Настройка туннеля IPSec – концентратор Cisco VPN 3000 к межсетевому экрану Checkpoint 4.1

Содержание

Введение

Этот документ демонстрирует, как сформировать туннель IPSec с предварительными ключами для соединения 2-х частных сетей:

внутренняя частная сеть концентратора Cisco VPN 3000 (192.168.1.x);

внутренняя частная сеть межсетевого экрана Checkpoint 4.1 (10.32.50.x).

Предполагается, что поток трафика из внутренней сети концентратора VPN и внутренней сети межсетевого экрана Checkpoint 4.1 в Интернет (представленный здесь сетями 172.18.124.X) существует до начала настройки этой конфигурации.

Предварительные условия

Требования

Для этого документа нет особых требований.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

Концентратор VPN 3000

Выпуск ПО 2.5.2.F на концентраторе VPN 3000

Межсетевой экран Checkpoint 4.1

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе в действующей сети необходимо понимать последствия выполнения любой команды.

Схема сети

В настоящем документе используется следующая схема сети:

Условные обозначения

Подробные сведения об условных обозначениях см. в документе Условное обозначение технических терминов Cisco.

Настройка концентратора VPN 3000

Для настройки концентратора VPN 3000 выполните следующие шаги.

Выберите **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals > Modify** (Конфигурация > Система > Протоколы туннелирования > IPSec > Предложения IKE > Изменить) для создания предложения обмена ключами в Интернете (IKE) под названием des-sha с хэшированием по алгоритму защищенного хэша (SHA), шифрованием по стандарту DES и 1-й группой Диффи-Хелмана. В поле Lifetime (Срок действия) оставьте значение по умолчанию – 86400 секунд.

Примечание. Диапазон допустимых значений срока действия IKE для концентратора VPN составляет от 60 до 2147483647 секунд.

Выберите **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals** (Конфигурация > Система > Протоколы туннелирования > IPSec > Предложения IKE). Для активации предложения IKE выберите des-sha и нажмите кнопку **Activate** (Активировать).

Выберите **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add** (Конфигурация > Система > Протоколы туннелирования > IPSec LAN–LAN > Добавить).

Задайте туннель IPsec to_checkpoint с адресом Checkpoint в качестве второй стороны (Peer). В поле Preshared Key (Предварительно согласованный ключ) введите действующий ключ. В поле Authentication (Аутентификация) выберите ESP/SHA/HMAC-160. В поле Encryption (Шифрование) выберите DES-56. Введите предложение IKE (в этом примере – des-sha), а также локальные и удаленные сети.

Выберите **Configuration > Policy Management > Traffic Management > Security Associations > Modify** (Конфигурация > Управление политиками > Управление трафиком > Ассоциации безопасности > Изменить). Убедитесь в том, что параметр Perfect Forward Secrecy (Защита от разглашения использованных ключей) установлен в значение **Disabled** (Отключено), а параметр IPsec Time Lifetime (Срок действия временного интервала IPSec) установлен в значение по умолчанию – **28800** секунд.

Примечание. Допустимый диапазон значений срока действия IPSec для концентратора VPN составляет от 60 до 2147483647 секунд.

Сохраните конфигурацию.

Настройка межсетевого экрана Checkpoint 4.1

Для настройки межсетевого экрана Checkpoint 4.1 выполните следующие шаги.

Поскольку у производителей различаются установленные по умолчанию сроки действия для IKE и IPSec, щелкните **Properties > Encryption** (Свойства > Шифрование), чтобы согласовать сроки действия на Checkpoint со значениями по умолчанию на концентраторе VPN.

Срок действия IKE по умолчанию для концентратора VPN – 86400 секунд (1440 минут).

Срок действия IPsec по умолчанию для концентратора VPN – 28800 секунд.

Для настройки объекта внутренней (cpinside) сети за устройством Checkpoint выберите **Manage > Network objects > New (или Edit) > Network** (Управление > Объекты сетей > Создать (Изменить) > Сеть). Настройка должна согласоваться со значением Remote Network (Удаленная сеть) на концентраторе VPN.

Для редактирования объекта шлюза, который является параметром Peer (Удаленная сторона) для концентратора VPN (устройство Checkpoint RTPCPVPN), выберите **Manage > Network objects > Edit** (Управление > Сетевые объекты > Изменить).

В поле Location (Местоположение) выберите **Internal** (Внутри). В поле Type (Тип) выберите **Gateway** (Шлюз). В разделе Modules Installed (Установленные модули) отметьте **VPN-1 & FireWall-1** и **Management Station** (Станция управления).

Для настройки объекта внешней (inside_cisco) сети за концентратором VPN выберите **Manage > Network objects > New (или Edit) > Network** (Управление > Объекты сетей > Создать (Изменить) > Сеть). Настройка должна согласоваться с настройкой «локальной» сети на концентраторе VPN.

Чтобы добавить объект для внешнего шлюза концентратора VPN (cisco_endpoint) выберите **Manage > Network objects > New > Workstation** (Управление > Сетевые объекты > Создать > Рабочая станция). Это открытый (Public) интерфейс концентратора VPN.

В разделе Location (Местоположение) выберите **External** (Снаружи). В поле Type (Тип) выберите **Gateway** (Шлюз).

Примечание. Не выбирайте флажок VPN-1/FireWall-1.

Для изменения параметров на вкладке VPN оконечного устройства шлюза Checkpoint (именуемого RTPCPVPN) выберите **Manage > Network objects > Edit** (Управление > Сетевые объекты > Изменить). На вкладке Domain (Домен) выберите Other (Другой) и затем адрес внутри сети Checkpoint (cpinside) в раскрывающемся списке. В разделе Encryption schemes defined (Определенные схемы шифрования) выберите **IKE** и нажмите кнопку **Edit** (Редактировать).

Измените свойства IKE для шифрования DES в соответствии с настройками **DES-56** и **Encryption Algorithm** (Алгоритм шифрования) на концентраторе VPN.

Измените свойства IKE для хэширования SHA1 в соответствии с алгоритмом **SHA/HMAC-160**, применяемым на концентраторе VPN.

Отмените **Aggressive Mode** (Агрессивный режим).

Отметьте флажок **Supports Subnets** (Поддерживает подсети).

В разделе Authentication Method (Метод аутентификации) отметьте флажок **Pre-Shared Secret** (Предварительно согласованный секретный ключ). Эти данные должны соотноситься с режимом аутентификации и предварительно согласованными ключами концентратора VPN.

Выберите **Edit Secrets** (Редактирование секретных ключей) для приведения предварительно согласованного ключа к фактическому значению параметра **Preshared Key** концентратора VPN.

isakmp key ключ address адрес netmask маска_подсети

Для редактирования вкладки VPN cisco_endpoint **Manage > Network objects > Edit** (Управление > Сетевые объекты > Изменить). В разделе Domain (Домен) выберите **Other** (Другой) и затем укажите внутреннее пространство сети Cisco (inside_cisco). В разделе Encryption schemes defined (Определенные схемы шифрования) выберите **IKE** и нажмите кнопку **Edit** (Редактировать).

Измените свойства IKE для шифрования DES в соответствии с настройками **DES-56, Encryption Algorithm** на концентраторе VPN.

Измените свойства IKE для хэширования SHA1 в соответствии с алгоритмом **SHA/HMAC-160**, применяемым на концентраторе VPN.

Измените следующие настройки

Отмените **Aggressive Mode** (Агрессивный режим).

Отметьте флажок **Supports Subnets** (Поддерживает подсети).

В разделе Authentication Method (Метод аутентификации) отметьте флажок **Pre-Shared Secret** (Предварительно согласованный секретный ключ). Эти данные должны соотноситься с режимом аутентификации и предварительно согласованными ключами концентратора VPN.

Выберите **Edit Secrets** (Редактирование секретных ключей) для приведения предварительно согласованного ключа к фактическому предварительно согласованному ключу концентратора VPN.

В окне Policy Editor (Редактор политик) вставьте правило, в качестве источника и назначения для которого используется inside_cisco и cpinside (двустороннее соединение). Задайте параметры: Service=Any, Action=Encrypt и Track=Long.

Затем под заголовком Action (Действие) щелкните зеленый значок **Encrypt** (Шифровать) и выберите пункт **Edit properties** (Изменить свойства), чтобы настроить политики шифрования.

Выберите **IKE**, затем выберите **Edit** (Редактировать).

В окне свойств IKE измените эти свойства в соответствии с преобразованиями IPSec для концентратора VPN.

В разделе Transform (Преобразование) выберите **Encryption + Data Integrity (ESP)** (Шифрование + контроль целостности данных [инкапсулирующая защита содержимого]). Требуется алгоритм шифрования **DES**, целостность данных SHA1, а разрешенным одноранговым шлюзом должен быть внешний шлюз Cisco (с именем cisco_endpoint). Нажмите кнопку **OK**.

После настройки контрольной точки выберите в меню Checkpoint пункты **Policy > Install** (Политика > Установить), чтобы изменения вступили в силу.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Поиск и устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Суммирование сетей

При настройке нескольких смежных внутренних сетей в домене шифрования на устройстве

Checkpoint последнее может автоматически суммировать сети с точки зрения трафика, представляющего интерес. Если концентратор VPN не настроен соответственно, то туннель с большой вероятностью функционировать не будет. Например, если внутренние сети 10.0.0.0/24 и 10.0.1.0/24 настроены на включение в туннель, они могут быть суммированы как 10.0.0.0/23.

Отладка концентратора VPN 3000

Концентратор VPN может выдавать следующие отладочные сообщения: IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE. Это настраивается в меню **Configuration > System > Events > Classes** (Конфигурация > Система > События > Классы).

Сообщения отладки можно просмотреть в разделе **Monitoring > Event log > Get Log** (Контроль > Журнал событий > Получить журнал).

Для наблюдения за туннельным трафиком между локальными сетями выберите **Monitoring > Sessions** (Контроль > Сеансы).

Для очистки туннеля выберите **Administration > Administer Sessions > LAN-to-LAN sessions > Actions - Logout** (Администрирование > Администрирование сеансов > Сеансы между локальными сетями > Действия – Выход).

Отладка межсетевого экрана Checkpoint 4.1

Примечание. Рассматривается установленная система Microsoft Windows NT. Поскольку в окне Policy Editor (Редактор политик) для отслеживания задан параметр Long (Длительно), в окне Log Viewer (Просмотр журнала) отклоненный трафик должен отображаться красным цветом. Для получения более подробных отладочных данных выполните команды:

и в другом окне:

Для сброса ассоциаций безопасности на устройстве Checkpoint выполните следующие команды:

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

На вопрос `Are you sure?` (Вы уверены?) ответьте **yes** (да).

Пример выходных данных отладки

Концентратор Cisco VPN 3000

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

Дополнительные сведения

- Протоколы IPsec Negotiation/IKE
- Cisco Systems – техническая поддержка и документация