтобы брандмауэр ISA мог взаимодействовать с компьютерами и другими устройствами в соответствующих дочерних сетях. Сетевой интерфейс с основным шлюзом используется для соединения с Интернетом напрямую или с помощью вышестоящих маршрутизаторов.

Записи в таблице маршрутизации являются критически важными для поддержки конфигураций брандмауэра ISA «сеть-в-Сети», которые представляют собой идентификатор сети, расположенной «за» сетевой интерфейсной картой брандмауэра ISA, т. е. не в локальной сети.

Например, на рис. 1 представлен образец простой конфигурации «сеть-в-Сети».

В этой схеме IP-адресов небольшой организации используется два идентификатора сети: 192.168.1.0/24 и 192.168.2.0/24. Сеть, локальная по отношению к внутреннему интерфейсу брандмауэра ISA, имеет идентификатор сети 192.168.1.0/24. Сеть, удаленная от внутреннего интерфейса брандмауэра ISA, — 192.168.2.0/24. Маршрутизатор корпоративной сети разделяет сеть и маршрутизирует пакеты между этими двумя идентификаторами сети.

Рисунок 1. Сеть в Сети

Сетевая модель брандмауэра ISA включает обе эти сети как часть одной Сети («Сеть» с заглавной буквы означает сеть, определенную на брандмауэре ISA). Можно предположить, что 192.168.1.0/24 является Сетью, определенной на брандмауэре ISA, потому что она включает в себя весь идентификатор сети, но также можно предположить, что идентификатор сети 192.168.2.0/24 определяется как вторая Сеть, определенная на брандмауэре ISA. Однако это неверно, потому что сетевая модель брандмауэра ISA включает все сети *(все* IP-адреса), доступные с конкретного интерфейса брандмауэра ISA, как часть одной и той же сети.

Это объясняется тем, что хосты в одной определенной на брандмауэре ISA Сети не используют брандмауэр ISA для взаимодействия между собой. Брандмауэр ISA не выступает в качестве посредника при взаимодействии между хостами с идентификаторами сети 192.168.1.0/24 и 192.168.2.0/24, потому что в этом случае хосты будут использовать брандмауэр для получения доступа к хостам, с которыми они могут взаимодействовать напрямую.

В этом примере должна быть запись в таблице маршрутизации на брандмауэре ISA, указывающая, что для получения доступа к идентификатору сети 192.168.2.0/24, соединение должно быть перенаправлено на IP-адрес 192.168.2.1 на корпоративном маршрутизаторе. Можно использовать консоль RRAS (Routing and Remote Access Service, служба маршрутизации и удаленного доступа) или команды ROUTE и netsh в командной строке для добавления записи в таблицу маршрутизации.

Брандмауэр ISA должен знать маршрут к каждому внутреннему идентификатору сети. Если окажется, что соединения направляются через брандмауэр ISA к хостам в корпоративной сети неправильно, нужно проверить записи в таблице маршрутизации на брандмауэре ISA: они должны указывать правильный шлюз для каждого из этих идентификаторов сети.

Можно существенно упростить определения сетей и таблицу маршрутизации брандмауэра ISA, создав корректную инфраструктуру IP-адресации с дочерними сетями, что позволит суммировать маршруты.

1.3 Размещение DNS-сервера

Чаще всего проблемы соединения с брандмауэром ISA связаны с DNS-сервером и разрешением имени хоста. Если инфраструктура разрешения имен в организации настроена неправильно, то одним из первых от неправильного разрешения имен пострадает брандмауэр ISA.

Брандмауэр ISA должен правильно разрешать как корпоративные DNS-имена, так и имена из Интернета. Брандмауэр ISA выполняет разрешение имен для клиентов Web-прокси и для клиентов брандмауэра. Если брандмауэр не может правильно выполнять разрешение имен, то клиентам Web-прокси и клиентам брандмауэра не удастся установить соединение с Интернетом.

Правильное разрешение имен для ресурсов корпоративной сети также является критически важным, потому что брандмауэр ISA должен правильно разрешать имена для ресурсов корпоративной сети, опубликованных по правилам Web-публикации.

Например, при создании правила Web-публикации по протоколу SSL брандмауэр ISA должен правильно перенаправлять входящие запросы на соединение на FQDN-имя (Fully Qualified Domain Name, полное имя домена), используемое для обычного имени на сертификате Web-сайта, связанного с опубликованным Web-сервером в корпоративной сети.

Идеальной инфраструктурой разрешения имен является расщепленная DNS, позволяющая внешним хостам разрешать имена в общедоступные адреса, а хостам корпоративной сети разрешать имена в частные адреса. На рис. 2 показано, как действует расщепленная инфраструктура DNS при разрешении имен для хостов в корпоративной сети, а также хостов, «блуждающих» между корпоративной сетью и удаленными узлами в Интернете.

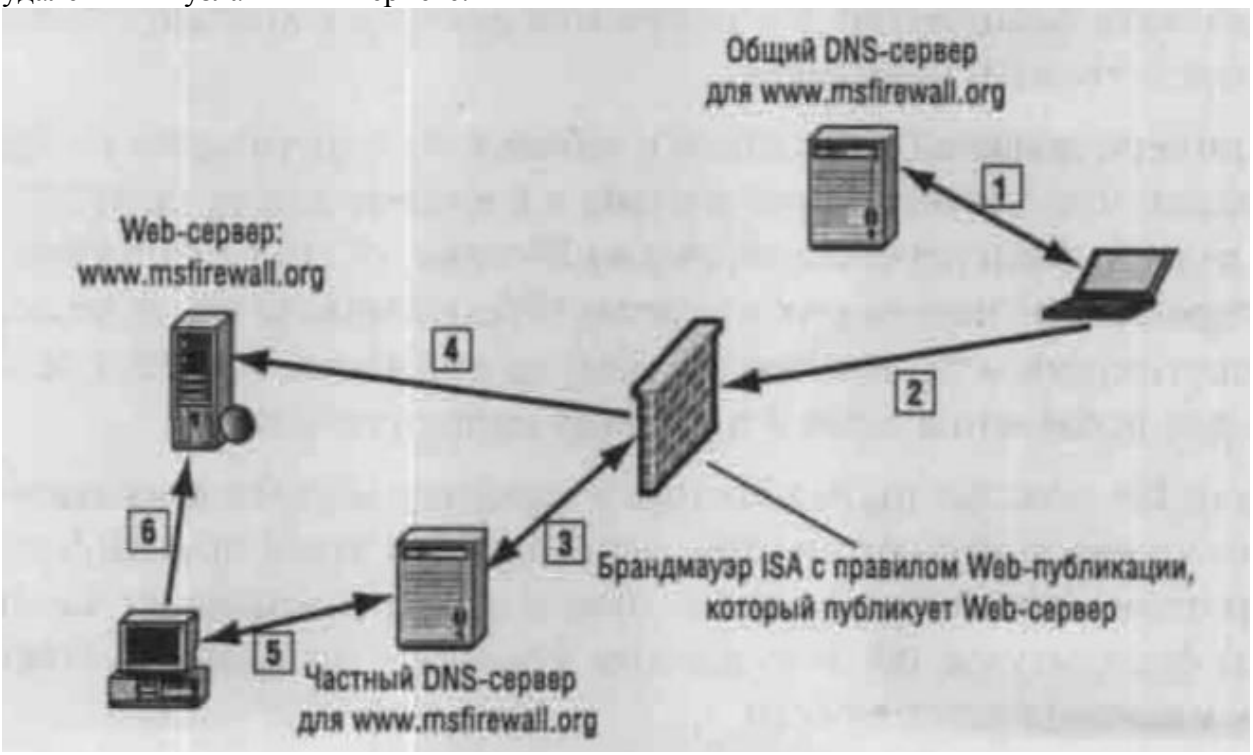

Рисунок 2. Работа расщепленной инфраструктуры DNS

1. Удаленному пользователю нужно получить доступ к ресурсам на корпоративном Web-сервере www.msfirewall.org, который обслуживается в Сети под защитой брандмауэра ISA и опубликован с помощью правила Web-публикации брандмауэра ISA. Удаленный пользователь отправляет запрос на www.msfirewall.org, и общий DNS-сервер, отвечающий за этот домен, выполняет разрешение имени в IP-адрес на внешнем интерфейсе брандмауэра ISA с помощью Web-приемника, указанного в правиле Web-публикации.
2. Удаленный Web-клиент отправляет запрос на IP-адрес на внешнем интерфейсе, используемом Web-приемником для правил Web-публикации.
3. Брандмауэр ISA разрешает имя www.msfirewall.org в реальный IP-адрес, связанный с Web-сайтом www. msfirewall.org в корпоративной сети, отсылая запрос на DNS-сервер внутренней сети, отвечающий за домен msfirewall.org.
4. Брандмауэр ISA перенаправляет соединение на реальный IP-адрес, связанный с Web-сайтом www.msfirewall.org в корпоративной сети.
5. Хосту в корпоративной сети нужно получить доступ к ресурсам на Web-сайте www.msfirewall.org. Пользователь корпоративной сети отправляет запрос на корпоративный DNS-сервер, отвечающий за домен msfirewall.org. Корпоративный DNS-сервер разрешает имя www.msfirewall.org в реальный IP-адрес, связанный с Web-сайтом www.msfirewall.org в корпоративной сети.

6. Web-клиент в корпоративной сети устанавливает прямое соединение с Web-сервером www.msfirewall.org. Web-клиент не выполняет замыкание через брандмауэр ISA для получения доступа к Web-сайту www.msfirewall.org в корпоративной сети, потому что клиенты Web-прокси настроены на прямой доступ к ресурсам в домене msfirewall.org.

Расщепленная инфраструктура DNS обеспечивает прозрачный доступ для пользователей независимо от того, где они находятся. Пользователи могут перемещаться между корпоративной сетью и удаленными узлами и использовать одно и то же имя для доступа к корпоративным ресурсам. Им не нужно менять настройки своих почтовых клиентов, новостных клиентов и других приложений, потому что для доступа к ресурсам используется одно и то же имя независимо от их местоположения. В любой организации, которой нужно обеспечить поддержку пользователей, «блуждающих» между корпоративной сетью и удаленными узлами, должна использоваться расщепленная инфраструктура DNS.

Требования к расщепленной инфраструктуре DNS включают в себя:

- DNS-сервер, отвечающий за домен, который разрешает имена для ресурсов этого домена во внутренние адреса, используемые для доступа к этим ресурсам;
- DNS-сервер, отвечающий за домен, который разрешает имена для ресурсов в этом домене в общие адреса, используемые для доступа к этим ресурсам;
- удаленным пользователям должны быть присвоены адреса DNS-сервера, которые перенаправляют запросы к домену на общий DNS-сервер. Это легко осуществить с помощью DHCP;
- корпоративным пользователям должны быть присвоены адреса DNS-сервера, которые перенаправляют запросы к домену на частный DNS-сервер. Это легко осуществить с помощью DHCP;
- брандмауэр ISA должен разрешать имена опубликованных ресурсов и других ресурсов Сети под защитой брандмауэра ISA в частный адрес, используемый для доступа к этому ресурсу.

В большинстве организаций, использующих брандмауэр ISA, есть один или несколько внутренних DNS-серверов. Хотя бы один из этих DNS-серверов должен быть настроен на разрешение имен внутренних хостов и хостов в Интернете, а брандмауэр ISA должен быть настроен на использование этого DNS-сервера. Если имеется DNS-сервер во внутренней сети, то не следует настраивать интерфейсы брандмауэра ISA на использование внешнего DNS-сервера. Это распространенная ошибка, которая ведет к замедлению разрешения имен или к ошибкам.

1.4 Конфигурирование сетевых интерфейсов брандмауэра ISA

Существуют два основных типа конфигурации сетевого интерфейса:

■ отлаженная инфраструктура разрешения имен в корпоративной сети под защитой брандмауэра ISA;

■ отсутствие отлаженной инфраструктуры разрешения имен в корпоративной сети под защитой брандмауэра ISA.

В табл. 2 и 3 показана правильная информация об IP-адресах для этих двух типов конфигурации для брандмауэра ISA с двумя сетевыми интерфейсами.

Табл.2. Отлаженная инфраструктура разрешения имен в корпоративной сети.

Параметры	**Внутренний интерфейс**	**Внешний интерфейс**
Клиент для сетей Microsoft Networks	Включен	Выключен
Совместное использование файлов и принтеров для Microsoft Networks	Включен, только если брандмауэр ISA поддерживает общие ресурсы для клиентов брандмауэра	Выключено

Драйвер монитора сети	Включен, если установлен монитор сети на брандмауэре ISA (рекомендуемая установка)	Включен, если установлен монитор сети на брандмауэре ISA (рекомендуемая установка)
Протокол Интернета (TCP/IP)	Включен	Включен
IP-адрес	Действительный IP-адрес в сети, к которой подключен внутренний интерфейс	Действительный IP-адрес в сети, к которой подключен внешний интерфейс, общий или частный в зависимости от сетевой инфраструктуры
Маска подсети	Действительная маска подсети в сети, к которой подключен внутренний интерфейс	Действительная маска подсети в сети, к которой подключен внешний интерфейс
Параметры	**Внутренний интерфейс**	**Внешний интерфейс**
Основной шлюз	Отсутствует. Никогда не следует настраивать основной шлюз на любом внутреннем интерфейсе или интерфейсе DMZ на брандмауэре ISA	IP-адрес вышестоящего маршрутизатора (либо в корпоративной сети, либо интернет-провайдера в зависимости от следующего перехода), обеспечивающего доступ в Интернет
Основной DNS-сервер	Внутренний DNS-сервер, который может разрешать имена хостов внутренней сети и Интернета	Отсутствует. Не указывайте адрес DNS-сервера на внешнем интерфейсе брандмауэра ISA
Альтернативный DNS-сервер	Второй внутренний DNS-сервер, который может разрешать имена хостов внутренней сети и Интернета	Отсутствует. Не указывайте адрес DNS-сервера на внешнем интерфейсе брандмауэра ISA
Регистрация адресов соединения в DNS	Отключена. Нужно вручную создавать записи на DNS-сервере во внутренней сети, чтобы разрешить клиентам разрешать имя внутреннего интерфейса брандмауэра ISA	Отключена
WINS	Введите IP-адрес еще одного DNS-сервера во внутренней сети. Особенно пригодится для VPN-клиентов, которые хотят просматривать серверы во внутренней сети с помощью NetBIOS-имени/службы браузера	Отсутствует
Настройки WINS NetBIOS	Стандартные	Отключить NetBIOS поверх TCP/IP
Порядок интерфейса	Верх списка интерфейса	Под внутренним интерфейсом

Табл. 3. Отсутствие отлаженной инфраструктуры разрешения имен в корпоративной сети.

Параметры	**Внутренний интерфейс**	**Внешний интерфейс**
Клиент для сетей Microsoft Networks	Включен	Выключен
Совместное использование файлов и принтеров для Microsoft Networks	Включен, только если брандмауэр ISA поддерживает общие ресурсы для клиентов брандмауэра	Выключено
Драйвер монитора сети	Включен, если установлен монитор сети на брандмауэре ISA (рекомендуемая установка)	Включен, если установлен монитор сети на брандмауэре ISA (рекомендуемая установка)
Протокол Интернета (TCP/IP)	Включен	Включен
IP-адрес	Действительный IP-адрес в сети, к которой подключен внутренний интерфейс	Действительный IP-адрес в сети, к которой подключен внешний интерфейс, общий или частный в зависимости от сетевой инфраструктуры. Или же DHCP, если это требование интернет-провайдера
Маска подсети	Действительная маска подсети в сети, к которой подключен внутренний	Действительная маска подсети в сети, к которой подключен внешний интерфейс.

	интерфейс	Может назначаться интернет-провайдером посредством DHCP
Основной шлюз	Отсутствует. Никогда не следует настраивать основной шлюз на любом внутреннем интерфейсе или интерфейсе DMZ на брандмауэре ISA	IP-адрес вышестоящего маршрутизатора (либо в корпоративной сети, либо интернет-провайдера в зависимости от следующего перехода), обеспечивающего доступ в Интернет. Может назначаться интернет-провайдером с помощью DHCP
Основной DNS-сервер	Внешний DNS-сервер, который может разрешать имена хостов Интернета. Обычно это DNS-сервер интернет-провайдера. Примечание: если для получения информации об IP-адресах для внешнего интерфейса используется DHCP, то не следует указывать DNS-сервер на внутреннем интерфейсе брандмауэра ISA	Отсутствует. Может быть назначен интернет-провайдером посредством DHCP
Альтернативный DNS-сервер	Второй внешний DNS-сервер, который может разрешать имена хостов Интернета. Примечание: если для получения информации об IP-адресах для внешнего интерфейса используется DHCP, то не следует указывать DNS-сервер на внутреннем интерфейсе брандмауэра ISA	Отсутствует. Не следует вводить адрес DNS-сервера на внешнем интерфейсе брандмауэра ISA за исключением случая, когда он назначен интернет-провайдером посредством DHCP
Регистрация адресов соединения в DNS	Выключен	Выключен
WINS	Отсутствует	Отсутствует
Настройки WINS NetBIOS	Стандартные	Отключить NetBIOS поверх TCP/IP
Порядок интерфейса	Верх списка интерфейса. Примечание: если для получения информации об IP-адресе для внешнего интерфейса от интернет-провайдера используется DHCP, то не нужно перемещать внутренний интерфейс вверх списка	Верх списка интерфейса при использовании DHCP-сервера интернет-провайдера для назначения адресов DNS-сервера

Важно не только уметь конфигурировать информацию об IP-адресах для интерфейсов сервера Windows, но и знать, как изменять порядок интерфейса. Порядок интерфейса необходим для того, чтобы определить предпочтительный сервер имен, адреса которого будут использоваться.

Для изменения порядка интерфейса выполните следующие действия:

1. Правой кнопкой мыши щелкните **My Network Places** (Сетевое окружение) на рабочем столе и выберите в контекстном меню пункт **Properties** (Свойства).
2. В окне **Network and Dial-up Connections** (Сетевые подключения) щелкните мышью меню **Advanced** (Дополнительно), а затем нажмите кнопку **Advanced Settings** (Дополнительные параметры).
3. В диалоговом окне **Advanced Settings** (Дополнительные параметры) (рис. 3) щелкните мышью внутренний интерфейс в списке **Connections** (Подключения) на вкладке **Adapters and Bindings** (Адаптеры и привязки). Выбрав внутренний интерфейс, щелкните мышью стрелку вверх, чтобы переместить этот внутренний интерфейс наверх списка интерфейсов.

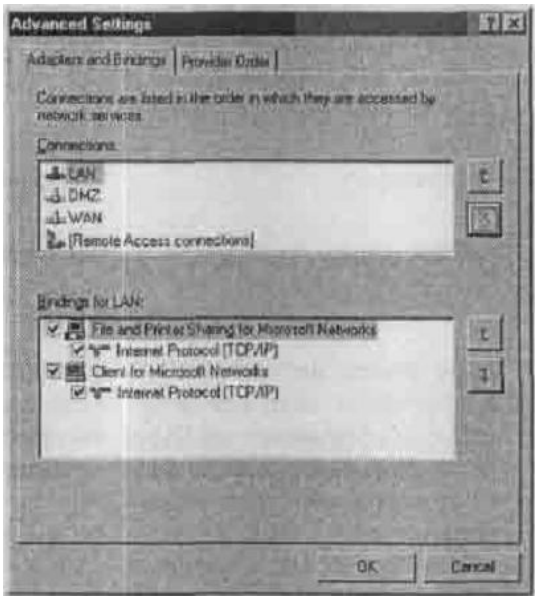

Рисунок 3. Диалоговое окно Advanced Settings (Дополнительные параметры)

4. Нажмите **кнопку OK** в диалоговом окне **Advanced Settings** (Дополнительные параметры).

2 Стандартная конфигурация брандмауэра ISA после установки

Программа установки брандмауэра ISA включает в себя настройки, которые пользователь вводит в процессе работы мастера установки. Программа установки также задает несколько стандартных настроек для полномочий пользователя (User Permissions), настроек сети (Network Settings), политики брандмауэра (Firewall Policy) и др. В табл. 4 представлены настройки, которые не задаются явно в процессе установки. Вкратце стандартную конфигурацию брандмауэра можно представить так:

- системные политики разрешают выборочный трафик с/на брандмауэр ISA;
- запрещен весь трафик через брандмауэр ISA, потому что есть только одно запрещающее правило;
- между сетями VPN/VPN-Q и внутренней сетью установлены отношения типа «маршрут»;
- между внутренней сетью и внешней сетью по умолчанию задано отношение трансляции адресов NAT;
- только администраторы могут менять политику брандмауэра ISA.

Табл. 4. Настройки брандмауэра ISA после его установки

Функция	Настройка после установки брандмауэра
Полномочия пользователя	Члены группы администраторов на локальном компьютере могут настраивать политику брандмауэра. Если брандмауэр ISA является членом домена, то администраторы домена автоматически добавляются к группе локальных администраторов
Настройки сети	Мастер установки создает следующие правила для сети (Network Rules): *Правило доступа к локальному хосту* определяет отношение маршрутизации между сетью локального хоста и другими сетями. Для разрешенных соединений с брандмауэра ISA к другим хостам задано отношение типа «маршрут» (не NAT, которое не используется между локальным хостом и другими сетями). *Правило доступа в Интернет* задает отношение NAT из внутренней сети, сети изолированных VPN-клиентов и сети VPN-клиентов во внешнюю сеть. Отношение NAT распространяется на все соединения из этих трех типов сетей к внешней сети. Доступ разрешен, только если правильно настроена соответствующая политика доступа. Правило отношения из сети VPN-клиентов во внутреннюю сеть определяет отношение типа «маршрут» между сетью VPN-клиентов и внутренней сетью. Доступ разрешен, только если разрешен доступ для VPN-клиентов

Политика брандмауэра	Стандартное правило доступа (под названием «запрещающее правило» (Default Rule)) запрещает трафик между всеми сетями
Системная политика	По умолчанию брандмауэр ISA полностью защищен. Некоторые правила системной политики включаются для того, чтобы разрешить необходимые службы. Нужно просмотреть конфигурацию системной политики и настроить ее так, чтобы были включены только наиболее важные для данной реализации функции
Создание Web-цепочек	Стандартное правило (Default Rule) определяет, что все запросы клиен тов Web-прокси обрабатываются непосредственно из Интернета. То есть по умолчанию создание Web-цепочек не задано.
Кэширование	Размер кэша установлен равным 0. Таким образом, кэширование отключено. Для включения кэширования нужно определить диск, на котором будет расположен кэш
Оповещения	Большинство оповещений включены. Нужно просмотреть и настроить оповещения в соответствии с потребностями конкретной сети
Конфигурация клиента	По умолчанию для клиентов брандмауэра и Web-прокси включено автоматическое обнаружение. Web-браузеры на клиентах брандмауэра настраиваются при установке клиента брандмауэра
Автообнаружение для клиентов брандмауэра и Web-прокси	По умолчанию публикация информации об автоматическом обнаружении отключена. Нужно включить публикацию информации об автоматическом обнаружении и подтвердить порт, на котором эта информация публикуется

3 Настройка системной политики после установки брандмауэра ISA

Политика брандмауэра ISA — набор правил, контролирующих доступ в/из сети локального хоста. Системная политика контролирует доступ в/из системы, она не настраивается для сетевого доступа между другими хостами. Одна из наиболее распространенных ошибок, совершаемых неопытными администраторами брандмауэра ISA, — использование системной политики для контроля доступа с хостов защищенной сети к хостам незащищенной сети.

В табл. 5 представлен список правил системной политики и их статуса после установки программного обеспечения брандмауэра ISA. Столбец Номер/Комментарии включает рекомендации по настройке конкретного правила системной политики.

Табл. 5. Стандартная системная политика после установки брандмауэра ISA

Номер/ Комментарии	Название	Действие	Протоколы	Источник/ Приемник	Адресат	Условие
1. Является ли брандмауэр ISA членом домена? Если нет, отключить это правило	Разрешить доступ к службам каталогов с целью проверки подлинности	Разрешить	LDAP, LDAP (UDP), LDAP GC (Global Catalog), LDAPS, LDAPS GC (Global Catalog)	Локальный хост	Внутренняя сеть	Все пользователи
2. Если удаленная MMC-оснастка для управления брандмауэром ISA не используется, отключить это правило	Разрешить удаленный доступ с выбранных компьютеров с помощью MMC-оснастки	Разрешить	Microsoft FirewallControl, дейтаграмма NetBIOS, служба имен NetBIOS, сеанс NetBIOS, RPC (все интерфейсы)	Компьютеры удаленного управления	Локальный хост	Все пользователи
3. Подтверждает, что подмножество компьютеров удаленного управления имеет адреса хостов, которые будут	Разрешает удаленное управление с выбранных компьютеров с помощью сервера терминалов	Разрешить	RDP (службы терминалов)	Компьютеры удаленного управления	Локальный хост	Все пользователи

управлять брандмауэром ISA. Чтобы не разрешать управление брандмауэром ISA по протоколу RDP, отключите это правило						
4. (По умолчанию отключено) Включите это правило, если нужно заходить на SQL-серверы	Разрешает удаленный вход на доверяемые серверы с помощью NetBIOS	Разрешить	дейтаграмма NetBIOS, служба имен NetBIOS, сеанс NetBIOS	Локальный хост	Внутренняя сеть	Все пользователи
5. Если не будет использоваться проверка подлинности с помощью RADIUS, то это правило следует отключить	Разрешить проверку подлинности RADIUS с ISA Server на доверяемые серверы RADIUS	Разрешить	RADIUS, RADIUS Accounting	Локальный хост	Внутренняя сеть	Все пользователи
Номер/ Комментарии	Название	Действие	Протоколы	Источник/ Приемник	Адресат	Условие
6. Если на брандмауэре ISA не будет проводится проверка подлинности, то отключите это правило	Разрешить проверку подлинности Kerberos с ISA Server к доверяемым серверам	Разрешить	KerberosSec (TCP), KerberosSec (UDP)	Локальный хост	Внутренняя сеть	Все пользователи
7. Это правило необходимо включить, чтобы брандмауэр ISA мог инициировать DNS-запросы	Разрешить DNS-запросы с ISA Server к выбранным серверам	Разрешить	DNS	Локальный хост	Везде	Все пользователи
8. Если брандмауэр ISA не будет выступать в роли DHCP-клиента, отключите это правило	Разрешить DHCP-запросы с ISA Server ко всем сетям	Разрешить (запрос)	DHCP	Локальный хост	Везде	Все пользователи
9. Если брандмауэр ISA не будет выступать в роли DHCP-клиента, отключите это правило	Разрешить DHCP-ответы от DHCP-сервера к ISA Server	Разрешить	DHCP (ответ)	Внутренняя сеть	Локальный хост	Все пользователи
10. Подтверждает, что для подмножества компьютеров удаленного управления правильно настроены IP-адреса	Разрешает ICMP (PING) запросы от выбранных компьютеров к ISA Server	Разрешить	Ping	Компьютеры удаленного управления	Локальный хост	Все пользователи

11. Это правило необходимо включить для того, чтобы брандмауэр ISA мог выполнять задачи по управлению сетью с помощью ICMP	Разрешить ICMP-запросы с ISA Server к выбранным серверам	Разрешить	Запрос информации ICMP, временная метка ICMP, Ping	Локальный хост	Все сети (и сеть локального хоста)	Все пользователи
12. (Отключено по умолчанию) Это правило автоматически включается при включении компонента VPN-сервера брандмауэра ISA	Весь трафик VPN-клиента на ISA Server	Разрешить	PPTP	Внешняя сеть	Локальный хост	Все пользователи
13. (Отключено по умолчанию) Это правило автоматически включается при включении VPN-подключений «узе-в-узел» с этим брандмауэром ISA	Разрешить VPN-подключения «узел-в-узел» с ISA Server	Разрешить	Нет	Внешние удаленные шлюзы IPSec	Локальный хост	Все пользователи
14. (Отключено по умолчанию) Это правило автоматически включается при включении VPN-подключений «узе-в-узел» с этим брандмауэром ISA	Разрешить VPN-подключения «узел-в-узел» с ISA Server	Разрешить	Нет	Локальный хост	Внешние удаленные шлюзы IPSec	Все пользователи
15. Если не нужен доступ с брандмауэра ISA к папкам общего доступа, то это правило следует отключить	Разрешить соединение по протоколу CIFS с ISA Server к доверяемым серверам	Разрешить	Microsoft CIFS (TCP), Microsoft CIFS (UDP)	Локальный хост	Внутренняя сеть	Все пользователи
16. (Отключено по умолчанию) Включите это правило, если нужно входить в систему с помощью SQL	Разрешить удаленный вход в систему с помощью SQL с ISA Server на выбранные серверы	Разрешить	Microsoft SQL (TCP), Microsoft SQL (UDP)	Локальный хост	Внутренняя сеть	Все пользователи
17. Включите это правило, если нужно разрешать брандмауэру ISA самостоятельно устанавливать соединения с сайтом Windows Update.	Разрешить HTTP/HTTPS запросы с ISA Server на указанные сайты	Разрешить	HTTP,HTTPS	Локальный хост	Сайты, разрешенные системной политикой	Все пользователи
18. (По	Разрешить	Разрешить	HTTP,HTTPS	Локальный	Все сети (и	Все

умолчанию отключено) Это правило включается при создании верификатора связи по протоколам HTTP/HTTPS	запросы по протоколам HTTP/HTTPS с ISA Serverк выбранным серверам для верификаторов связей			хост	сеть локального хоста)	пользователи
19. (По умолчанию отключено) Это правило включается, если на брандмауэре ISA устанавливается общий ресурс клиента брандмауэра	Разрешить доступ с надежных компьютеров к общему ресурсу с установочными файлами клиента брандмауэра на ISA Server	Разрешить	Microsoft CIFS (TCP), Microsoft CIFS (UDP), дейтаграмма NetBIOS, служба имен NetBIOS, сеанс NetBIOS	Внутренняя сеть	Локальный хост	Все пользователи
20. (Отключено по умолчанию) Включите это правило, если нужно выполнять удаленный мониторинг производительности брандмауэра ISA	Разрешить удаленный мониторинг производительности ISA Server с доверяемых серверов	Разрешить	дейтаграмма NetBIOS, служба имен NetBIOS, сеанс NetBIOS	Компьютеры удаленного управления	Локальный хост	Все пользователи
21. Включите это правило, если нужно обеспечить доступ к общим папкам с брандмауэра ISA	Разрешить NetBIOS с ISA Server к доверяемым серверам	Разрешить	дейтаграмма NetBIOS, служба имен NetBIOS, сеанс NetBIOS	Локальный хост	Внутренняя сеть	Все пользователи
22. Включите это правило, если нужно использовать протокол RPC для соединения с другими серверами	Разрешить RPC-соединения с ISA Server к доверяемым серверам	Разрешить	RPC (все интерфейсы)	Локальный хост	Внутренняя сеть	Все пользователи
23. Это правило разрешает брандмауэру ISA отправлять сообщения об ошибках в корпорацию Microsoft	Разрешить сообщения об ошибках по протоколам HTTP/HTTPS с ISA Server к указанным сайтам Microsoft	Разрешить	HTTP,HTTPS	Локальный хост	Сайты Microsoft по обработке сообщений об ошибках	Все пользователи
24. (Отключено по умолчанию) Это правило следует включить, если включена проверка подлинности SecurID	Разрешить проверку подлинности SecurID с ISA Server к доверяемым серверам	Разрешить	SecurID	Локальный хост	Внутренняя сеть	Все пользователи
25. (Отключено по умолчанию) Включите это	Разрешить удаленный мониторинг с	Разрешить	Microsoft Operations Manager Agent	Локальный хост	Внутренняя сеть	Все пользователи

правило, если нужно использовать MOM (Microsoft Operations Manager, менеджер операций Microsoft) для мониторинга брандмауэра ISA	ISA Server на доверяемые серверы с помощью агента MOM					
26. (Отключено по умолчанию) Включите это правило, если нужно обеспечить доступ брандмауэра ISA к CRL (он необходим, если брандмауэр ISA завершает любые SSL-соединения)	Разрешить весь HTTP-трафик с ISA Server ко всем сетям (для загрузок CRL)	Разрешить	HTTP	Локальный хост	Все сети (и локальный хост)	Все пользователи
27. Это правило следует изменить, разрешив контакт с доверяемым NTP-сервером организации	Разрешить NTP-соединения с ISA Server к доверяемым NTP-серверам	Разрешить	NTP (UDP)	Локальный хост	Внутренняя сеть	Все пользователи
28. Это правило следует отключить, если не нужно использовать протокол SMTP для отправки оповещений. В противном случае нужно заменить внутренний адресат (Internal Destination) конкретным компьютером, который будет принимать SMTP-сообщения с брандмауэра ISA	Разрешить SMTP-соединения с ISA Server к доверяемым серверам	Разрешить	SMTP	Локальный хост	Внутренняя сеть	Все пользователи
29. (Отключено по умолчанию) Это правило автоматически включается при включении заданий на загрузку содержимого	Разрешить HTTP-соединения с ISA Server к выбранным компьютерам с целью выполнения заданий на загрузку содержимого	Разрешить	HTTP	Локальный хост	Все сети (и локальный хост)	Системная и сетевая служба
30. Это правило нужно включить, если планируется использовать удаленную MMC-оснастку	Разрешить брандмауэру контролировать соединения с выбранными компьютерами	Разрешить	Весь исходящий трафик	Локальный хост	Компьютеры удаленного доступа	Все пользователи

Правила системной политики брандмауэра ISA оцениваются прежде всех задаваемых пользователями правил доступа в том порядке, как они перечислены в табл. 5. Системную политику брандмауэра ISA можно просмотреть, щелкнув мышью **Firewall Policy** (Политика брандмауэра) в левой панели консоли, а затем щелкнув вкладку **Tasks** (Задачи). На вкладке Tasks (Задачи) щелкните мышью **Show System Policy Rules** (Показать правила системной политики). Щелкните мышью **Hide System Policy Rules** (Скрыть правила системной политики), когда закончите просматривать системную политику брандмауэра.

Изменить системную политику брандмауэра ISA можно, **щелкнув** мышью пункт **Edit System Policy** (Редактировать системную политику) на вкладке **Tasks** (Задачи). Откроется окно редактора системной политики **System Policy Editor** (Редактор системной политики) (рис. 4). Для каждого правила системной политики имеются вкладки **General** (Общие) и **From** (От) или **To** (К). Вкладка **General** (Общие) для каждой **Configuration Group** (Группы конфигурирования) содержит объяснение правил(а), а вкладки From (От) и To (К) позволяют контролировать доступ от/к компьютеру брандмауэра ISA.

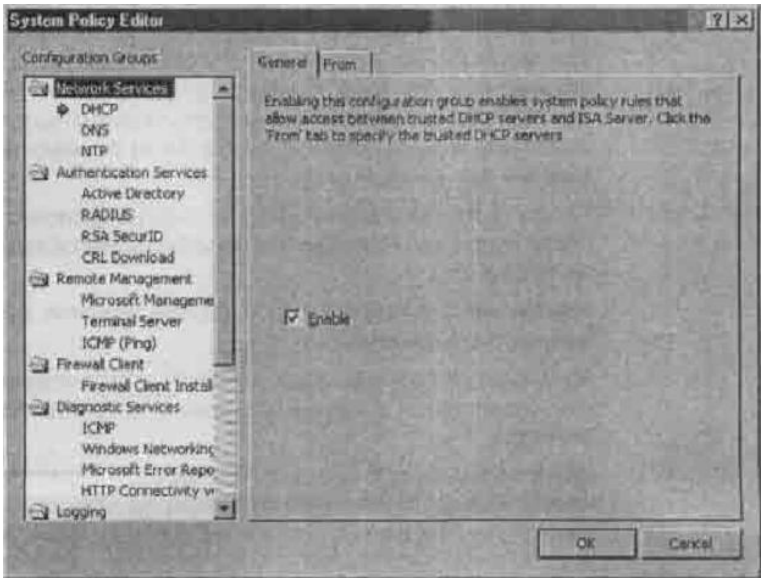

Рисунок 4. Диалоговое окно **System** Policy **Editor** (Редактор системной политики)

Табл. 6. Стандартная конфигурация системы брандмауэра ISA после его установки

Функция	Стандартное значение
Полномочия пользователей	Члены группы администраторов на локальном компьютере могут конфигурировать политику брандмауэра. Если брандмауэр ISA является членом домена, то глобальная группа администраторов домена автоматически включается в локальную группу администраторов
Определение внутренней сети	Внутренняя сеть содержит IP-адреса, указанные в процессе установки программного обеспечения брандмауэра ISA
Сетевые правила	Правило доступа к локальному хосту определяет отношения типа «маршрут» (а не NAT) между сетью локального хоста и всеми остальными сетями. Правило доступа к Интернету определяет отношения NAT между внутренней сетью, сетью изолированных VPN-клиентов и сетью VPN-клиентов с одной стороны и внешней сетью с другой. Соединение этих трех типов сетей с Интернетом осуществляется с помощью NAT. Доступ разрешается, только если настроены соответствующие правила доступа. Правило отношений между сетью VPN-клиентов и внутренней сетью определяет отношение типа «маршрут» между этими сетями. Доступ разрешается, только **если** разрешен доступ для VPN-клиентов
Политика брандмауэра	Правило по умолчанию (Default Rule) запрещает трафик между всеми сетями
Системная политика	По умолчанию ISA Server является хорошо **защищенным,** при этом он разрешает работу нескольких важных служб. После установки некоторые правила системной политики включаются для того, чтобы разрешить работу необходимых служб. Рекомендуется просмотреть конфигурацию системной политики и настроить ее, чтобы были включены службы, важные для данной сети

Создание Web-цепочек	Правило по умолчанию (Default Rule) определяет, что все запросы клиентов Web-прокси обрабатываются непосредственно из Интернета
Кэширование	Размер кэша установлен равным 0. Таким образом, кэширование полностью отключено
Оповещения	Большинство оповещений включено. Рекомендуется настроить оповещения в соответствиями с потребностями конкретной сети
Конфигурация клиента	Для клиента брандмауэра и Web-прокси включено автоматическое обнаружение. Web-браузеры на клиентах брандмауэра конфигурируются при установке клиента брандмауэра

4 Установка брандмауэра ISA на компьютере с одним сетевым адаптером (брандмауэр ISA с одним сетевым интерфейсом)

Программное обеспечение брандмауэра ISA можно установить на компьютере с одной сетевой интерфейсной картой. Такая конфигурация имитирует конфшурацию Proxy Server 2.0 или брандмауэр ISA Server 2000 в режиме только кэширования. Брандмауэр ISA Server 2004 не может работать в режиме только кэширования, но при установке этого брандмауэра на компьютере с одним сетевым адаптером можно лишить брандмауэр существенной части его функций.

Если брандмауэр ISA устанавливается в режиме с одним сетевым адаптером, теряются следующие его функции:

- поддержка клиентов брандмауэра;
- поддержка полной защиты и функциональности клиента SecureNAT;
- правила публикации серверов;
- поддержка всех протоколов, за исключением HTTP, HTTPS и FTP, по HTTP-туннелю (Web-прокси);
- VPN-подключения удаленного доступа;
- VPN-подключения «узел-в-узел»;
- функции поддержки работы с несколькими сетями (все адресное пространство IPv4 в одной сети);
- проверка на уровне приложения для всех протоколов, кроме HTTP.

Хотя такая сокращенная версия брандмауэра ISA сохраняет лишь часть своей способности выступать в роли сетевого брандмауэра для защиты хостов в корпоративной сети, она тем не менее способна обеспечить собственную защиту, как и полнофункциональный брандмауэр. Брандмауэр ISA будет напрямую доступен для внешних и внутренних хостов только в том случае, если будут включены правила системной политики, разрешающие этот доступ.

Для конфигурации сетевой интерфейсной карты на брандмауэре ISA с одним сетевым интерфейсом в качестве адреса основного шлюза должен быть указан IP-адрес любого шлюза в сети, позволяющий брандмауэру ISA с одним сетевым интерфейсом получить доступ к Интернету. Все прочие нелокальные маршруты должны быть настроены в таблице маршрутизации брандмауэра ISA с одним сетевым интерфейсом.

Если нужно только, чтобы служба Web-прокси работала в прямом и обратном режиме, то следует установить программное обеспечение брандмауэр ISA на компьютере с одной сетевой интерфейсной картой.

5 Конфигурирование брандмауэра ISA для быстрого старта

В этом руководстве по быстрой установке и конфигурированию брандмауэра используется сеть, к которой предъявляются следующие требования:

- в этой сети нет других серверов Windows. Это руководство включает в себя инструкции по установке служб DNS и DHCP на брандмауэре ISA. Если в сети уже имеется DNS- или DHCP-сервер, на брандмауэре ISA их устанавливать не нужно;
- установка брандмауэра ISA Server 2004 производится на базе ОС Windows Server 2003;
- на компьютере установлена ОС Windows Server 2003 со стандартными настройками и нет другого программного обеспечения;
- на компьютере на базе Windows Server 2003 установлено два сетевых адаптера. Одна сетевая интерфейсная карта соединена с внутренней сетью, а другая напрямую

соединяется с Интернетом через сетевой маршрутизатор или же перед ней есть DSL или кабельный NAT-«маршрутизатор»

- компьютеры во внутренней сети настроены как DHCP-клиенты и будут использовать компьютер брандмауэра ISA Server 2004 в качестве своего DHCP-сервера;
- компьютер на базе ОС Windows Server 2003, на котором устанавливается программное обеспечение брандмауэра ISA Server 2004, не является членом домена Windows. Хотя позже рекомендуется сделать брандмауэр ISA членом домена, компьютер, на котором установлено программное обеспечение брандмауэра ISA, не обязательно должен быть членом домена. Это требование необходимо в данном руководстве, потому что предполагается, что в данной сети нет других серверов на базе Windows (но в ней могут быть серверы на базе Linux, Netware и других производителей).

На рис. 5 показан брандмауэр ISA и его отношения с внутренней и внешней сетью. Внутренний интерфейс подключен к концентратору или коммутатору внутренней сети, а внешний интерфейс подключен к концентратору или коммутатору, который также подключен к маршрутизатору.

Рисунок 5. Физические связи между брандмауэром ISA Server 2004, внутренней и внешней сетью

Для быстрой установки и конфигурирования брандмауэра ISA нужно выполнить следующие действия:

- настроить сетевые интерфейсы брандмауэра ISA;
- установить и настроить DNS-сервер на компьютере брандмауэра ISA Server 2004;
- установить и настроить DHCP-сервер на компьютере брандмауэра ISA Server 2004;
- установить и настроить программное обеспечение ISA Server 2004;
- настроить компьютеры внутренней сети как DHCP-клиенты.

5.1 Конфигурирование сетевых интерфейсов брандмауэра ISA

У брандмауэра ISA должен быть хотя бы один внутренний сетевой интерфейс и один внешний сетевой интерфейс. Чтобы правильно настроить сетевые интерфейсы на брандмауэре ISA, нужно сделать следующее:

- назначить IP-адреса внутреннему и внешнему сетевым интерфейсам;
- назначить адрес DNS-сервера внутреннему интерфейсу брандмауэра ISA;
- поместить внутренний интерфейс в верх списка сетевых интерфейсов.

Назначение IP-адресов и DNS-сервера

Прежде всего нужно назначить статические IP-адреса внутреннему и внешнему интерфейсу брандмауэра ISA. Для брандмауэра ISA также требуется адрес DNS-сервера,

связанного с его внутренним интерфейсом. Для всех сетевых интерфейсов брандмауэра ISA не используется DHCP-сервер, потому что у внутреннего интерфейса должен всегда быть статический IP-адрес, а внешний интерфейс не поддерживает динамические адреса, поскольку он находится за маршрутизатором.

Если в учетной записи Интернета используется DHCP для присвоения общего адреса, то DSL или кабельный маршрутизатор могут получать и обновлять общий адрес. Кроме того, если для соединения с интернет-провайдером используется PPPoE (Point-to-Point Protocol over Ethernet, протокол «точка-точка» через Ethernet) или VPN, то маршрутизатор также может выполнять эти задачи.

Конфигурирование внутреннего сетевого интерфейса

Внутренний интерфейс должен иметь IP-адрес с того же идентификатора сети, что и другие компьютеры во внутренней сети. Этот адрес должен входить в адресный диапазон частной сети и не должен уже использоваться в сети.

Брандмауэр ISA будет настроен на использование адреса внутреннего интерфейса качестве адреса DNS-сервера.

На брандмауэре ISA должен быть статический IP-адрес, связанный с его внутренним интерфейсом. На компьютере на базе ОС Windows Server 2003 нужно выполнить следующие действия:

1. Правой кнопкой мыши щелкните My Network Places (Сетевое окружение) на рабочем столе и выберите в контекстном меню пункт Properties (Свойства).

2. В окне Network Connections (Сетевые подключения) правой кнопкой мыши щелкните внутренний сетевой интерфейс и выберите в контекстном меню пункт Properties (Свойства).

3. В диалоговом окне сетевого интерфейса Properties (Свойства) щелкните правой кнопкой мыши Internet Protocol (TCP/IP) (Протокол Интернета, TCP/IP) и выберите в контекстном меню пункт Properties (Свойства).

4. В диалоговом окне Internet Protocol (TCP/IP) Properties (Свойства: Протокол Интернета, TCP/IP) выберите Use the following IP address (Использовать следующий IP-адрес). Введите IP-адрес внутреннего интерфейса в текстовое поле IP address (IP-адрес). Введите маску подсети для внутреннего интерфейса в текстовом поле Subnet mask (Маска подсети). Не вводите основной шлюз для внутреннего интерфейса.

5. Выберите Use the following DNS server addresses (Использовать следующие адреса DNS-серверов). Введите IP-адрес внутреннего интерфейса брандмауэра ISA в текстовом поле Preferred DNS server (Предпочитаемый DNS-сервер). Это тот же адрес, который был введен в текстовое поле IP-address (IP-адрес) в п. 4. Нажмите кнопку ОК в диалоговом окне Internet Protocol (TCP/IP) Properties (Свойства: Протокол Интернета, TCP/IP).

6. Нажмите кнопку ОК в диалоговом окне Properties (Свойства) внутреннего интерфейса.

Конфигурирование внешнего сетевого интерфейса

Для того чтобы настроить информацию об IP-адресах на внешнем интерфейсе брандмауэра ISA, выполните следующие действия:

1. Правой кнопкой мыши щелкните My Network Places (Сетевое окружение) на рабочем столе и в контекстном меню выберите пункт Properties (Свойства).

2. В окне Network Connections (Сетевые подключения) правой кнопкой мыши щелкните внешний сетевой интерфейс и в контекстном меню выберите пункт Properties (Свойства).

3. В диалоговом окне сетевого интерфейса Properties (Свойства) щелкните мышью Internet Protocol (TCP/IP) (Протокол Интернета, TCP/IP) и выберите пункт меню Properties (Свойства).

4. В диалоговом окне Internet Protocol (TCP/IP) Properties (Свойства: протокол Интернета, TCP/IP) выберите Use the following IP address (Использовать следующий IP-

адрес). Введите IP-адрес внешнего интерфейса в текстовое поле IP address (IP-адрес). Введите маску подсети для внешнего интерфейса в текстовое поле Subnet mask (Маска подсети). Введите основной шлюз для внешнего интерфейса в текстовое поле Default gateway (Основной шлюз). Основной шлюз — это адрес маршрутизатора в сети.

5. Нажмите кнопку OK в диалоговом окне Properties (Свойства) внешнего интерфейса.

5.2 Установка и конфигурирование DNS-сервера на брандмауэре ISA

На брандмауэре ISA будет установлен DNS-сервер в режиме только кэширования. Это позволит компьютерам во внутренней сети и брандмауэру ISA разрешать имена хостов в Интернете. Отметим, что если во внутренней сети уже есть DNS-сервер, то устанавливать его еще раз не нужно. Если во внутренней сети есть DNS-сервер, то можно попробовать настроить компьютер брандмауэра ISA как DNS-сервер в режиме только кэширования, а затем настроить компьютеры во внутренней сети так, чтобы они использовали компьютер с ISA Server 2004 в качестве DNS-сервера или применяли DNS-сервер внутренней сети, а DNS-сервер внутренней сети настроить так, чтобы он использовал брандмауэр ISA в качестве сервера пересылок DNS.

Установка службы DNS

Служба DNS-сервера не устанавливается по умолчанию в операционных системах Windows для серверов. Сначала нужно установить службу DNS-сервера на компьютере на базе Windows Server 2003, который будет играть роль брандмауэра ISA.

Установка службы DNS-сервера на базе Windows Server 2003

Выполните следующие действия, чтобы установить службу DNS на компьютере с Windows Server 2003:

1. Нажмите кнопку Start (Пуск), установите курсор мыши на Control Panel (Панель управления) и щелкните мышью Add or Remove Programs (Установка и удаление программ).

2. В окне Add or Remove Programs (Установка и удаление программ) щелкните мышью Add/Remove Windows Components (Установка компонентов Windows).

3. В диалоговом окне Windows Components Wizard (Мастер компонентов Windows) выберите Networking Services (Сетевые службы) из списка Components (Компоненты Windows). Не устанавливайте флажок в поле! Выделив запись Networking Services (Сетевые службы), нажмите кнопку Details (Состав).

4. В диалоговом окне Networking Services (Сетевые службы) установите флажок в поле Domain Name System (DNS) и нажмите кнопку OK.

5. Нажмите кнопку Next (Далее) в диалоговом окне Windows Components (Компоненты Windows).

6. Нажмите кнопку OK в диалоговом окне Insert Disk (Вставка диска). В диалоговом окне Files Needed (Требуемые файлы) укажите путь к папке i386 на установочном компакт-диске Windows Server 2003 в текстовом поле Copy files from (Размещение файлов) и нажмите кнопку OK.

7. Нажмите кнопку Finish (Готово) на странице Completing the Windows Components Wizard (Завершение работы мастера компонентов Windows).

8. Закройте окно Add or Remove Programs (Установка и удаление программ).

Конфигурирование службы DNS на брандмауэре ISA

DNS-сервер на компьютере с брандмауэром ISA выполняет DNS-запросы имен хостов в Интернете от имени компьютеров внутренней сети. DNS-сервер на брандмауэре ISA настроен в режиме только кэширования. DNS-сервер в режиме только кэширования не имеет информации об общих или частных DNS-именах и доменах. Он разрешает имена

хостов в Интернете и кэширует результаты; он не отвечает на DNS-запросы имен в частной DNS-зоне внутренней сети или в общей DNS-зоне.

Если во внутренней сети имеется DNS-сервер, поддерживающий домен Active Directory, то расположенный на брандмауэре ISA DNS-сервер можно настроить в режиме только кэширования так, чтобы направлять клиентские запросы к домену внутренней сети на DNS-сервер внутренней сети. В итоге DNS-сервер в режиме только кэширования на компьютере брандмауэра ISA Server 2004 не будет мешать текущей установке DNS-сервера.

Конфигурирование службы DNS в Windows Server 2003

Для того чтобы настроить службу DNS на компьютере с Windows Server 2003 выполните следующие действия:

1. Нажмите кнопку Start (Пуск) и установите курсор мыши на Administrative Tools (Администрирование). Щелкните мышью запись DNS.

2. Правой кнопкой мыши щелкните имя сервера в левой панели консоли, установите курсор мыши на View (Вид) и щелкните пункт Advanced (Расширенный).

3. Разверните все узлы в левой панели консоли DNS.

4. Правой кнопкой мыши щелкните имя сервера в левой панели консоли DNS и в контекстном меню выберите пункт Properties (Свойства).

5. В диалоговом окне Properties (Свойства) сервера щелкните мышью вкладку Interfaces (Интерфейсы). Выберите вариант Only the following IP addresses (Только по указанным IP-адресам). Щелкните мышью любой IP-адрес, не связанный с внутренним интерфейсом компьютера. Выделив такой IP-адрес, нажмите кнопку Remove (Удалить). Нажмите кнопку Apply (Применить).

6. Щелкните мышью вкладку Forwarders (Пересылка) (рис. 6). Введите IP-адрес DNS-сервера интернет-провайдера в текстовое поле Selected domain's forwarder IP address list (Список IP-адресов серверов пересылки для выбранного домена), а затем нажмите кнопку Add (Добавить). Установите флажок в поле Do not use recursion for this domain (Не использовать рекурсию для этого домена). Этот вариант запрещает попытки DNS-сервера на брандмауэре ISA выполнять разрешение имен самостоятельно. В итоге, если сервер пересылки не может разрешить имя, запрос на разрешение имени отвергается. Нажмите кнопку Apply (Применить).

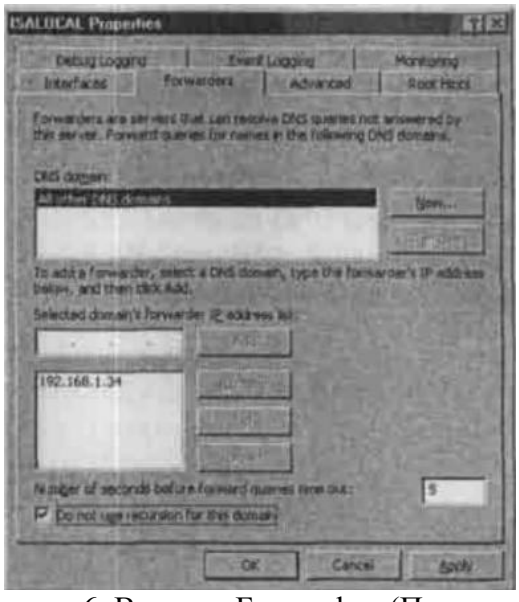

Рисунок 6. Вкладка Forwarders (Пересылка)

7. Нажмите кнопку OK в диалоговом окне Properties (Свойства).

8. Правой кнопкой мыши щелкните имя сервера, установите курсор на All Tasks (Все задачи) и нажмите кнопку Restart (Перезапустить).

Эти действия нужно выполнять, только если во внутренней сети нет DNS-сервера, который используется для поддержки домена Active Directory.

5.3 Установка и конфигурирование DHCP-сервера на брандмауэре ISA

У каждого компьютера должен быть IP-адрес и другая информация, позволяющая ему взаимодействовать с другими компьютерами в сети и в Интернете. Служба DHCP-сервера может быть установлена на брандмауэре ISA, она предоставляет информацию об IP-адресах компьютерам во внутренней сети. Предположим, что брандмауэр ISA будет использоваться в качестве DHCP-сервера.

Установка службы DHCP-сервера на базе Windows Server 2003

Для того чтобы установить службу DNS-сервера на базе Windows Server 2003, выполните следующие действия:

1. Нажмите кнопку Start (Пуск), установите курсор мыши на Control Panel (Панель управления) и выберите пункт Add or Remove Programs (Установка и удаление программ).

2. В окне Add or Remove Programs (Установка или удаление программ) щелкните мышью Add/Remove Windows Components (Установка/Удаление компонентов Windows).

3. В диалоговом окне Windows Components Wizard (Мастер компонентов Windows) выберите Networking Services (Сетевые службы) из списка Components (Компоненты Windows). Не устанавливайте флажок в поле! Выделив запись Networking Services (Сетевые службы) нажмите кнопку Details... (Состав...).

4. В диалоговом окне Networking Services (Сетевые службы) (рис. 7) установите флажок в поле Dynamic Host Configuration Protocol (DHCP) и нажмите кнопку ОК.

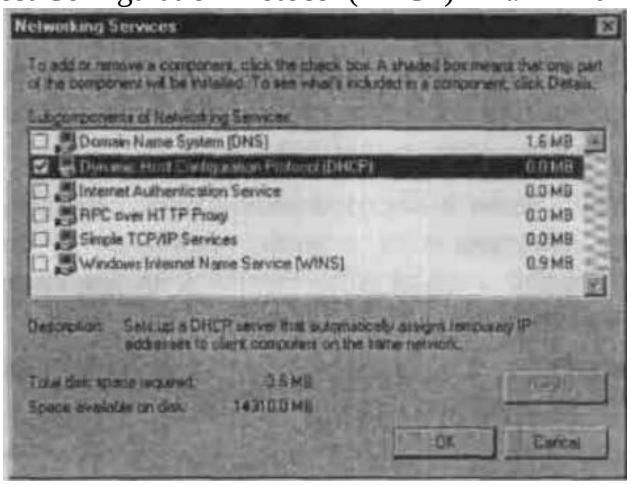

Рисунок 7. Диалоговое окно Networking Services (Сетевые службы)

5. Нажмите кнопку Next (далее) в диалоговом окне Windows Components (Компоненты Windows).

6. Нажмите кнопку Finish (Готово) на странице Completing the Windows Components Wizard (Завершение мастера компонентов Windows).

7. Закройте окно Add or Remove Programs (Установка или удаление программ).

Конфигурирование службы DHCP

DHCP-сервер должен быть сконфигурирован с набором IP-адресов, которые он может присваивать компьютерам в частной сети. DPICP-сервер также предоставляет дополнительную информацию помимо IP-адреса, включающую адрес DNS-сервера, основной шлюз и первичное имя домена.

Адреса DNS-сервера и основного шлюза, назначаемые компьютеру, совпадают с IP-адресом внутреннего интерфейса брандмауэра ISA. DHCP-сервер использует область DHCP, чтобы предоставить эту информацию клиентам внутренней сети. Необходимо

создать область DHCP, которая предоставляет клиентам внутренней сети правильную информацию об IP-адресах.

ПРИМЕЧАНИЕ: DHCP-сервер не должен назначать адреса, которые уже используются в сети. Нужно создать исключения для этих IP-адресов. В качестве примера можно привести статические или зарезервированные адреса, назначенные печатным, файловым, почтовым или Web-серверам, это лишь несколько примеров устройств или серверов, которые постоянно используют одни и те же назначенные им на постоянной основе IP-адреса. Если для этих адресов не создать исключения, то DHCP-сервер выполнит разрешение адресов, а когда он обнаружит, что эти адреса уже используются, то он поместит их в группу плохих адресов (bad address group). Кроме того, хорошо сконфигурированная сеть сгруппирует компьютеры в смежные блоки IP-адресов. Например, все компьютеры, которым должны быть назначены статические IP-адреса, входят в один блок.

Для того чтобы настроить DHCP-сервер на базе Windows Server 2003 с областью, которая будет назначать правильную информацию об IP-адресах клиентам внутренней сети, выполните следующие действия:

ПРЕДУПРЕЖДЕНИЕ: Если в корпоративной сети уже есть DHCP-сервер, не выполняйте эти действия и не устанавливайте DHCP-сервер на брандмауэре ISA. DHCP-сервер следует устанавливать на брандмауэре ISA, только если во внутренней сети нет DHCP-сервера.

1. Нажмите кнопку Start (Пуск) и установите курсор мыши на Administrative Tools (Администрирование). Нажмите кнопку DHCP.

2. Разверните все узлы в левой панели консоли DHCP. Правой кнопкой мыши щелкните имя сервера в левой панели консоли и нажмите кнопку New Scope (Создать область).

3. Нажмите кнопку Next (Далее) на странице Welcome to the New Scope Wizard (Вас приветствует мастер создания области).

4. Введите SecureNAT Client Scope (Область для клиента SecureNAT) в текстовом поле Name (Имя) на странице Scope Name (Имя области). Нажмите кнопку Next (Далее).

5. На странице IP Address Range (Диапазон адресов) введите первый IP-адрес и последний IP-адрес диапазона в текстовые поля Start IP address (Начальный IP-адрес) и End IP address (Конечный IP-адрес). Например, при использовании идентификатора сети 192.168.1.0 с маской подсети 255.255.255-0 введите начальный IP-адрес 192.168.1.1, а конечный IP-адрес 192.168.1.254. Нажмите кнопку Next (Далее).

6. На странице Add Exclusions (Добавление исключений) введите IP-адрес внутреннего интерфейса брандмауэра ISA в текстовое поле Start IP address (Начальный IP-адрес) и нажмите кнопку Add (Добавить). Если в сети имеются серверы или рабочие станции со статическими IP-адресами, которые не нужно менять, добавьте эти адреса в список исключений. Нажмите кнопку Next (Далее), после того как будут добавлены все адреса, которые нужно исключить из области DHCP.

7. На странице Lease Duration (Срок действия аренды адреса) оставьте стандартное значение и нажмите кнопку Next (Далее).

8. На странице Configuring DHCP Options (Настройка параметров DHCP) выберите Yes, I want to configure these options now (Да, настроить эти параметры сейчас) и щелкните кнопку Next (Далее).

9. На странице Router (Маршрутизатор, основной шлюз) введите IP-адрес внутреннего интерфейса брандмауэра ISA и нажмите кнопку Add (Добавить). Нажмите кнопку Next (Далее).

10. На странице Domain Name and DNS Servers (Имя домена и DNS-серверы) введите IP-адрес внутреннего интерфейса брандмауэра ISA в текстовое поле IP address (IP-адрес) и нажмите кнопку Add (Добавить). Если во внутренней сети имеется домен Active Directory, введите имя домена внутренней сети в текстовое поле Parent domain

(Родительский домен). Не вводите имя домена в текстовое поле Parent domain (Родительский домен), если во внутренней сети нет домена Active Directory. Щелкните кнопку Next (Далее).

11. Не вводите никакую информацию на странице WINS Servers (WINS-серверы), если во внутренней сети нет WINS-сервера. Если во внутренней сети имеется WINS-сервер, введите этот IP-адрес в текстовое поле IP address (IP-адрес). Нажмите кнопку Next (Далее).

12. Выберите Yes, I want to activate this scope now (Да, я хочу активировать эту область сейчас) на странице Activate Scope (Активировать область) и нажмите кнопку Yes (Да).

13. Нажмите кнопку Finish (Готово) на странице Completing the New Scope Wizard (Завершение мастера создания области).

5.4 Установка и конфигурирование программного обеспечения ISA Server 2004

Чтобы установить программное обеспечение брандмауэра ISA на компьютере на базе ОС Windows Server 2003 с двумя сетевыми адаптерами, выполните следующие действия:

1. Вставьте установочный компакт-диск для ISA Server 2004 в дисковод для компакт-дисков или установите соединение с общим сетевым ресурсом, в котором находятся установочные файлы ISA Server 2004. Если программа установки не запустится автоматически, дважды щелкните мышью файл isaautorun.exe в корне дерева установочных файлов.

2. На странице Microsoft Internet Security and Acceleration Server 2004 щелкните мышью Review Release Notes (Информация о версии) и прочтите информацию о версии. Эта информация о версии содержит полезные данные о важных моментах и возможностях конфигурирования. После просмотра информации о версии щелкните мышью Read Setup and Feature Guide (Прочесть руководство по установке и функциям). Не обязательно читать все руководство сразу, его можно распечатать и прочесть потом. Щелкните мышью Install ISA Server 2004 (Установить ISA Server 2004).

3. Нажмите кнопку Next (Далее) на странице Welcome to the Installation Wizard for Microsoft ISA Server 2004 (Мастер установки Microsoft ISA Server 2004).

4. Выберите вариант I accept the terms in the license agreement (Я согласен) на странице License Agreement (Лицензионное соглашение). Нажмите кнопку Next (Далее).

5. На странице Customer Information (Информация о пользователе) введите имя пользователя и название организации в текстовые поля User Name (Имя) и Organization (Организация). Введите серийный номер в текстовое поле Product Serial Number (Серийный номер). Щелкните кнопку Next (Далее).

6. На странице Setup Type (Тип установки) щелкните мышью вариант Custom (Пользовательская). Если не нужно устанавливать программное обеспечение брандмауэра ISA на диске C: , щелкните мышью кнопку Change (Изменить), чтобы изменить место установки программы на жестком диске. Нажмите кнопку Next (Далее).

7. На странице Custom Setup (Пользовательская установка) выберите устанавливаемые компоненты. По умолчанию устанавливаются компоненты Firewall Services, Advanced Logging и ISA Server Management. Средство контроля SMTP-сообщений (Message Screener), которое используется для того, чтобы контролировать спам и вложения, поступающие в сеть и исходящие из нее, не устанавливается по умолчанию. Прежде чем устанавливать Message Screener, нужно установить SMTP-службу IIS 6.0 на компьютере брандмауэра ISA Server 2004. В данном случае будет установлен общий ресурс с установочными файлами для клиента брандмауэра Firewall Client Installation Share, чтобы впоследствии можно было установить клиент брандмауэра на других компьютерах во внутренней сети. Щелкните мышью значок x слева от параметра Firewall

Client Installation Share и щелкните мышью This feature, and all subfeatures, will be installed on the local hard drive (Эта функция и все подфункции будут установлены на локальном жестком диске) (рис. 8). Использование клиента брандмауэра позволяет лучше защитить сеть, по возможности следует всегда устанавливать клиент брандмауэра на клиентских компьютерах во внутренней сети. Нажмите кнопку Next (Далее).

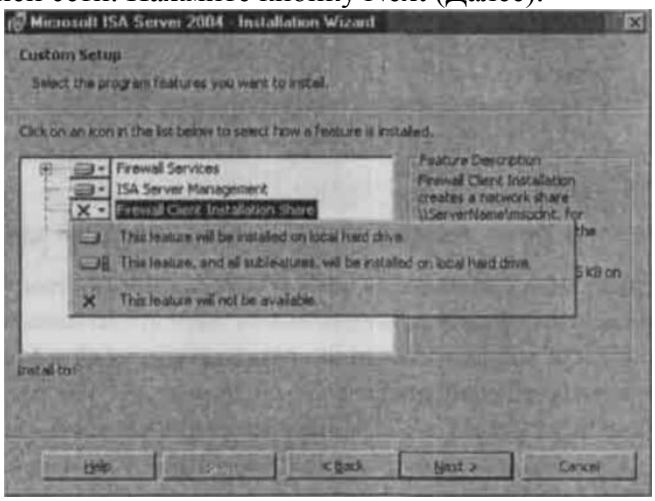

Рисунок 8. Страница Custom Setup (Пользовательская установка)

8. На странице Internal Network (Внутренняя сеть) нажмите кнопку Add (Добавить). Внутренняя сеть отличается от таблицы локальных адресов (LAT, Local Address Table), которая использовалась в брандмауэре ISA Server 2000. Внутренняя сеть включает в себя доверяемые сетевые службы, с которыми должен взаимодействовать брандмауэр ISA. В качестве примера таких служб можно привести контроллеры домена Active Directory, DNS, DHCP, службы терминалов и др. Системная политика брандмауэра использует определение внутренней сети во многих правилах системной политики.

9. На странице Internal Network (Внутренняя сеть) нажмите кнопку Select Network Adapter (Выбрать сетевой адаптер).

10. На странице Configure Internal Network (Настроить внутреннюю сеть) снимите флажок в поле Add the following private ranges... (Добавить следующие частные диапазоны...). Оставьте флажок в поле Add address ranges based on the Windows Routing Table (Добавить диапазоны адресов на основе таблицы маршрутизации Windows) (рис. 9). Установите флажок в поле рядом с адаптером, соединенным со внутренней сетью. В данном случае сетевые интерфейсы были переименованы так, чтобы имя интерфейса отражало его расположение. Нажмите кнопку OK.

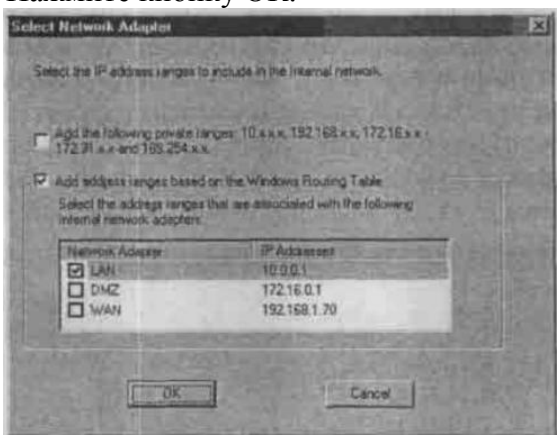

Рисунок 9. Страница Select Network Adapter (Выбрать сетевой адаптер)

11. Нажмите кнопку OK в диалоговом окне с сообщением о том, что внутренняя сеть была определена на основании таблицы маршрутизации Windows.

12. Щелкните кнопку OK в диалоговом окне Internal network address ranges (Диапазоны адресов внутренней сети).

13. Нажмите кнопку Next (Далее) на странице Internal Network (Внутренняя сеть).

14. Не устанавливайте флажок в поле Allow computers running earlier versions of Firewall Client software to connect (Разрешить соединения компьютерам с более ранними версиями программного обеспечения клиента брандмауэра). Этот параметр предполагает применение клиента брандмауэра нового брандмауэра ISA. Предыдущие версии клиента брандмауэра (входящие в Proxy 2.0 и ISA Server 2000) не поддерживаются. Этот параметр также разрешает клиенту брандмауэра отправлять верительные данные пользователя по зашифрованному каналу на брандмауэр ISA и проходить проверку подлинности на брандмауэре ISA в прозрачном режиме. Щелкните кнопку Next (Далее).

15. На странице Services (Службы) отметьте, чтобы службы SNMP и IIS Admin Service были остановлены на время установки. Если на компьютере брандмауэра ISA Server 2004 установлены службы Internet Connection Firewall (ICF)/Internet Connection Sharing (ICF) и/или служба IP Network Address Translation, то они будут отключены, т. к. они конфликтуют с программным обеспечением брандмауэра ISA Server 2004.

16. Щелкните кнопку Install (Установить) на странице Ready to Install the Program (Установка программы).

17. На странице Installation Wizard Completed (Завершение работы мастера установки) нажмите кнопку Finish (Готово).

18. Щелкните кнопку Yes (Да) в диалоговом окне Microsoft ISA Server, в котором сообщается, что нужно перезапустить сервер.

19. Выполните вход в систему как администратор после перезапуска компьютера.

20. Нажмите кнопку Start (Пуск) и установите курсор на All Programs (Программы). Установите курсор на Microsoft ISA Server и выберите пункт ISA Server Management. Откроется консоль управления Microsoft Internet Security and Acceleration Server 2004, и появится страница Welcome to Microsoft Internet Security and Acceleration Server 2004.

Конфигурирование брандмауэра ISA

Теперь можно настроить политику доступа на брандмауэре ISA. Нужно создать пять правил доступа:

• правило, разрешающее клиентам внутренней сети доступ к DHCP-серверу на брандмауэре ISA;

• правило, разрешающее брандмауэру ISA отправлять DHCP-сообщения хостам во внутренней сети;

• правило, разрешающее DNS-серверу внутренней сети использовать брандмауэр ISA в качестве своего DNS-сервера. Это правило следует создавать, только если во внутренней сети имеется DNS-сервер;

• правило, разрешающее клиентам внутренней сети доступ к DNS-серверу в режиме только кэширования на брандмауэре ISA. Это правило используется, только если во внутренней сети нет DNS-сервера или если нужно использовать брандмауэр ISA в качестве DNS-сервера в режиме только кэширования с зоной-заглушкой, указывающей на домен внутренней сети;

• правило «все открыто», разрешающее клиентам внутренней сети доступ ко всем протоколам и узлам Интернета.

В табл. 7 – 11 представлена подробная информация о каждом из этих правил.

Табл.7. Правило для запроса к DHCP-серверу

Название	DHCP Request to Server (запрос к PHCP-серверу)
Действие	Разрешающее
Протоколы	DHCP (запрос)
Источник	Любой
Адресат	Локальный хост
Пользователи	Все
График	Всегда

Типы содержимого	Все
Назначение	Это правило разрешает DHCP-клиентам отправлять DHCP-запросы на DHCP-сервер, установленный на брандмауэре ISA

Литература

1 Томас В. Шиндер, Дебра Л. Шиндер / ISA Server 2004. – БХВ-Петербург, Русская Редакция, 2005. – 1064 с.