Настраивание концентратора Cisco VPN 3000 для маршрутизатора Cisco

Содержание

Введение

Этот пример конфигурации показывает, как подключить частную сеть позади маршрутизатора, который выполняет программное обеспечение Cisco IOS к частной сети позади Cisco VPN 3000 Concentrator. Устройства в сетях знают друг друга по своим частным адресам.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Маршрутизатор Cisco 2611 с программным обеспечением Cisco IOS версии 12.3. (1) а**Примечание:** Удостоверьтесь, что Маршрутизаторы серии Cisco 2600 установлены с крипто-Образом IOS IPSec VPN, который поддерживает функцию VPN.
- Cisco VPN 3000 Concentrator с 4.0.1 B

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 Условные обозначения технических терминов Cisco.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети.

Конфигурации

В данном документе используется следующая конфигурация.

Настройка маршрутизатора

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1 encr 3des
hash md5 authentication pre-share group 2 crypto isakmp
key cisco123 address 200.1.1.2 ! !--- IPsec policies.
crypto ipsec transform-set to_vpn esp-3des esp-md5-hmac
! crypto map to_vpn 10 ipsec-isakmp set peer 200.1.1.2
set transform-set to_vpn !--- Traffic to encrypt. match
address 101 ! interface Ethernet0/0 ip address
203.20.20.2 255.255.255.0 ip nat outside half-duplex
crypto map to_vpn ! interface Ethernet0/1 ip address
172.16.1.1 255.255.255.0 ip nat inside half-duplex ! ip
nat pool mypool 203.20.20.3 203.20.20.3 netmask
```

```
255.255.255.0 ip nat inside source route-map nonat pool
mypool overload ip http server no ip http secure-server
ip classless ip route 0.0.0.0 0.0.0.0 203.20.20.1 ip
route 172.16.20.0 255.255.255.0 172.16.1.2 ip route
172.16.30.0 255.255.255.0 172.16.1.2 ! !--- Traffic to
encrypt. access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.10.0 0.0.0.255 access-list 101 permit ip
172.16.1.0 0.0.0.255 192.168.40.0 0.0.0.255 access-list
101 permit ip 172.16.1.0 0.0.0.255 192.168.50.0
0.0.0.255 access-list 101 permit ip 172.16.20.0
0.0.0.255 192.168.10.0 0.0.0.255 access-list 101 permit
ip 172.16.20.0 0.0.0.255 192.168.40.0 0.0.0.255 access-
list 101 permit ip 172.16.20.0 0.0.0.255 192.168.50.0
0.0.0.255 access-list 101 permit ip 172.16.30.0
0.0.0.255 192.168.10.0 0.0.0.255 access-list 101 permit
ip 172.16.30.0 0.0.0.255 192.168.40.0 0.0.0.255 access-
list 101 permit ip 172.16.30.0 0.0.0.255 192.168.50.0
0.0.0.255 !--- Traffic to except from the NAT process.
access-list 110 deny ip 172.16.1.0 0.0.0.255
192.168.10.0 0.0.0.255 access-list 110 deny ip
172.16.1.0 0.0.0.255 192.168.40.0 0.0.0.255 access-list
110 deny ip 172.16.1.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 deny ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255 access-list 110 deny ip
172.16.20.0 0.0.0.255 192.168.40.0 0.0.0.255 access-list
110 deny ip 172.16.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 deny ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255 access-list 110 deny ip
172.16.30.0 0.0.0.255 192.168.40.0 0.0.0.255 access-list
110 deny ip 172.16.30.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any !
route-map nonat permit 10 match ip address 110 ! line
con 0 line aux 0 line vty 0 4 ! end
```

Конфигурация концентраторов VPN

В этих лабораторных параметрах к Концентратору VPN сначала обращаются через консольный порт, и минимальная настройка добавлена так, чтобы дальнейшая конфигурация могла быть реализована через графический пользовательский интерфейс (GUI).

Выберите **Administration> System Reboot> Schedule reboot> Reboot with Factory/Default Configuration**, чтобы гарантировать, что нет никакой существующей конфигурации в Концентраторе VPN.

Концентратор VPN появляется в Быстрой настройке, и эти элементы настроены после перезагрузки:

- Время/Дата
- **Пункт Interfaces/Masks в меню Configuration > Interfaces (public=200.1.1.2/24, private=192.168.10.1/24)**
- **Шлюз по умолчанию в конфигурации > System > IP routing > Default_Gateway (200.1.1.1)**

На этом этапе Концентратор VPN доступен через HTML от внутренней сети.

Примечание: Поскольку VPN Concentrator управляется снаружи, вам также необходимо выбрать:

- **Configuration> Interfaces> с 2 общественностью> Выбирает IP Filter> 1. Частный (По умолчанию)**.
- **Administration> Access Rights> Access Control List> Add Manager Workstation** для добавления IP-адреса *внешнего менеджера*.

Это не необходимо, пока вы не управляете Концентратором VPN *снаружи*.

1. Выберите **Configuration> Interfaces** для перепроверки интерфейсов после внедрения GUI.
2. Выберите **Configuration> System> IP Routing> Default Gateways** для настройки **По умолчанию** (Интернет) **шлюз** и **Туннельный По умолчанию** (в) **шлюзе** для IPsec для достижения других подсетей в частной сети.
3. Выберите **Configuration> Policy Management> Network Lists** для создания списков сетей, которые определяют трафик, который будет зашифрован.Это - локальные сети:Это удаленные сети:
4. По завершении получаются следующие два списка сетей:**Примечание:** Если Туннель IPSec не подходит, проверьте, чтобы видеть, совпадает ли представляющий интерес трафик с обеих сторон. Представляющий интерес трафик определен списком доступа на коробках PIX и маршрутизаторе. Они определены списками сетей в Концентраторах VPN.
5. Выберите **Configuration> System> Tunneling Protocols> IPSec LAN-to-LAN** и определите туннель между локальными сетями (LAN-to-LAN).
6. **После того, как вы нажмете на Apply, появляется окно с другой конфигурацией, которая автоматически создается в результате настройки LAN-to-LAN туннеля.**Ранее созданные Параметры IPSec LAN-LAN могут просматриваться или модифицироваться в **Configuration> System> Tunneling Protocols> IPsec LAN-to-LAN**.
7. Выберите **Configuration> System> Tunneling Protocols> IPSec> IKE Proposals** для подтверждения Предложения по активному предложению IKE.
8. Выберите**> Security Configuration> Policy Management> Traffic Management Ассоциации** для просмотра списка Сопоставлений безопасности.
9. Нажмите Имя сопоставления безопасности (SA), и затем нажмите **Modify** для проверки Сопоставлений безопасности.

Проверка

Этот раздел перечисляет команды show, используемые в этой конфигурации.

На маршрутизаторе

В данном разделе содержатся сведения о проверке работы конфигурации.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- **show crypto ipsec sa – отображает текущие настройки связей безопасности.**
- **show crypto isakmp sa** все текущие Сопоставления безопасности Обмена ключами между сетями в узле.
- **show crypto engine connection active** — Показывает текущие активные соединения

шифрованного сеанса для всех ядер шифрования.

Можно использовать Средство поиска команд IOS Command Lookup Tool (только зарегистрированные клиенты) для наблюдения дополнительных сведений об определенных командах.

На концентраторе VPN

Выберите **Configuration> System> Events> Classes> Modify** для включения регистрации. Эти опции доступны:

- IKE
- IKEDBG
- IKEDECODE
- IPSec
- IPSECDBG
- IPSECDECODE

Код серьезности ошибки для регистрации = 1-13

Код серьезности ошибки для консоли = 1-3

Выберите **Monitoring> Event Log** для получения журнала событий.

Устранение неполадок

На маршрутизаторе

См. раздел Важные сведения о командах отладки перед попыткой любых команд отладки.

- **debug crypto engine– показывает зашифрованный трафик.**
- **debug crypto ipsec – отображает согласования IPSec на Этапе 2.**
- **debug crypto isakmp – отображает согласования ISAKMP на 1-м этапе.**

Проблема - неспособный инициировать туннель

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

Решение

Завершите это действие, чтобы настроить необходимый номер одновременных входов в систему или установить одновременные входы в систему в 5 для этого SA:

Перейдите к **Configuration> User Management> Groups,> Modify 10.19.187.229> Общий> Входы в систему Simultaneouts** и изменяют количество входов в систему к 5.

БЕЗОПАСНАЯ ПЕРЕСЫЛКА (PFS)

При согласовании IPsec безопасная пересылка (PFS) позволяет гарантировать отсутствие

связи нового ключа шифрования со всеми предыдущими ключами. Или включите или отключите безопасную пересылку (PFS) на обоих равноправные пользователи туннеля. В противном случае LAN-LAN (L2L) Туннель IPSec не установлен в маршрутизаторах.

Чтобы указать, что IPsec должен попросить безопасную пересылку (PFS), когда новые Сопоставления безопасности запрашивают на этот элемент криптокарты, или что IPsec требует безопасной пересылки (PFS), когда это получает запросы о новых Сопоставлениях безопасности, используйте **команду set pfs** в режиме конфигурации криптокарты. Чтобы указать, что IPsec не должен запрашивать безопасную пересылку (PFS), используйте **эту команду с параметром no**.

```
set pfs [group1 | group2] no set pfs
```

Для **команды set pfs**:

- *group1* — Указывает, что IPsec должен использовать 768-разрядный Диффи-Хеллман главная группа модуля, когда выполнен новый Обмен Диффи-Хеллмана.
- *group2* — Указывает, что IPsec должен использовать 1024-разрядный Диффи-Хеллман главная группа модуля, когда выполнен новый Обмен Диффи-Хеллмана.

По умолчанию PFS не запрашивается. Если никакая группа не задана с этой командой, *group1* используется в качестве по умолчанию.

Пример:

```
Router(config)#crypto map map 10 ipsec-isakmp Router(config-crypto-map)#set pfs group2
```

См. Справочник по командам Безопасности Cisco IOS для получения дополнительной информации о **команде set pfs**.

Дополнительные сведения

- Устранение наиболее распространенных проблем удаленных VPN-подключений и VPN-туннелей LAN — LAN на базе протокола IPSec
- Cisco VPN 3000 Series Concentrators
- Cisco VPN 3002 Hardware Client
- Согласование IPsec/Протоколы IKE
- Cisco Systems – техническая поддержка и документация