Содержание

Введение

Этот документ объясняет начальную конфигурацию Концентратора Cisco VPN 5000 и демонстрирует, как соединиться с сетью с помощью IP и как предложить возможность VPN - подключения LAN-LAN Основного режима IPSec.

Можно установить Концентратор VPN в любой из двух конфигураций, в зависимости от того, где вы подключаете его с сетью относительно межсетевого экрана. Концентратор VPN имеет два Порта Ethernet, один из которых (Ethernet 1) только передает Трафик IPSec. Другой порт (Ethernet 0) направляет весь IP - трафик. Если вы планируете установить Концентратор VPN параллельно с межсетевым экраном, необходимо использовать оба порта так, чтобы Ethernet 0 поверхностей защищенная LAN и Ethernet 1 стояла перед Интернетом через Маршрутизатор интернет-шлюза сети. Можно также установить Концентратор VPN позади межсетевого экрана на защищенной LAN и подключить его через Ethernet 0 портов, так, чтобы Трафик IPSec, проходящий между Интернетом и концентратором, передали через межсетевой экран.

Предварительные условия

Требования

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Сведения в этом документе основываются на Концентраторе Cisco VPN 5000.

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Базовая конфигурация связности

Самый легкий способ установить базовое сетевое подключение состоит в том, чтобы подключить кабель последовательного порта с консольным портом на Концентраторе VPN и программном обеспечении терминала использования для настройки IP-адреса на Ethernet 0 портов. После настройки IP-адреса на Ethernet 0 портов можно использовать Telnet для соединения с Концентратором VPN для завершения конфигурации. Можно также генерировать файл конфигурации в соответствующем текстовом редакторе и передать его к Концентратору VPN с помощью TFTP.

Использование программного обеспечения терминала через консольный порт, вам первоначально предлагают для пароля. Используйте пароль "letmein". После отвечания паролем выполните **команду configure ip ethernet 0**, ответив на приглашения с вашими сведениями о системе. Последовательность приглашений должна быть похожей на следующий пример.

```
*[ IP Ethernet 0 ]# configure ip ethernet 0      Section 'ip ethernet 0' not found in the
config.      Do you want to add it to the config? y      Configure parameters in this section by
entering:      <Keyword> = <Value>      To find a list of valid keywords and additional help
enter "?"       *[ IP Ethernet 0 ]# ipaddress=192.168.233.1      *[ IP Ethernet 0 ]#
subnetmask=255.255.255.0      *[ IP Ethernet 0 ]# ipbroadcast=192.168.233.255      *[ IP
Ethernet 0 ]# mode=routed      *[ IP Ethernet 0 ]#
```

Теперь вы готовы настроить порт Ethernet 1.

Конфигурация порта Ethernet 1

Адресная информация TCP/IP на порту Ethernet 1 является внешним, Интернет-маршрутизируемым адресом TCP/IP, который вы назначили для Концентратора VPN. Избегайте использования адреса в той же сети TCP/IP как Ethernet 0, как это отключит TCP/IP в концентраторе.

Введите **команды configure ip ethernet 1**, ответив на приглашения с вашими сведениями о системе. Последовательность приглашений должна быть похожей на следующий пример.

```
*[ IP Ethernet 0 ]# configure ip ethernet 1      Section 'ip ethernet 1' not found in the
config.      Do you want to add it to the config? y      Configure parameters in this section by
entering:      <Keyword> = <Value>      To find a list of valid keywords and additional help
enter "?"      *[ IP Ethernet 1 ]# ipaddress=206.45.55.1      *[ IP Ethernet 1 ]#
subnetmask=255.255.255.0      *[ IP Ethernet 1 ]# ipbroadcast=206.45.55.255      *[ IP Ethernet
1 ]# mode=routed      *[ IP Ethernet 1 ]#
```

Теперь необходимо настроить Шлюз IPSEC.

Конфигурация шлюза IPSec

Шлюз IPSEC управляет, куда Концентратор VPN передает весь IPSec или туннелировал, трафик. Это независимо от маршрута по умолчанию, который вы настраиваете позже. Запустите путем ввода **команды configure general**, ответа на приглашения со сведениями о системе. Последовательность приглашений должна быть похожей на пример, показанный ниже.

```
* IntraPort2+_A56CB700# configure general      Section 'general' not found in the config.
Do you want to add it to the config? y      Configure parameters in this section by entering:
=       To find a list of valid keywords and additional help enter "?"      *[ General ]#
ipsecgateway=206.45.55.2      *[ General ]# exit      Leaving section editor.      *
IntraPort2+_A56CB700#
```

Примечание: В версиях 6.x и позже, **команда ipsecgateway** была изменена на **команду vpngateway**.

Теперь давайте настроим политику Протокола IKE.

Настройка политики IKE

Интернет-протокол управления ключами сопоставления безопасности (ISAKMP) / контроль за параметрами IKE, как Концентратор VPN и клиент определяют и аутентифицируют друг друга для установления туннельных сеансов. Это начальное согласование упоминается как Фаза 1. Параметры фазы 1 являются глобальным к устройству и не привязаны к определенному интерфейсу. Ключевые слова, распознанные в этом разделе, описаны ниже. Параметры согласования фазы 1 для туннелей между локальными сетями (LAN-to-LAN) могут быть установлены в [<Section ID> Партнера по туннелю] раздел. Ike согласование фазы 2 управляет, как Концентратор VPN и Клиент VPN обрабатывают отдельные туннельные сеансы. Параметры Ike согласование фазы 2 для Концентратора VPN и Клиента VPN установлены в [<name> Группы VPN] устройство.

Синтаксис для Набора правил IKE следующие.

```
* IntraPort2+_A56CB700# configure general      Section 'general' not found in the config.
Do you want to add it to the config? y      Configure parameters in this section by entering:
=       To find a list of valid keywords and additional help enter "?"      *[ General ]#
ipsecgateway=206.45.55.2      *[ General ]# exit      Leaving section editor.      *
IntraPort2+_A56CB700#
```

Защитное ключевое слово задает пакет защиты для согласования ISAKMP/IKE между Концентратором VPN и Клиентом VPN. Это ключевое слово может появиться многократно в этом разделе, в этом случае Концентратор VPN предлагает все заданные наборы защиты. Клиент VPN принимает одну из опций для согласования. Первая часть каждой опции, MD5 (Профиль сообщения 5), является алгоритмом аутентификации, используемым для согласования. SHA обозначает Защищенный алгоритм хэширования, который, как полагают, более безопасен, чем MD5. Вторая часть каждой опции является алгоритмом шифрования. DES (Стандарт шифрования данных) использует 56-разрядный ключ для шифрования данных. Третьей частью каждой опции является Группа Диффи-Хеллмана, используемая для обмена ключами. Поскольку большее число используется Группой 2 алгоритма (G2), это более безопасно, чем Группа 1 (G1).

Для начала конфигурации введите **команду configure IKE policy**, ответив на приглашения со сведениями о системе. Ниже приводится пример.

```
* IntraPort2+_A56CB700# configure IKE Policy      Section 'IKE Policy' was not found in the
```

```
config.      Do you want to add it to the config? y      Configure parameters in this section by
entering:      <Keyword> = <Value>      To find a list of valid keywords and additional help
enter "?"      *[ IKE Policy ] Protection = MD5_DES_G1       *[ IKE Policy ] exit      Leaving
section editor.      * IntraPort2+_A56CB700#
```

Теперь, когда вы настроили основы, пора определить параметры IP-коммуникаций и туннель.

Конфигурация основного режима узел-узел

Для настройки Концентратора VPN для поддержки прямых соединений локальных сетей необходимо определить конфигурацию туннеля, а также параметры IP-коммуникаций, которые будут использоваться в туннеле. Вы сделаете это в двух разделах, [Виртуальная частная сеть партнера по туннелю x] раздел, и [VPN X IP] раздел. Для любой данной конфигурации от узла к узлу должен совпасть *x*, определенный в этих двух разделах, так, чтобы конфигурация туннеля была должным образом привязана к конфигурации протокола.

Давайте посмотрим на каждый из этих разделов подробно.

Конфигурация раздела партнера по туннелю

В разделе партнера по туннелю необходимо определить, по крайней мере, следующие восемь параметров.

- Преобразовать
- Партнер
- KeyManage
- Общий ключ
- Режим
- LocalAccess
- Одноранговый узел
- BindTo

Преобразовать

Ключевое слово Преобразования задает типы защиты и алгоритмы, используемые для сеансов IKE - клиента. Каждая опция, привязанная к этому параметру, является элементом защиты, который задает аутентификацию и параметры шифрования. Параметр Преобразования может появиться многократно в этом разделе, в этом случае Концентратор VPN предлагает указанные элементы защиты в заказе, они проанализированы, пока каждый не принят клиентом для использования во время сеанса. В большинстве случаев только один Преобразовывает ключевое слово, необходим.

Опции для ключевого слова Преобразования следующие.

```
* IntraPort2+_A56CB700# configure IKE Policy      Section 'IKE Policy' was not found in the
config.      Do you want to add it to the config? y      Configure parameters in this section by
entering:      <Keyword> = <Value>      To find a list of valid keywords and additional help
enter "?"      *[ IKE Policy ] Protection = MD5_DES_G1       *[ IKE Policy ] exit      Leaving
section editor.      * IntraPort2+_A56CB700#
```

ESP стенды для Безопасного закрытия полезной нагрузки и AH обозначают Заголовок аутентификации. И эти заголовки используются, чтобы зашифровать и аутентифицировать

пакеты. DES (Стандарт шифрования данных) использует 56-разрядный ключ для шифрования данных. 3DES использует три других ключа и три приложения алгоритма DES для шифрования данных. MD5 является алгоритмом хэширования message-digest 5. SHA является Защищенный алгоритм хэширования, который, как полагают, несколько более безопасен, чем MD5.

ESP (MD5, DES) настройка по умолчанию и рекомендуется для большинства настроек. ESP (MD5) и ESP (SHA) используют ESP для аутентификации пакетов (без шифрования). AH (MD5) и AH (SHA) используют AH для аутентификации пакетов. AH (MD5) +ESP (DES), AH (MD5) +ESP (3DES), AH (SHA) +ESP (DES), и AH (SHA) +ESP (3DES) использование AH, чтобы аутентифицировать пакеты и ESP зашифровать пакеты.

Партнер

Ключевое слово партнера определяет IP-адрес другого оконечного устройства туннеля в туннельном партнерстве. Этот номер должен быть общественностью, маршрутизируемым IP - адресом, с которым локальный Концентратор VPN может создать IP - безопасное соединение.

KeyManage

Ключевое слово keymanage определяет, как эти два Концентратора VPN в туннельном партнерстве определяют, какое устройство инициирует туннель и какой процедура образования туннеля для придержаний. Опциями является Auto, Initiate, Respond и Manual. Можно использовать первые три опции для настройки туннелей IKE и Ключевого слова manual для настройки туннелей с фиксированным шифрованием. Этот документ не покрывает, как настроить туннели с фиксированным шифрованием. Автоматический указывает, что партнер по туннелю может и инициировать и ответить на запросы настройки туннеля. Инициируйте указывает, что партнер по туннелю только отправляет запросы настройки туннеля, он не отвечает на них. Ответьте указывает, что партнер по туннелю к отвечает на запросы настройки туннеля, но никогда не инициирует их.

Общий ключ

Ключевое слово sharedkey используется в качестве общего секрета IKE. Необходимо установить то же Значение sharedkey на обоих партнерах по туннелю.

Режим

Ключевое слово mode определяет протокол Ike согласование. Настройка по умолчанию Агрессивна, так для установки Концентратора VPN для режима совместимости, необходимо установить Ключевое слово mode в Основной.

LocalAccess

LocalAccess определяет IP-адреса, к которым можно обратиться через туннель от маски хоста до маршрута по умолчанию. Ключевое слово LocalProto определяет, к каким номерам Протокола "IP" можно обратиться через туннель, такой как ICMP (1), TCP (6), UDP (17), и так далее. Если вы хотите передать все IP-адреса, то необходимо установить LocalProto=0. LocalPort определяет, какие номера портов могут быть достигнуты через туннель. И по

умолчанию LocalProto и LocalPort к 0, или все-доступ.

Одноранговый узел

Одноранговое ключевое слово задает, какие подсети найдены через туннель. PeerProto задает, какие протоколы позволены через удаленную оконечную точку туннеля и наборы PeerPort, к каким номерам портов можно обратиться в другом конце туннеля.

BindTo

BindTo задает, какой Порт Ethernet завершает соединения от узла к узлу. Необходимо всегда установить этот параметр к Ethernet 1, кроме тех случаев, когда Концентратор VPN работает в режиме одного порта.

Настройка параметры

Для настройки этих параметров введите **команду configure Tunnel Partner VPN 1**, ответив на приглашения со сведениями о системе.

Последовательность приглашений должна быть похожей на пример ниже.

```
*IntraPort2+_A56CB700# configure Tunnel Partner VPN 1      Section ?config Tunnel Partner VPN 1?
not found in the config.      Do you want to add it to the config? y      Configure parameters
in this section by entering:       =       To find a list of valid keywords and additional help
enter "?"      *[ Tunnel Partner VPN 1 ]# transform=ESP(MD5,DES)      *[ Tunnel Partner VPN 1 ]#
sharedkey=letmein      *[ Tunnel Partner VPN 1 ]# partner=208.203.136.10      *[ Tunnel Partner
VPN 1 ]# mode=main      *[ Tunnel Partner VPN 1 ]# peer=10.0.0.0/8      *[ Tunnel Partner VPN 1
]# localaccess=192.168.233.0/24      *[ Tunnel Partner VPN 1 ]# bindto=Ethernet 1      *[ Tunnel
Partner VPN 1 ]# exit      Leaving section editor.
```

Теперь пора настроить раздел IP.

Настройка IP-раздела

Можно использовать нумерованные или ненумерованные соединения (в качестве в IP - конфигурации на подключениях к глобальной сети (WAN)) в разделе IP - конфигурации каждого туннельного партнерства. Здесь, мы использовали ненумерованный.

Минимальная конфигурация для ненумерованного подключения узел-узел требует двух операторов: numbered=false и mode=routed. Запустите путем ввода **команд configure ip vpn 1** и ответьте на системные приглашения следующим образом.

```
*[ IP Ethernet 0 ]# configure ip vpn 1      Section ?IP VPN 1? not found in the config.      Do
you want to add it to the config? y      Configure parameters in this section by entering:
<Keyword> = <Value>      To find a list of valid keywords and additional help enter "?"      *[
IP VPN 1 ]# mode=routed      *[ IP VPN 1 ]# numbered=false
```

Теперь пора установить маршрут по умолчанию.

Конфигурация маршрута по умолчанию (таблица маршрутизации TCP/IP)

Необходимо настроить маршрут по умолчанию, который Концентратор VPN может использовать для передачи всего трафика TCP/IP, предназначенного за сетями кроме сети (сетей), к которой это напрямую подключается, или для которого это имеет динамические

маршруты. Маршрут по умолчанию указывает назад ко всем сетям, найденным на внутреннем порте. Вы уже настроили Intraport для передачи Трафика IPSec к и из Интернета с помощью Параметра шлюза IPsec. Для начала конфигурации маршрута по умолчанию войдите, редактирование конфигурируют IP статическую команду, отвечая на приглашения со сведениями о системе. Последовательность приглашений должна быть похожей на пример ниже.

```
*IntraPort2+_A56CB700# edit config ip static      Section 'ip static' not found in the config.
Do you want to add it to the config? y      Configuration lines in this section have the
following format:      <Destination> <Mask> <Gateway> <Metric> [<Redist=(RIP|none)>]
Editing "[ IP Static ]"...      1: [ IP Static ]      End of buffer      Edit [ IP Static ]>
append 1      Enter lines at the prompt. To terminate input, enter      a . on a line all by
itself.      Append> 0.0.0.0 0.0.0.0 192.168.233.2 1      Append> .      Edit [ IP Static ]>
exit      Saving section...      Checking syntax...      Section checked successfully.
*IntraPort2+_A56CB700#
```

Завершающие операции

Последний шаг должен сохранить конфигурацию. Когда спросили, если вы уверены, что хотите загрузить конфигурацию и перезапустить устройство, **тип y** и нажать **Enter**. Не выключайте Концентратор VPN во время процесса загрузки. После того, как концентратор перезагрузил, пользователи могут подключить использование ПО Cisco VPN Client концентратора.

Для сохранения конфигурации введите **команду save**, следующим образом.

```
*IntraPort2+_A56CB700# save      Save configuration to flash and restart device? y
```

Если вы связаны с Концентратором VPN с помощью Telnet, выходные данные выше - все, что вы будете видеть. Если вы будете связаны через консоль, то вы будете видеть выходные данные, подобные следующему, только намного дольше. В конце этих выходных данных Концентратор VPN возвращает "Консоль приветствия..." и просит пароль. Это - то, как вы знаете, что закончены.

```
*IntraPort2+_A56CB700# save      Save configuration to flash and restart device? y
```

Дополнительные сведения

- Объявление об окончании продажи концентраторов Cisco серии VPN 5000
- Страница поддержки концентратора Cisco VPN 5000
- Страница поддержки Cisco VPN 5000 Client
- Страница поддержки IPSec
- Cisco Systems – техническая поддержка и документация