IOS VPN (Маршрутизатор): Добавьте или удалите сеть на примере конфигурации VPN-туннеля L2L

Содержание

Введение

Этот документ предоставляет пример конфигурации для того, как добавить или удалить сеть на существующем LAN-LAN (L2L) VPN-туннель.

Предварительные условия

Требования

Гарантируйте корректную настройку текущего VPN-туннеля IPSec L2L перед попыткой этой конфигурации.

Используемые компоненты

Сведения в этом документе основываются на двух маршрутизаторах Cisco IOS®, которые работают под управлением ПО версии 12.4 (15) T1.

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

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

В настоящее время существует VPN-туннель L2L между главным офисом (HQ) офис и филиалом компании (BO). Офис HQ просто добавил новую сеть, которая будет использоваться группой продаж. Эта команда требует доступа к ресурсам, которые находятся в офисе BO. Задача под рукой состоит в том, чтобы добавить новую сеть к уже существующему VPN-туннелю L2L.

Настройка

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

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:

Конфигурации

Этот документ использует конфигурации, описанные в этом разделе. Эти конфигурации включают VPN L2L, которая выполняется между 172.16.10.0 сетями офиса HQ и 10.10.10.0 сетями офиса BO. Выходные данные отобразились полужирным, текст показывает требуемую конфигурацию для интеграции новой сети 192.168.10.0 из офиса HQ в тот же VPN-туннель с 10.10.10.0 как сеть назначения.

Маршрутизатор HQ

```
HQ-Router#show running-config Building configuration...
Current configuration : 1439 bytes ! version 12.4
service timestamps debug uptime service timestamps log
uptime no service password-encryption ! hostname HQ-
Router ! !--- Output suppressed. ! crypto isakmp policy
1 hash md5 authentication pre-share crypto isakmp key
cisco123 address 209.165.200.225 ! ! crypto ipsec
transform-set rtpset esp-des esp-md5-hmac ! crypto map
rtp 1 ipsec-isakmp set peer 209.165.200.225 set
transform-set rtpset match address 115 ! interface
Ethernet0 ip address 172.16.10.1 255.255.255.0 ip nat
inside ! interface Ethernet1 ip address 209.165.201.2
255.255.255.224 ip nat outside crypto map rtp !
interface Ethernet2 ip address 192.168.10.1
255.255.255.0 ip nat inside ! interface Serial0 no ip
address shutdown no fair-queue ! interface Serial1 no ip
address shutdown ! ip nat inside source route-map nonat
interface Ethernet1 overload ip classless ip route
```

```
0.0.0.0 0.0.0.0 209.165.201.1 ! !--- Output suppressed.
access-list 110 deny ip 172.16.10.0 0.0.0.255 10.10.10.0
0.0.0.255 access-list 110 permit ip 172.16.10.0
0.0.0.255 any ! !--- Add this ACL entry to include
192.168.10.0 !--- network with the nat-exemption rule.
access-list 110 deny ip 192.168.10.0 0.0.0.255
10.10.10.0 0.0.0.255 access-list 110 permit ip
192.168.10.0 0.0.0.255 any access-list 115 permit ip
172.16.10.0 0.0.0.255 10.10.10.0 0.0.0.255 ! !--- Add
this ACL entry to include 192.168.10.0 !--- network into
the crypto map. access-list 115 permit ip 192.168.10.0
0.0.0.255 10.10.10.0 0.0.0.255 route-map nonat permit 10
match ip address 110 ! !--- Output suppressed. end
```

МАРШРУТИЗАТОР BO

```
BO-Router#show running-config Building configuration...
Current configuration : 2836 bytes ! version 12.4
service timestamps debug datetime msec service
timestamps log datetime msec no service password-
encryption ! hostname BO-Router ! !--- Output
suppressed. ! crypto isakmp policy 1 hash md5
authentication pre-share crypto isakmp key cisco123
address 209.165.201.2 ! ! crypto ipsec transform-set
rtpset esp-des esp-md5-hmac ! crypto map rtp 1 ipsec-
isakmp set peer 209.165.201.2 set transform-set rtpset
match address 115 ! !--- Output suppressed. interface
FastEthernet0/0 ip address 209.165.200.225
255.255.255.224 ip nat outside ip virtual-reassembly
duplex auto speed auto crypto map rtp ! interface
FastEthernet0/1 ip address 10.10.10.1 255.255.255.0 ip
nat inside ip virtual-reassembly duplex auto speed auto
! ip route 0.0.0.0 0.0.0.0 FastEthernet0/1 ! !--- Output
suppressed. ! ip http server no ip http secure-server ip
nat inside source route-map nonat interface
FastEthernet0/0 overload ! !--- Add this ACL entry to
include 192.168.10.0 !--- network with the nat-exemption
rule. access-list 110 deny ip 10.10.10.0 0.0.0.255
192.168.10.0 0.0.0.255 access-list 110 deny ip
10.10.10.0 0.0.0.255 172.16.10.0 0.0.0.255 access-list
110 permit ip 10.10.10.0 0.0.0.255 any access-list 115
permit ip 10.10.10.0 0.0.0.255 172.16.10.0 0.0.0.255 !
!--- Add this ACL entry to include 192.168.10.0 !---
network into the crypto map. access-list 115 permit ip
10.10.10.0 0.0.0.255 192.168.10.0 0.0.0.255 ! route-map
nonat permit 10 match ip address 110 ! !--- Output
suppressed. ! end
```

Удалите сеть из туннеля IPSec

Выполните шаги, описанные в этом разделе для удаления сети из конфигурации Туннеля IPSec. Обратите внимание на то, что сеть 192.168.10.0/24 была удалена из конфигурации маршрутизатора HQ.

1. Используйте эту команду для разъединения IP - безопасного соединения:`HQ-Router#`**`clear crypto sa`**
2. Используйте эту команду для очистки Ассоциаций ISAKMPSecurity (SA):`HQ-Router#`**`clear crypto isakmp`**
3. Используйте эту команду для удаления ACL представляющего интерес трафика для Туннеля IPSec:`HQ-Router(config)#`**`no access-list 115 permit ip 192.168.10.0 0.0.0.255 10.10.10.0 0.0.0.255`**

4. Используйте эту команду для удаления туземно-освобожденного оператора ACL для 192.168.10.0 сетей:`HQ-Router(config)#`**`no access-list 110 deny ip 192.168.10.0 0.0.0.255 10.10.10.0 0.0.0.255`**
5. Используйте эту команду для очистки преобразования NAT:`HQ-Router#`**`clear ip nat translation *`**
6. Используйте эти команды, чтобы удалить и повторно применить криптокарту на интерфейсе, чтобы гарантировать, что текущее крипто - настройка вступает в силу:`HQ-Router(config)#`**`int ethernet 1`** `HQ-Router(config-if)#`**`no crypto map rtp`** `*May 25 10:35:12.153: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF HQ-Router(config-if)#`**`crypto map rtp`** `*May 25 10:36:09.305: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON` **Примечание:** Удаление криптокарты от интерфейса рвет все существующие VPN-подключения, привязанные к той криптокарте. Прежде, чем сделать это, удостоверьтесь, что вы заняли требуемое время простоя и придерживались политики управления изменениями вашей организации соответственно.
7. Используйте **команду write memory** для сохранения активной конфигурации к флэш-памяти.
8. Выполните эти шаги на другом конце VPN-туннеля (Маршрутизатор BO) для удаления конфигураций.
9. Инициируйте Туннель IPSec и проверьте соединение.

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Используйте эту последовательность эхо-запроса, чтобы гарантировать, что новая сеть может передать данные через VPN-туннель:

`HQ-Router#`**`clear crypto sa`** `HQ-Router# HQ-Router#`**`ping 10.10.10.1 source 172.16.10.1`** `Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds: Packet sent with a source address of 172.16.10.1 .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 20/20/20 ms HQ-Router#`**`ping 10.10.10.1 source 192.168.10.1`** `Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds: Packet sent with a source address of 192.168.10.1 .!!!! Success rate is 80 percent (4/5), round-trip min/avg/max = 20/20/20 ms HQ-Router#`**`ping 10.10.10.1 source 192.168.10.1`** `Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds: Packet sent with a source address of 192.168.10.1 !!!!! Success rate is` **`100 percent`** `(5/5), round-trip min/avg/max = 20/20/20 ms`

show crypto ipsec sa

```
HQ-Router#show crypto ipsec sa interface: Ethernet1
Crypto map tag: rtp, local addr. 209.165.201.2 local
ident (addr/mask/prot/port):
(192.168.10.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
current_peer: 209.165.200.225 PERMIT,
flags={origin_is_acl,} #pkts encaps: 9, #pkts encrypt:
9, #pkts digest 9 #pkts decaps: 9, #pkts decrypt: 9,
#pkts verify 9 #pkts compressed: 0, #pkts decompressed:
0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts
decompress failed: 0 #send errors 1, #recv errors 0
local crypto endpt.: 209.165.201.2, remote crypto
endpt.: 209.165.200.225 path mtu 1500, ip mtu 1500, ip
mtu interface Ethernet1 current outbound spi: FB52B5AB
inbound esp sas: spi: 0x612332E(101856046) transform:
esp-des esp-md5-hmac , in use settings ={Tunnel, } slot:
0, conn id: 2002, flow_id: 3, crypto map: rtp sa timing:
```

```
remaining key lifetime (k/sec): (4607998/3209) IV size:
8 bytes replay detection support: Y inbound ah sas:
inbound pcp sas: outbound esp sas: spi:
0xFB52B5AB(4216501675) transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, } slot: 0, conn id: 2003,
flow_id: 4, crypto map: rtp sa timing: remaining key
lifetime (k/sec): (4607998/3200) IV size: 8 bytes replay
detection support: Y outbound ah sas: outbound pcp sas:
local ident (addr/mask/prot/port):
(172.16.10.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
current_peer: 209.165.200.225 PERMIT,
flags={origin_is_acl,} #pkts encaps: 4, #pkts encrypt:
4, #pkts digest 4 #pkts decaps: 4, #pkts decrypt: 4,
#pkts verify 4 #pkts compressed: 0, #pkts decompressed:
0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts
decompress failed: 0 #send errors 1, #recv errors 0
local crypto endpt.: 209.165.201.2, remote crypto
endpt.: 209.165.200.225 path mtu 1500, ip mtu 1500, ip
mtu interface Ethernet1 current outbound spi: C9E9F490
inbound esp sas: spi: 0x1291F1D3(311554515) transform:
esp-des esp-md5-hmac , in use settings ={Tunnel, } slot:
0, conn id: 2000, flow_id: 1, crypto map: rtp sa timing:
remaining key lifetime (k/sec): (4607999/3182) IV size:
8 bytes replay detection support: Y inbound ah sas:
inbound pcp sas: outbound esp sas: spi:
0xC9E9F490(3387552912) transform: esp-des esp-md5-hmac ,
in use settings ={Tunnel, } slot: 0, conn id: 2001,
flow_id: 2, crypto map: rtp sa timing: remaining key
lifetime (k/sec): (4607999/3182) IV size: 8 bytes replay
detection support: Y outbound ah sas: outbound pcp sas:
```

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

Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

- **debug crypto ipsec – отображает согласования IPSec на Этапе 2.**
- **debug crypto isakmp – отображает согласования ISAKMP на 1-м этапе.**
- **debug crypto engine– служит для просмотра шифруемых сеансов.**

Дополнительные сведения

- Введение в шифрование IPSec
- Страница технической поддержки протоколов согласования IPSec и IKE
- Настройка динамических участников LAN-LAN и клиентов VPN маршрутизатора IPsec
- Cisco Systems – техническая поддержка и документация