Динамичный к динамическому примеру конфигурации туннеля IPSec

Содержание

Введение

Этот документ описывает , как создать Туннель IPSec между локальными сетями между маршрутизаторами Cisco, когда оба конца имеют динамические IP - адреса, но настроена Динамическая система имен доменов (DDNS).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Сквозной VPN-соединение с Туннелем IPSec и Универсальной инкапсуляцией маршрутизации (GRE)
- Интерфейс виртуальных туннелей IPsec (VTI)
- [Поддержка динамических DN программного обеспечения Cisco IOS](#)

Совет: См. раздел VPN Настройки Cisco и Руководство по конфигурации программного обеспечения серии 1900 серии 2900, серии 3900 и статья Configuring a Virtual Tunnel Interface with IP Security для получения дополнительной информации.

Используемые компоненты

Сведения в этом документе основываются на Маршрутизаторе ISR Cisco 2911, который выполняет Версию 15.2 (4) M6a.

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.

Общие сведения

Когда туннель между локальными сетями (LAN-to-LAN) должен быть установлен, IP-адрес обоих Узлов IPsec должен быть известен. Если один из IP-адресов не известен, потому что это динамично, такой как один полученный через DHCP, то альтернатива должна использовать динамическую криптокарту. Это работает, но туннель может только быть переведен в рабочее состояние узлом, который имеет динамический IP - адрес, так как другой узел не знает, где найти его узел.

Для получения дополнительной информации о динамическом к помехам, обратитесь к Динамический-в-статичному каналу IPSec маршрутизатор-маршрутизатор с поддержкой NAT Настройки.

Настройка

Разрешение в реальном времени для узла туннеля IPSec

Cisco IOS® представил новую характеристику в Версии 12.3 (4) T, которая позволяет Полному доменному имени (FQDN) Узла IPsec быть заданным. Когда существует трафик, который совпадает с крипто- списком доступа, IOS Cicso тогда решает FQDN и получает IP-адрес узла. Это тогда пытается перевести туннель в рабочее состояние.

Примечание: Существует ограничение на эту функцию: разрешение имен DNS для удаленных узлов IPsec будет работать, только если они используются в качестве инициатора. Первый пакет, который должен быть зашифрован, инициирует Поиск DNS; после того, как Поиск DNS завершен, последующие пакеты инициируют Протокол IKE. Разрешение в реальном времени не будет работать на респондента.

Чтобы обратиться к ограничению и быть в состоянии инициировать туннель от каждого узла, у вас будет запись динамической криптокарты на обоих маршрутизаторах, таким образом, можно будет сопоставить входящие IKE - подключения с динамическим крипто-. Это необходимо, так как статическая запись с функцией разрешения В реальном времени не работает, когда это действует как респондент.

Маршрутизатор A

```
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
!
ip access-list extended crypto-ACL
permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set myset esp-aes esp-sha-hmac
!
crypto dynamic-map dyn 10
set transform-set myset
!
crypto map mymap 10 ipsec-isakmp
match address 140
set peer example-b.cisco.com dynamic
set transform-set myset
crypto map mymap 65535 ipsec-isakmp dynamic dyn
!
interface fastethernet0/0
ip address dhcp
crypto map secure_b
```

Маршрутизатор B

```
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
!
ip access-list extended crypto-ACL
permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set myset esp-aes esp-sha-hmac
!
crypto dynamic-map dyn 10
set transform-set myset
!
crypto map mymap 10 ipsec-isakmp
match address 140
set peer example-a.cisco.com dynamic
set transform-set myset
crypto map mymap 65535 ipsec-isakmp dynamic dyn
```

```
!
interface fastethernet0/0
ip address dhcp
crypto map secure_b
```

Примечание: Так как вы не знаете, какой IP-адрес FQDN будет использовать, необходимо использовать Предварительный общий ключ подстановочного знака: 0.0.0.0 0.0.0.0

Обновление назначения туннеля со встроенным диспетчером событий (EEM)

Вы можете также VTI для выполнения этого. Базовую конфигурацию показывают здесь:

Маршрутизатор A

```
crypto isakmp policy 10
encryption aes
authentication pre-share
group 2

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 no-xauth

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile
set transform-set ESP-AES-SHA
!
interface Tunnel1
ip address 172.16.12.1 255.255.255.0
tunnel source fastethernet0/0
tunnel destination example-b.cisco.com
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
```

Маршрутизатор B

```
crypto isakmp policy 10
encryption aes
authentication pre-share
group 2

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0 no-xauth

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto ipsec profile ipsec-profile
set transform-set ESP-AES-SHA
!
interface Tunnel1
ip address 172.16.12.2 255.255.255.0
tunnel source fastethernet0/0
tunnel destination example-a.cisco.com
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
```

Как только предыдущая конфигурация существует с FQDN как назначение туннеля, **команда show run** показывает IP-адрес вместо названия. Это вызвано тем, что разрешение

происходит только однажды:

```
RouterA(config)#do show run int tunn 1
Building configuration...

Current configuration : 130 bytes
!
interface Tunnel1
ip address 172.16.12.1 255.255.255.250
tunnel source fastethernet0/0
tunnel destination 209.165.201.1
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
endRouterB(config)#do show run int tunn 1
Building configuration...

Current configuration : 130 bytes
!
interface Tunnel1
ip address 172.16.12.2 255.255.255.250
tunnel source fastethernet0/0
tunnel destination 209.165.200.225
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
end
```

Обходной путь для этого должен настроить апплет для решения назначения туннеля каждую минуту:

Маршрутизатор A

```
RouterB(config)#do show run int tunn 1
Building configuration...

Current configuration : 130 bytes
!
interface Tunnel1
ip address 172.16.12.2 255.255.255.250
tunnel source fastethernet0/0
tunnel destination 209.165.200.225
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
end
```

Маршрутизатор B

```
RouterB(config)#do show run int tunn 1
Building configuration...

Current configuration : 130 bytes
!
interface Tunnel1
ip address 172.16.12.2 255.255.255.250
tunnel source fastethernet0/0
tunnel destination 209.165.200.225
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
end
```

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

```
RouterA(config)#do show ip int brie
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 209.165.200.225 YES NVRAM up up
FastEthernet0/1 192.168.10.1 YES NVRAM up up
Tunnel1 172.16.12.1 YES manual up up


RouterB(config)#do show ip int brie
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 209.165.201.1 YES TFTP up up
FastEthernet0/1 192.168.20.1 YES manual up up
Tunnel1 172.16.12.2 YES manual up upRouterA(config)#do show cry isa sa
dst src state conn-id slot status
209.165.200.225 209.165.201.1 QM_IDLE 2 0 ACTIVE

RouterB(config)#do show cry isa sa
dst src state conn-id slot status
209.165.200.225 209.165.201.1 QM_IDLE 1002 0 ACTIVERouterA(config)#do show cry ipsec sa

interface: Tunnel1
Crypto map tag: Tunnel1-head-0, local addr 209.165.200.225

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 209.165.201.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 209.165.200.225, remote crypto endpt.: 209.165.201.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x8F1592D2(2400555730)

inbound esp sas:
spi: 0xF7B373C0(4155732928)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2002, flow_id: AIM-VPN/BPII-PLUS:2, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4501866/3033)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x8F1592D2(2400555730)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2001, flow_id: AIM-VPN/BPII-PLUS:1, crypto map: Tunnel1-head-0
```

```
sa timing: remaining key lifetime (k/sec): (4501866/3032)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

```
RouterB(config)#do show cry ipsec sa

interface: Tunnel1
Crypto map tag: Tunnel1-head-0, local addr 209.165.201.1

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 209.165.200.225 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 209.165.201.1, remote crypto endpt.: 209.165.200.225
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0xF7B373C0(4155732928)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8F1592D2(2400555730)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2003, flow_id: NETGX:3, sibling_flags 80000046, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4424128/3016)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xF7B373C0(4155732928)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2004, flow_id: NETGX:4, sibling_flags 80000046, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (k/sec): (4424128/3016)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcp sas:
```

После изменения записи DNS для b. cisco . com на сервере DNS от 209.165.201.1 до 209.165.202.129, EEM сделает маршрутизатор A причины для понимания, и

туннель восстановит с корректным новым IP-адресом.

```
RouterB(config)#do show ip int brie
Interface IP-Address OK? Method Status Protocol
FastEthernet0/0 209.165.202.129 YES TFTP up up
FastEthernet0/1 192.168.20.1 YES manual up up
Tunnel1 172.16.12.2 YES manual up up


RouterA(config-if)#do show run int tunn1
Building configuration...

Current configuration : 192 bytes
!
interface Tunnel1
ip address 172.16.12.1 255.255.255.252
tunnel source fastethernet0/0
tunnel destination 209.165.202.129
tunnel mode ipsec ipv4
tunnel protection ipsec profile ipsec-profile
endRouter1841A#show cry isa sa
dst src state conn-id slot status
209.165.200.225 209.165.202.129 QM_IDLE 3 0 ACTIVE
```

Устранение неполадок

Можно обратиться к IPSec IOS и отладкам IKE - Устранение проблем Основного режима IKEv1 для общего IKE/УСТРАНЕНИЯ ПРОБЛЕМ ПРОТОКОЛА IPSEC.

Дополнительные сведения

- Разрешение в реальном времени для узла туннеля IPSec
- Cisco Systems – техническая поддержка и документация