Содержание

Введение

Это руководство объясняет начальную конфигурацию Концентратора Cisco VPN 5000, в частности как настроить его для соединения с сетью с помощью IP и подключения клиента удаленного доступа предложения.

Можно установить концентратор в любой из двух конфигураций, в зависимости от того, где вы подключаете его с сетью относительно межсетевого экрана. Концентратор 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 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 этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на Концентраторе Cisco VPN 5000.

Сведения, представленные в этом документе, были получены от устройств, работающих в

специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

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 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 для завершения конфигурации. Можно также генерировать файл конфигурации в соответствующем текстовом редакторе и передать его к концентратору 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 это:

```
*[ 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.

Порт Ethernet 1

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

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

```
*[ 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 маршрут по умолчанию.

Маршрут по умолчанию

Необходимо настроить маршрут по умолчанию, который концентратор 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. Позже, вы настроите 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 это:

```
*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#
```

Теперь необходимо настроить Шлюз IPSEC.

IPSec - шлюз

Шлюз IPSEC управляет, куда концентратор передает весь IPSec или туннелировал, трафик. Это независимо от маршрута по умолчанию, который вы просто настроили. Запустите путем ввода **команды configure general**, ответа на приглашения со сведениями о системе. Последовательность приглашений должна быть похожей на это:

```
* 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#
```

Затем, настройте Набор правил IKE.

Политика IKE

Установите интернет-Протокол управления ключами Сопоставления безопасности / Обмен ключами между сетями (ISAKMP/IKE) параметры для концентратора. Этот контроль за параметрами настройки, как концентратор 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 клиенты использует индивидуальный сеанс для туннеля. Параметры Ike согласование фазы 2 для Концентратора VPN и клиента 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. Это ключевое слово может появиться многократно в этом разделе, в этом случае концентратор предлагает все заданные наборы защиты. Клиент принимает одну из опций для согласования. Первая часть каждой опции, MD-5 (message-digest 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.

```
* 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 основы настроены, введите параметры группы.

Конфигурация группы VPN

При вводе параметров группы помните, что Имя группы VPN не должно содержать пробелы, даже при том, что синтаксический анализатор командной строки позволяет вам вводить пробелы в Имя группы VPN. Имя группы VPN может содержать буквы, номера, тире и подчеркивания.

Существует четыре основных параметра, которые требуются в каждой Группе VPN для операции IP:

- Maxconnections
- StartIPaddress или LocalIPNet
- Преобразовать
- IPNet

Параметр Maxconnections является максимальным числом параллельных сеансов клиента, позволенных в этой определенной Конфигурации группы VPN. Помните этот номер, поскольку он работает в сочетании с StartIPAddress или параметром LocalIPNet.

Концентратор VPN назначает IP-адреса на удаленных клиентов двумя другими схемами, StartIPAddress и LocalIPNet. StartIPAddress назначает IP-адреса от подсети, связанной с Ethernet 0 и Proxy-arp для подключенных клиентов. LocalIPNet назначает IP-адреса на удаленных клиентов от подсети, уникальной для клиентов VPN, и требует, чтобы остаток сети был сделан знающий о существовании подсети VPN через статическую или динамическую маршрутизацию. StartIPAddress предлагает более легкую конфигурацию, но может ограничить размер адресного пространства. LocalIPNet предлагает большую гибкость адресации для удаленных пользователей, но требует, чтобы немного больше работало для настройки необходимой маршрутизации.

Для StartIPAddress используйте первый IP-адрес, назначенный на туннельный сеанс

входящего клиента. В настройке базовой конфигурации это должно быть IP-адресом во внутренней сети TCP/IP (та же сеть как Ethernet 0 портов). В нашем примере ниже, первому сеансу клиента назначают эти 192.168.233.50 адреса, следующий параллельный сеанс клиента назначен 192.168.233.51 и так далее. Мы назначили значение Maxconnections 30, что означает, что у нас должен быть блок 30 неиспользованных IP-адресов (включая серверы DHCP, если у вас есть кто-либо) начиная с 192.168.233.50 и заканчивающийся 192.168.233.79. Избегите накладываться на IP-адреса, используемые в других Конфигурациях группы VPN.

LocalIPNet назначает IP-адреса на удаленных клиентов от подсети, которая должна быть неиспользована в другом месте на LAN. Например, при определении параметра "LocalIPNet=182.168.1.0/24" в конфигурации группы VPN концентратор назначает IP-адреса на клиентов начиная с 192.168.1.1. Поэтому необходимо назначить "Maxconnections=254", поскольку концентратор не учтет границы подсети при присвоении IP-адресов с помощью LocalIPNet.

Ключевое слово Преобразования задает типы защиты и алгоритмы, которые концентратор использует для сеансов IKE - клиента. Опции 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#
```

Каждая опция является элементом защиты, который задает аутентификацию и параметры шифрования. Это ключевое слово может появиться многократно в этом разделе, в этом случае концентратор 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.

ESP (SHA, DES), ESP (SHA, 3DES), ESP (MD5, DES), и ESP (MD5,3DES) обозначают заголовок Безопасного закрытия полезной нагрузки (ESP), 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, и SHA является Защищенный алгоритм хэширования, который, как полагают, несколько более безопасен, чем MD5.

ESP (MD5, DES) настройка по умолчанию и рекомендуется для большинства установок. ESP (MD5) и ESP (SHA) используют заголовок ESP для аутентификации пакетов без шифрования. AH (MD5) и AH (SHA) используют Заголовок аутентификации (AH) для аутентификации пакетов. AH (MD5) +ESP (DES), AH (MD5) +ESP (3DES), AH (SHA) +ESP (DES), и AH (SHA) +ESP (3DES) использование Заголовок аутентификации для аутентификации пакетов и заголовка ESP для шифрования пакетов.

Примечание: Клиентское программное обеспечение Mac OS не поддерживает опцию AH. Необходимо задать по крайней мере один параметр ESP при использовании Клиентского программного обеспечения Mac OS.

Поле IPNet важно, так как оно управляет, куда могут пойти клиенты концентратора. Значения, которые вы вводите в это поле, определяют, какой трафик TCP/IP туннелирован, или более обычно, где клиент, который принадлежит этой Группе VPN, может пойти на вашу сеть.

Cisco рекомендует настроить внутреннюю сеть (в данном примере 192.168.233.0/24), таким образом, весь трафик от клиента, переходящего к внутренней сети, передается через туннель, и поэтому аутентифицируется и шифруется (если вы включаете шифрование). В этом сценарии не туннелирован никакой другой трафик; вместо этого, это обычно маршрутизируется. У вас могут быть несколька точек входа, включая сингл или адреса узла. Формат является адресом (в нашем примере, сетевой адрес 192.168.233.0) и затем маска, привязанная к тому адресу в битах (/24, который является маской Класса C).

Запустите эту часть конфигурации путем ввода **команды configure VPN group basic-user**, и затем ответьте на приглашения со сведениями о системе. Вот пример последовательности полной конфигурации:

```
*IntraPort2+_A56CB700# configure VPN group basic-user      Section 'VPN Group basic-user' 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 "?"      *[ VPN Group "basic-user" ]# startipaddress=192.168.233.50
or      *[ VPN Group "basic-user" ]# localipnet=192.168.234.0/24      *[ VPN Group "basic-user"
]# maxconnections=30      *[ VPN Group "basic-user" ]# Transform=ESP(SHA,DES)      *[ VPN Group
"basic-user" ]# ipnet=192.168.233.0/24      *[ VPN Group "basic-user" ]# exit      Leaving
section editor.      *IntraPort2_A51EB700#
```

Следующий шаг должен определить базу данных пользователя.

Конфигурация пользователя VPN

В этом разделе конфигурации вы определяете базу данных пользователей VPN. Каждая линия определяет пользователя VPN наряду с Конфигурацией группы VPN и паролем того пользователя. Многострочные записи должны иметь разрывы строки, заканчивающиеся наклонной чертой влево. Однако разрывы строки, включенные в двойные кавычки, сохранены.

Когда клиент VPN начинает туннельный сеанс, имя пользователя клиента передано к устройству. Если устройство находит пользователя в этом разделе, оно использует информацию в записи для устанавливания туннеля. (Можно также использовать сервер RADIUS для аутентификации пользователей VPN). Если устройство не находит имя пользователя, и вы не настроили сервер RADIUS для выполнения аутентификации, туннельный сеанс не открыт, и ошибка возвращена клиенту.

Запустите конфигурацию путем ввода **команды edit config VPN users**. Давайте посмотрим на пример, который добавляет пользователя под названием "User1" к Группе VPN "рядовой пользователь".

```
*IntraPort2+_A56CB700# edit config VPN users      Section 'VPN users' not found in the config.
Do you want to add it to the config? y      <Name> <Config> <SharedKey>      Editing "[ VPN
Users ]"...      1: [ VPN Users ]      End of buffer      Edit [ VPN Users ]> append 1
Enter lines at the prompt. To terminate input, enter      a . on a line all by itself.
Append> User1 Config="basic-user" SharedKey="Burnt"      Append> .      Edit [ VPN Users ]> exit
Saving section...      Checking syntax...      Section checked successfully.
*IntraPort2+_A56CB700#
```

Общий ключ этого пользователя "Записан". Все эти значения конфигурации учитывают регистр; если вы настраиваете "User1", пользователь должен ввести "User1" в клиентское программное обеспечение. Ввод "user1" приводит к недопустимому сообщению об ошибках или сообщению об ошибках неавторизованный пользователя. Можно продолжить вводить пользователей вместо того, чтобы выйти из редактора, но помнить, необходимо ввести период для выхода из редактора. Сбой, чтобы сделать так может вызвать неправильные

элементы в конфигурации.

Завершающие операции

Ваш последний шаг сохраняет конфигурацию. Когда спросили, если вы уверены, что хотите загрузить конфигурацию и перезапустить устройство, тип y и нажать Клавишу Enter. Не выключайте концентратор 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 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 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