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). ПОСТРОЕНИЕ VPN-СЕТИ НА БАЗЕ 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

1. Обзор использования VPN межсетевым экраном ISA.

Создание VPN-сервера на базе брандмауэра ISA 2004 — это решение, дающее администраторам именно такой уровень контроля доступа. Когда VPN-клиенты соединяются с VPN-сервером, они помещаются во встроенный сетевой объект, названный *VPN Clients Network (сеть VPN-клиентов).* Брандмауэр ISA 2004 трактует эту сеть, как любую другую, что означает возможность строгого, ориентированного на пользователей/группы контроля данных, перемещающихся между сетью VPN-клиентов и корпоративной сетью.

Все, что для этого требуется, — *создать* учетные записи пользователей и сформировать политику доступа на брандмауэре ISA 2004/VPN-сервере, ограничивающую машины и протоколы, которые пользователи/группы могут использовать, и все эти сетевые компоненты будут защищены от доступа VPN-пользователей удаленного доступа.

1.1 Политика брандмауэра, применяемая к VPN-соединениям конфигурации узел-в-узел

VPN-соединение с конфигурацией узел-в-узел соединяет две или несколько сетей (а не отдельный клиент и сеть) через Интернет. Использование VPN-канала конфигурации узел-в-узел может дать существенное снижение себестоимости по сравнению с выделенными соединениями (dedicated link) WAN (Wide-Area Network, глобальная сеть), использующими выделенные каналы (dedicated circuits) (например, соединение двух сайтов с помощью специализированной многоканальной телефонной линии T-1).

Для применения VPN-соединения узел-в-узел каждому сайту нужен VPN-шлюз и сравнительно недорогое Интернет-соединение. Когда VPN-шлюзы установят соединения друг с другом, VPN-соединение типа узел-в-узел установлено. Далее пользователи на каждом конце соединения могут связываться с другими сетями через VPN-соединение типа узел-в-узел так, как они это делали бы с помощью маршрутного соединения в их собственной сети. VPN-шлюзы действуют как маршрутизаторы и пересылают пакеты в соответствующую сеть.

В VPN-соединениях конфигурации узел-в-узел используются те же технологии, что и в VPN-соединениях (удаленного доступа) типа клиент-сервер, и обычно они сталкиваются с той же проблемой безопасности. Все пользователи получают доступ ко всей сети, с которой соединена их собственная сеть. Единственное, что может оградить пользователей от самовольного доступа к ресурсам без разрешения, — локальные средства управления доступом на серверах.

VPN-соединения конфигурации узел-в-узел обычно устанавливаются между сетями филиала и центрального офиса. Предоставление пользователям филиала доступа ко всей сети центрального офиса может создать серьезную угрозу безопасности ресурсов.

Брандмауэр ISA 2004/VPN-сервер может, контролировать исходящие данные, которые передаются по каналу узел-в-узел. Доступ пользователей филиала можно ограничить только теми ресурсами сети центрального офиса, которые нужны им для работы, и таким образом помешать доступу к другим сетевым ресурсам центрального офиса. Как и VPN-клиентам удаленного доступа, пользователям филиала следует разрешить применение только определенных протоколов, требующихся на серверах, к которым пользователи получили доступ.

1.2 VPN-карантин

Временная изоляция, или VPN-карантин (VPN-Q), — новое свойство, позволяющее тщательно проверять машины VPN-клиентов, прежде чем разрешить им доступ к корпоративной сети. VPN-карантин, включенный в состав ISA Server 2004, подобен сетевому

карантину служб маршрутизации и удаленного доступа (RRAS) в операционной системе Windows Server 2003.

Для использования VPN-Q нужно создать модуль CMAK (Connection Manager Administration Kit, комплект администрирования менеджера соединений), включающий сценарий VPN-Q клиента (VPN-Q client) и VPN-Q клиентской стороны (VPN-Q client-side). Клиент запускает сценарий и передает результаты серверному компоненту VPN-Q на брандмауэре ISA 2004/VPN-сервере. VPN-клиент перемещается из сети «VPN Quarantine» (VPN-карантин) в сеть «VPN Clients» (VPN-клиенты), если сценарий сообщает, что клиент соответствует требованиям, предъявляемым к сетевым соединениям. Вы можете задать для хостов в сети VPN-карантина политику доступа, отличающуюся от политики доступа сети VPN-клиентов.

1.3 Отображение пользователей для VPN-клиентов

Отображение пользователей (User mapping) — способ, позволяющий отображать клиентов виртуальной частной сети, соединяющихся с ISA Server, с помощью метода аутентификации, отличного от «Windows-аутентификации» (например, RADIUS-или EAP-аутентификация), в пространство имен Windows. Включенное и должным образом настроенное отображение пользователей дает возможность применять к пользователям, подтвердившим подлинность без применения Windows-аутентификации, политику правил доступа брандмауэра, определяющую наборы пользователей для пользователей и групп ОС Windows. По умолчанию политика правил доступа брандмауэра не распространяется на пользователей из других (не Windows) пространств имен до тех пор, пока не определено отображение пользователей.

Функциональная возможность отображения пользователей расширяет набор мощных, основанных на пользователе/группе средств управления доступом, которые можно применять к VPN-клиентам, использующим метод аутентификации, отличный от Windows-аутентификации.

1.4 VPN конфигурации узел-в-узел с применением туннельного режима протокола IPSec

Брандмауэры ISA 2004 позволяют использовать туннельный режим протокола IPSec для соединений конфигурации узел-в-узел между VPN-шлюзом брандмауэра ISA 2004 и VPN-шлюзом стороннего производителя. Кроме того, что вы можете применять протокол PPTP или протокол L2TP/ IPSec с высоким уровнем защиты для создания каналов типа узел-в-узел между двумя брандмауэрами ISA Server/VPN-шлюзами, брандмауэр ISA 2004 позволяет использовать плохо защищенное соединение *с* применением туннельного режима протокола IPSec для подключения к VPN-шлюзам сторонних фирм.

Туннельный режим протокола IPSec поддерживается только для VPN-соединений конфигурации узел-в-узел. Клиент-серверные VPN-соединения удаленного доступа тем не менее используют только протоколы PPTP или L2TP/IPSec. Туннельный режим протокола IPSec уязвим для нескольких хорошо известных атак, а протокол L2TP/IPSec требует более строгой аутентификации и не подвержен этим атакам. Таким образом, если есть выбор, гораздо лучше применять набор протоколов L2TP/IPSec для VPN-соединений конфигурации узел-в-узел.

1.5 Поддержка аутентификации секретным ключом в VPN-соединениях по протоколу IPSec

В брандмауэре ISA Server 2004, когда создаются VPN-соединения удаленного доступа и межшлюзовые VPN-соединения, можно использовать секретные ключи (pre-shared keys) вместо сертификатов. Все машины VPN-клиентов, на которых выполняется обновленное программное обеспечение VPN-клиента для протокола L2TP/IPSec, могут использовать секретный ключ для создания соединения удаленного доступа VPN-клиента по протоколу L2TP/IPSec с брандмауэром ISA 2004/VPN-сервером. VPN-шлюзы ОС Windows 2000 и Windows Server 2003 также можно настроить для применения секретного ключа и установки соединений узел-в-узел.

Имейте в виду, что отдельный сервер удаленного доступа может использовать только один секретный ключ (pre-shared key) для всех соединений по протоколу L2TP/IPSec, требующему секретный ключ для аутентификации. Необходимо предоставить один и тот же секретный ключ (pre-shared key) всем VPN-клиентам, соединяющимся по протоколу L2TP/IPSec с сервером удаленного доступа, который использует секретный ключ.

1.6 Мониторинг соединений VPN-клиентов

В брандмауэре ISA Server 2004 существует политика брандмауэра ко *всем* соединениям с брандмауэром, включая VPN-соединения. Можно воспользоваться программой просмотра журнала регистрации в режиме реального времени для проверки действующих соединений VPN-клиентов удаленного доступа и установить в ней фильтр для вывода только VPN-соединений. Если соединения регистрируются в машине базы данных MSDE (Microsoft Data Engine), можно запросить базу данных и вывести хронологический список VPN-соединений. В брандмауэре ISA 2004/VPN-сервере вы не только получаете полную информацию о том, кто подключился к брандмауэру ISA 2004/VPN, но и сведения о том, к каким ресурсам обращались эти пользователи и какие протоколы они использовали для подключения к ресурсам.

Например, можно задать критерии VPN-фильтрации в программе просмотра регистрационного журнала, если воспользоваться прямой регистрацией (live logging) и сохранить регистрации в файле. Применяя запись журналов регистрации в файл, нельзя запросить у программы просмотра регистрационных журналов брандмауэра ISA архивные данные. Но можно фильтровать и отслеживать в реальном времени VPN-соединения в программе просмотра регистрационного журнала. Кроме того, можно фильтровать VPN-соединения для отображения сеансов (Sessions view) или регистрации (Log view).

2. Создание VPN-сервера удаленного доступа по протоколу PPTP

2.1 Включение VPN-сервера

Необходимо включить компонент VPN-сервера, так как он по умолчанию отключен. Первый шаг — активизация функции VPN-сервера и конфигурирование его компонентов. Делается это на консоли управления Microsoft Internet Security and Acceleration Server 2004 (Сервер защищенного быстрого доступа к сети Интернет 2004), а не на консоли сервиса RRAS.

Выполните следующие шаги для включения и настройки VPN-сервера ISA 2004.

1. Откройте консоль управления Microsoft Internet Security and Acceleration Server 2004 (Сервер защищенного быстрого доступа к сети Интернет 2004) и раскройте окно, связанное с именем сервера. Щелкните кнопкой мыши узел Virtual Private Networks (VPN) (Виртуальные частные сети).
2. Щелкните мышью вкладку Tasks (Задачи) на панели задачи. Щелкните кнопкой мыши ссылку Enable VPN Client Access (Разрешить доступ VPN-клиентов).

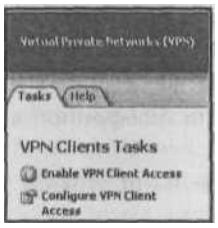


Рис. 9.1. Ссылка Enable VPN Client Access (Разрешить доступ VPN-клиентов)

3. Щелкните мышью кнопку Apply (Применить) для сохранения изменений и обновления политики брандмауэра.

4. Щелкните мышью кнопку OK в диалоговом окне Apply New Configuration (Применить новую конфигурацию).

5. На вкладке Tasks (Задачи) щелкните кнопкой мыши ссылку Configure VPN Client Access (Настроить доступ VPN-клиента).

6. На вкладке General (Общие) (рис. 9.2) в диалоговом окне VPN Clients Properties (Свойства VPN-клиентов) измените значение параметра Maximum number of VPN clients allowed (Максимальное число разрешенных VPN-клиентов) с 5 на 10. Версия Standard Edition брандмауэра ISA поддерживает до 1000 параллельных VPN-соединений. Это жестко заданный предел, и он не меняется независимо от количества VPN-соединений, поддерживаемых операционной системой Windows, в которой установлен брандмауэр ISA. У версии Enterprise edition брандмауэра ISA нет жестко заданного лимита и количество поддерживаемых VPN-соединений определяется базовой операционной системой. Точно число неизвестно, но если брандмауэр ISA установлен в ОС Windows Server 2003 версии Enterprise, вы можете создать к брандмауэру ISA 1б 000 VPN-подключений по протоколу PPTP и 30 000 — по протоколу L2TP/IPSec.

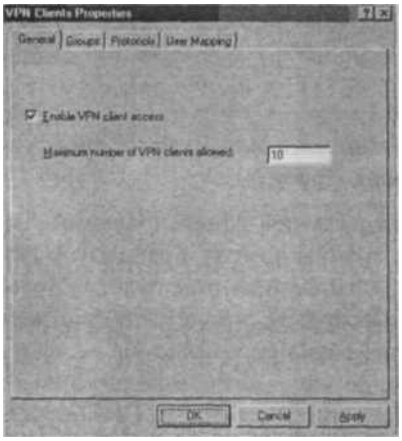


Рис. 9.2. Вкладка General (Общие)

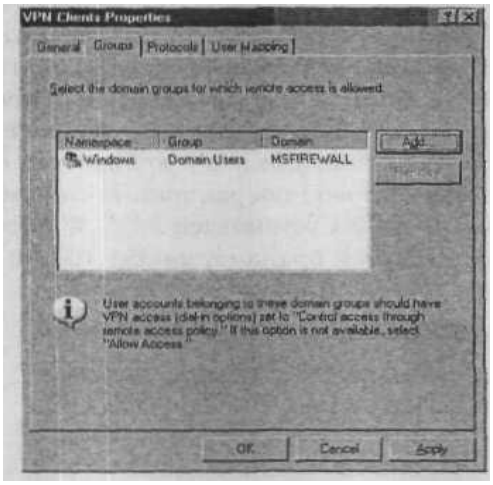
Убедитесь, что имеется количество IP-адресов для VPN-клиентов, по меньшей мере, равное числу, указанному в текстовом поле Maximum number of VPN clients allowed (Максимальное число разрешенных VPN-клиентов). Определите количество VPN-клиентов, которые необходимо соединить с брандмауэром ISA, а затем добавьте единицу для самого брандмауэра ISA. Это и будет число, которое нужно ввести в данное текстовое поле.

8. Щелкните кнопкой мыши вкладку Groups (Группы). На этой вкладке щелкните мышью кнопку Add (Добавить).

9. В диалоговом окне Select Groups (Выберите группы) щелкните мышью кнопку Locations (Местонахождения). В диалоговом окне Locations (Местонахождения) щелкните кнопкой мыши адрес msfirewall.org, а затем кнопку OK.

10. В диалоговом окне Select Groups (Выберите группы) в текстовое поле Enter the object names to select (Введите имена выбранных объектов) введите Domain Users (Пользователи домена). Щелкните мышью кнопку Check Names (Проверить имена). Как только имя группы будет найдено в базе данных Active Directory, оно будет подчеркнуто. Щелкните

мышью кнопку ОК.



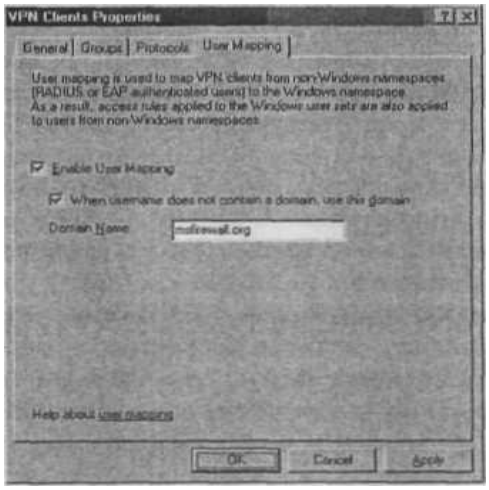


Рис. 9.3.-9.4. Group и User Mapping

11. Щелкните кнопкой мыши вкладку User Mapping (Отображение пользователя) (рис. 9.4). Установите флажок Enable User Mapping (Разрешить отображение пользователей) и флажок When username does not contain a domain, use this domain (Если имя пользователя не содержит имя домена, использовать данный домен). Введите имя msfirewall.org в текстовое поле Domain Name (Имя домена). Имейте в виду, что эти установки будут применяться при использовании аутентификации RADIUS/EAR Они игнорируются, когда используется аутентификация Windows (например, когда машина с брандмауэром ISA 2004 принадлежит домену и пользователь явно вводит верительные данные домена). Щелкните мышью кнопки Apply (Применить) и ОК. Вы увидите диалоговое окно Microsoft Internet Security and Acceleration Server 2004 (Сервер защищенного быстрого доступа к сети Интернет 2004), информирующее вас о том, что необходимо перезапустить компьютер для ввода в действие установленных параметров. Если так, щелкните мышью кнопку ОК в диалоговом окне

12. На вкладке Tasks (Задачи) щелкните кнопкой мыши строку Select Access Networks (Выбрать сети доступа).

13. В диалоговом окне Virtual Private Networks (VPN) Properties (Свойства виртуальных частных сетей) (рис. 9.5) щелкните кнопкой мыши вкладку Access Networks (Сети доступа). Обратите внимание на то, что установлен флажок External (Внешняя). Это означает, что внешний интерфейс ожидает входящие соединения от VPN-клиентов.

Если вы хотите внутренних пользователей подключить к брандмауэру ISA, выберите флажок Internal (Внутренняя) Есть также варианты, разрешающие VPN-подключения из All Networks (and Local Host Network) (Все сети, и сеть локального хоста) и All Protected

Networks (Все защищенные сети).

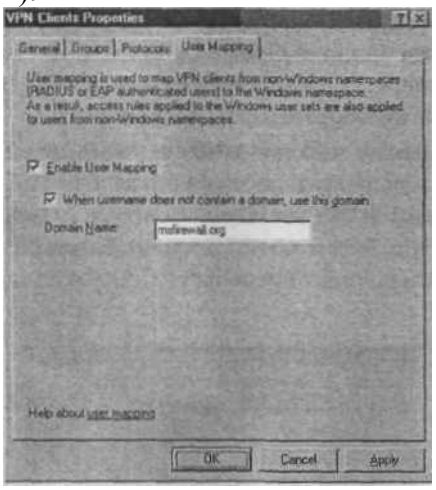


Рис. 9.5. Выбор и настройка параметров сетей доступа

14. Щелкните кнопкой мыши вкладку Address Assignment (Назначение адреса) (рис. 9.6). Выберите в раскрывающемся списке Use the following network to obtain DHCP, DNS and WINS services (Использовать следующую сеть для получения сервисов DHCP, DNS и WINS) элемент Internal (Внутренняя). Это важная установка, поскольку она определяет сеть, в которой осуществляется доступ к сервису DHCP.

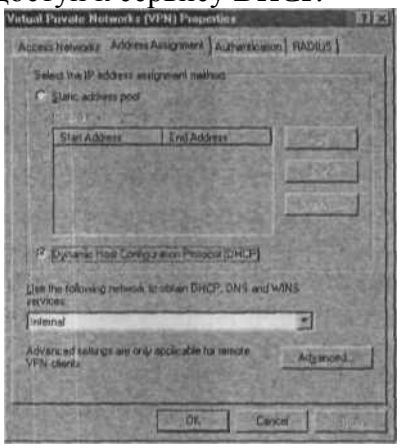


Рис. 9.6. Вкладка Address Assignment (Назначение адреса)

Можно назначить VPN-клиентам адреса сервера имен, не зависящие от конфигурации сервера имен и любого интерфейса брандмауэра ISA. Щелкните мышью кнопку Advanced (Дополнительно) и увидите диалоговое окно Name Resolution (Разрешение имен). По умолчанию установлены переключатели Obtain DNS server addresses using DHCP configuration (Получать адреса DNS-сервера с помощью DHCP-конфигурации) и Obtain WINS server addresses using DHCP configuration (Получать адреса сервера WINS с помощью DHCP-конфигурации). Конечно, невозможно получить параметры DHCP (Dynamic Host Configuration Protocol, протокол динамической конфигурации хоста) для VPN-клиентов, пока на брандмауэре ISA не установлен и не настроен DHCP Relay Agent (агент ретрансляции DHCP). Сервис RRAS брандмауэра ISA будет получать только блоки IP-адресов для VPN-клиентов, а не варианты DHCP.

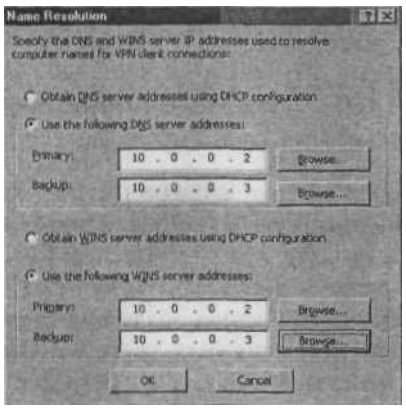


Рис. 9.7. Диалоговое окно Name Resolution (Разрешение имен

15. Щелкните кнопкой мыши вкладку Authentication (Аутентификация) (рис. 9.7). Отметьте, что установлен только флажок Microsoft encrypted authentication version 2 (MS-CHAPv2) (Шифрованная аутентификация версии 2, Протокол проверки подлинности запроса-подтверждения Microsoft версии 2). Для обеспечения самого высокого уровня безопасности аутентификации установите флажок Extensible authentication protocol (EAP) with smart card or other certificate (Наращиваемый протокол аутентификации, (EAP) с помощью смарт-карты или другого сертификата).

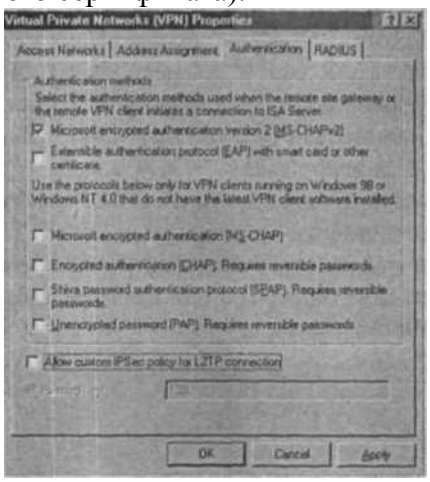


Рис. 9.9. Вкладка Authentication (Аутентификация)

16. Щелкните кнопкой мыши вкладку RADIUS (Remote Authentication Dial-In User Service, служба аутентификации удаленного дозванивающегося (коммутируемого) пользователя). На этой вкладке можно настроить VPN-сервер брандмауэра ISA 2004 для применения аутентификации VPN-пользователей с помощью сервиса RADIUS. Преимущество подтверждения подлинности средствами RADIUS заключается в том, что можно привлечь базу данных пользователей службы Active Directory (или других каталогов) для аутентификации пользователей без обязательного членства в домене брандмауэра ISA. Мы подробно рассмотрим способы конфигурирования сервиса RADIUS для поддержки аутентификации VPN-пользователей позже в этой главе

17. В диалоговом окне Virtual Private Networks (VPN) Properties (Свойства виртуальных частных сетей) щелкните мышью кнопку Apply (Применить) и затем кнопку ОК.

18. Щелкните мышью кнопку Apply (Применить) для сохранения изменений и обновления политики брандмауэра.

19. Щелкните мышью кнопку ОК в диалоговом окне Apply New Configuration (Применить новую конфигурацию).

20. Перезапустите машину с брандмауэром ISA.

2.2 Создание правила доступа, предоставляющего VPN-клиентам доступ к разре-

шенным ресурсам

Выполните следующие шаги для создания правила доступа, обеспечивающего неограниченный доступ для VPN-клиентов.

1. На консоли управления The Microsoft Internet Security and Acceleration Server 2004 (Сервер защищенного быстрого доступа к сети Интернет 2004), раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел Firewall Policy (Политика брандмауэра). Щелкните правой кнопкой мыши узел Firewall Policy (Политика брандмауэра), укажите левой кнопкой мыши команду New (Новое) и затем Access Rule (Правило доступа).
2. На странице Welcome to the New Access Rule Wizard (Вас приветствует мастер создания нового правила доступа) введите название правила в текстовое поле Access Rule name (Название правила доступа). В данном примере — VPN Client to Internal. Щелкните мышью кнопку Next (Далее).
3. На странице Rule Action (Действие правила) выберите вариант Allow (Разрешить) и щелкните мышью кнопку Next (Далее).
4. На странице Protocols (Протоколы) выберите вариант All outbound protocols (Все исходящие протоколы) в списке This rule applies to (Это правило применяется к). Щелкните мышью кнопку Next (Далее).
5. На странице Access Rule Sources (Источники в правиле доступа) щелкните мышью кнопку Add (Добавить). В диалоговом окне Add Network Entities (Добавить сетевые объекты) щелкните кнопкой мыши папку Networks (Сети) и дважды щелкните мышью узел VPN Clients (VPN-клиенты). Щелкните мышью кнопку Close (Закрыть).
6. Щелкните мышью кнопку Next (Далее) на странице Access Rule Sources (Источники в правиле доступа).
7. На странице Access Rule Destinations (Адресаты в правиле доступа) щелкните мышью кнопку Add (Добавить). В диалоговом окне Add Network Entities (Добавить сетевые объекты) щелкните кнопкой мыши папку Networks (Сети) и дважды щелкните мышью узел Internal (Внутренняя). Щелкните мышью кнопку Close (Закрыть).
8. На странице User Sets (Наборы пользователей) согласитесь с установкой по умолчанию All Users (Все пользователи) и щелкните мышью кнопку Next (Далее).
9. Щелкните кнопку Finish (Готово) на странице Completing the New Access Rule Wizard (Завершение мастера создания нового правила).
10. Щелкните мышью кнопку Apply (Применить) для сохранения изменений и обновления политики брандмауэра.
11. Щелкните мышью кнопку ОК в диалоговом окне Apply New Configuration (Применить новую конфигурацию). Политика VPN-клиента теперь отражена в верхнем правиле доступа, приведенном в списке политики доступа.

2.3 Разрешение удаленного доступа по телефонной линии

В доменах Active Directory, находящихся в неосновном режиме (non-native mode), для всех учетных записей пользователей по умолчанию удаленный доступ по телефонной линии (dial-in) запрещен. Вы должны разрешить такой доступ, основываясь на учетных записях для этих доменов Active Directory, находящихся в неосновном режиме. Напротив, в доменах Active Directory, находящихся в основном режиме (native mode), по умолчанию удаленный доступ по телефонной линии управляется политикой удаленного доступа (Remote Access Policy). В доменах ОС Windows NT 4.0 удаленный доступ по телефонной ли-

нии управляется посредством учетных записей пользователя.

В лаборатории, технические средства которой применялись для написания этой книги, служба Active Directory в смешанном режиме (mixed mode) установлена в ОС Windows Server 2003, поэтому нам понадобилось вручную изменить установки для удаленного доступа по телефонной линии в каждой учетной записи пользователя домена, которой требуется доступ к VPN-серверу.

Выполните следующие шаги на контроллере домена для разрешения удаленного доступа по телефонной линии для учетной записи Administrator.

1. Щелкните мышью кнопку Start (Пуск) и строку Administrative Tools (Администрирование). Щелкните мышью оснастку Active Directory Users and Computers (Active Directory — пользователи и компьютеры).
2. В оснастке Active Directory Users and Computers (Active Directory' - пользователи и компьютеры) щелкните мышью узел Users (Пользователи) на левой панели. Дважды щелкните кнопкой мыши учетную запись Administrator на правой панели оснастки.
3. Щелкните кнопкой мыши вкладку Dial-in (Соединение по телефонной линии). В области Remote Access Permission (Dial-in or VPN) (Разрешение удаленного доступа, по модему или через сеть VPN) выберите переключатель Allow access (Разрешить доступ). Щелкните мышью кнопку Apply (Применить) и затем кнопку ОК.
4. Закройте оснастку Active Directory Users and Computers (Active Directory - пользователи и компьютеры).

Другой вариант — создать группы на самом брандмауэре ISA и поместить их в группы. Этот метод позволит применить установочные параметры по умолчанию в учетных записях пользователей, созданных на брандмауэре, для которых по умолчанию выбран для удаленного доступа по телефонной линии Control access via Remote Access Policy (Контроль доступа с помощью политики удаленного доступа).

Несмотря на то, что этот вариант не слишком хорошо регулируется, он вполне жизнеспособен в тех организациях, у которых ограниченное количество VPN-пользователей и которые не хотят применять подтверждения подлинности с помощью системы RADIUS или не имеют RADIUS-сервер а для использования.

Выполните следующие шаги для создания группы пользователей, имеющих доступ к VPN-серверу брандмауэра ISA.

1. На рабочем столе брандмауэра ISA щелкните правой кнопкой пиктограмму My Computer (Мой компьютер) и щелкните левой кнопкой мыши команду Manage (Управление).
2. На консоли Computer Management (Управление компьютера) раскройте узел System Tools (Служебные программы) и затем узел Local Users and Groups (Локальные пользователи и группы). Щелкните правой кнопкой мыши папку Groups (Группы) и левой кнопкой мыши щелкните команду New Group (Новая группа).
3. В диалоговом окне New Group (Новая группа) введите имя группы в текстовое поле Group Name (Имя группы). В данном примере мы назовем группу VPN Users. Щелкните мышью кнопку Add (Добавить).
4. В диалоговом окне Select: users (Выбор: пользователи) щелкните мышью кнопку Advanced (Дополнительно).
5. В диалоговом окне Select: users (Выбор: пользователи) выберите пользователей или группы, которые вы хотите сделать членами группы VPN Users. В этом примере мы выберем Authenticated Users (Аутентифицированные пользователи). Щелкните мышью кнопку ОК.
6. Щелкните мышью кнопку ОК в диалоговом окне Select: users (Выбор: пользователи).
7. Щелкните мышью кнопку Create (Создать), а затем кнопку Close (Закрыть).

Теперь настроим компонент VPN-сервера брандмауэра ISA для разрешения доступа

членам группы VPN Users.

1. На консоли управления Microsoft Internet Security and Acceleration Server 2004 (Сервер защищенного быстрого доступа к сети Интернет 2004) раскройте окно, связанное с именем сервера, и щелкните кнопкой мыши узел Virtual Private Networking (VPN) (Виртуальные частные сети). Щелкните кнопкой мыши строку Configure VPN Client Access (Конфигурировать доступ VPN-клиента) на вкладке Tasks (Задачи) на панели задачи.

2. В диалоговом окне VPN Clients Properties (Свойства VPN-клиентов) щелкните мышью кнопку Add (Добавить).

3. В диалоговом окне Select Groups (Выберите группы) введите VPN Users в текстовое поле Enter the object name to select (Введите имя выбранного объекта) и щелкните мышью кнопку Check Names (Проверить имена). Найденное имя
группы будет подчеркнуто. Щелкните мышью кнопку ОК.

В данном примере мы ввели локальную группу VPN Users на вкладке Groups (Группы), потому что VPN-доступ может контролироваться с помощью режима Control access through Remote Access Policy (Контроль доступа с помощью политики удаленного доступа), установленного для учетных записей пользователей в локальном диспетчере SAM (Security Accounts Manager, диспетчер учетных записей безопасности) брандмауэра ISA. Вы также можете ввести пользователей и группы домена (если брандмауэр ISA является членом домена пользователей), если домен поддерживает удаленный доступ по телефонной линии с помощью политики удаленного доступа. Мы поговорим более подробно о пользователях и группах домена и политике удаленного доступа позже в этой главе

4. Щелкните мышью кнопку Apply (Применить), а затем кнопку ОК в диалоговом окне VPN Client Properties (Свойства VPN-клиентов).

5. Щелкните мышью кнопку Apply (Применить) для сохранения изменений и обновления политики брандмауэра.

6. Щелкните мышью кнопку ОК в диалоговом окне Apply New Configuration (Применить новую конфигурацию).

2.4 Тестирование VPN-соединения по протоколу PPTP

Теперь VPN-сервер брандмауэра ISA 2004 готов для приема соединений от VPN-клиентов. Установите пиктограмму (connectoid) VPN-соединения на вашем VPN-клиенте и затем установите VPN-соединение с брандмауэром ISA. В тестовой лаборатории при подготовке этой книги мы использовали клиент под управлением ОС Windows XP с установленным Service Pack 1.

Выполните следующие шаги для тестирования VPN-сервера.

1. На машине внешнего клиента с ОС Windows XP щелкните правой кнопкой мыши пиктограмму **My Network Places** (Сетевое окружение) на рабочем столе и выберите команду **Properties** (Свойства).

2. Дважды щелкните кнопкой мыши строку **New Connection Wizard** (Мастер новых подключений) в окне **Network Connections** (Сетевые подключения).

3. Щелкните мышью кнопку **Next** (Далее) на странице **Welcome to the New Connection Wizard** (Вас приветствует мастер новых подключений).

4. На странице **Network Connection Type** (Тип сетевого подключения) выберите переключатель **Connect to a private network at my workplace** (Подключить к сети на рабочем месте) и щелкните мышью кнопку **Next** (Далее).

5. На странице **Network Connection** (Сетевое подключение) выберите переключатель **Virtual Private Network connection** (Подключение к виртуальной
частной сети) и щелкните мышью кнопку **Next** (Далее).

6. На странице **Connection Name** (Имя подключения) введите **VPN** в текстовое поле **Company Name** (Организация) и щелкните мышью кнопку **Next** (Далее).

7. На странице **VPN Server Selection** (Выбор VPN-сервера) введите IP-адрес на внеш-

нем интерфейсе брандмауэра ISA (в данном примере — 192.168.1,70) в текстовое поле **Host name or IP address** (Имя компьютера или IP-адрес). Щелкните мышью кнопку **Next** (Далее).

8. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Connection Wizard** (Завершение Мастера новых подключений).

9. В диалоговом окне **Connect VPN** (VPN-подключение) введите имя пользователя **Administrator** и пароль для учетной записи администратора (если брандмауэр ISA — член домена, введите имя компьютера или имя домена перед именем пользователя в формате NAME\username). Щелкните мышью кнопку **Connect** (Подключиться).

10. VPN-клиент устанавливает соединение с VPN-сервером брандмауэра ISA 2004. Щелкните мышью кнопку ОК в диалоговом окне **Connection Complete** (Соединение установлено), информирующем об установке соединения.

11.Дважды щелкните кнопкой мыши пиктограмму соединения на системной панели задач, а затем щелкните мышью вкладку **Details** (Сведения). Вы увидите шифрование **MPPE 128** (Microsoft Point-to-Point Encryption), применяемое для защиты данных, и IP-адрес, назначенный VPN-клиенту. Щелкните мышью кнопку **Close** (Закрыть).

12. Если вы используете лабораторную установку, описанную в этой книге, щелкните мышью кнопку **Start** (Пуск), а затем команду **Run** (Выполнить). В диалоговом окне **Run** введите **\\EXCHANGE2003BE** в текстовое поле **Open** (Открыть) *к* щелкните мышью кнопку ОК. Появятся ресурсы, совместно используемые (shares) на компьютере контроллера домена. Закройте окна, отображающие содержимое контроллера домена. Обратите внимание на то, что мы могли использовать имя без доменного суффикса (single label name) для соединения с контроллером домена, потому что брандмауэр ISA назначил VPN-клиенту адрес сервера WINS. Имя без доменного суффикса сработало бы и в случае DNS-запроса, если бы машина VPN-клиента была настроена на полное определение имен без доменного суффикса с помощью корректного имени домена.

13. Щелкните правой кнопкой мыши по пиктограмме соединения на панели задач и щелкните левой кнопкой мыши кнопку **Disconnect** (Отключить).

3. Поддержка исходящих VPN-соединений через брандмауэр ISA

Можно конфигурировать брандмауэр ISA для разрешения исходящего доступа к VPN-серверам в Интернет**.** Брандмауэр ISA поддерживает все действительные (true) VPN-протоколы, включая PPTP, L2TP/IPSec и IPSec NAT Traversal (NAT-T) (обходящий NAT по протоколу IP-безопасности).

Брандмауэр ISA может пропускать VPN-подключения по протоколу PPTP из любой защищенной сети к Интернету с помощью своего PPTP-фильтра. PPTP-фильтр брандмауэра ISA перехватывает соединение от клиента защищенной сети и служит промежуточным звеном для сообщений по протоколу GRE (Generic Routing Encapsulation/IP Protocol 47, обобщенная инкапсуляция маршрутизации) и канала управления (TCP 1723) протокола PPTP. Единственное, что от вас требуется, — создать правило доступа, разрешающее исходящий доступ по протоколу PPTP.

Выполните следующие шаги для разрешения исходящего доступа по протоколу PPTP через брандмауэр ISA.

1. На консоли управления **Microsoft Internet Security and Acceleration Server 2004** (Сервер защищенного быстрого доступа к сети Интернет Server 2004), раскройте окно, связанное с именем сервера, щелкните кнопкой мыши узел **Firewall Policy** (Политика брандмауэра).
2. В узле **Firewall Policy** (Политика брандмауэра) щелкните кнопкой мыши вариант **Create New Access Rule** (Создать новое правило доступа) на вкладке **Tasks** (Задачи) на панели задач.
3. На странице **Welcome to the New Access Rule Wizard** (Вас приветствует мастер создания нового правила) введите название правила в текстовое поле **Rule name** (Название

правила). В данном примере — **Outbound PPTP for Administrators.** Щелкните мышью кнопку **Next** (Далее).

4. На странице **Rule Action** (Действие правила) выберите вариант **Allow** (Разрешить) и щелкните мышью кнопку **Next** (Далее).

5. На странице **Protocols** (Протоколы) выберите строку **Selected protocols** (Выбранные протоколы) из списка **This rule applies to** (Это правило применяется к). Щелкните мышью кнопку **Add** (Добавить).

6. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **VPN and IPSec** и дважды щелкните по элементу **PPTP.** Щелкните мышью кнопку **Close** (Закрыть).

7. Щелкните мышью кнопку **Next** (Далее) на странице **Protocols** (Протоколы).

8. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните мышью папку **Computer Sets** (Наборы компьютеров) и дважды щелкните мышью элемент **Remote Management Computers** (Компьютеры удаленного управления). Щелкните мышью кнопку **Close** (Закрыть).

9. Щелкните мышью кнопку **Next** (далее) на странице **Access Rule Sources** (Источники правила доступа).

10. На странице **Access Rule Destinations** (Адресаты в правиле доступа) щелкните мышью кнопку **Add** (Добавить).

11. В диалоговом окне **Add Network Entities** (Добавить сетевые объекты) щелкните кнопкой мыши пункт меню **New** (Новый) и команду **Computer** (Компьютер).

12. В диалоговом окне **New Computer Rule Element** (Новый элемент правила, компьютер) введите имя внешнего VPN-сервера в текстовое поле **Name** (Имя). Введите IP-адрес авторизованного VPN-сервера в текстовое поле **Computer IP Address** (IP-адрес компьютера). В данном примере — **Authorized VPN Server.** Щелкните мышью кнопку ОК.

13. Щелкните кнопкой мыши папку **Computers** (Компьютеры). Дважды щелкните кнопкой мыши элемент **Authorized VPN Server.** Щелкните мышью кнопку **Close** (Закрыть).

14. Щелкните мышью кнопку Next (Далее) на странице **Access Rule Destinations** (Адресаты в правиле доступа).

15. Щелкните мышью кнопку Next (Далее) на странице **User Sets** (Наборы пользователей).

16. Щелкните мышью кнопку **Finish** (Готово) на странице **Completing the New Access Rule Wizard** (Завершение мастера создания нового правила).

Литература

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