Dinâmico ao exemplo de configuração dinâmico do túnel de IPsec

Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Configurar](#)
[Definição do tempo real para o par do túnel de IPsec](#)
[Atualização do destino de túnel com o gerente encaixado do evento (EEM)](#)
[Verificar](#)
[Troubleshooting](#)
[Informações Relacionadas](#)

Introdução

Este documento descreve como construir um túnel IPSec de LAN para LAN entre roteadores Cisco quando o ambas as extremidades tem endereços IP dinâmicos mas o Domain Name System dinâmico (DDNS) está configurado.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- VPN de Site-para-Site com um túnel de IPsec e o Generic Routing Encapsulation (GRE)
- Interface de túnel virtual do IPsec (VTI)
- Os DN Dinâmicos apoiam para o Cisco IOS Software

Tip: Refira a seção configurando VPN do Cisco 3900 Series, 2900 Series, e manual de configuração do software do 1900 Series e configurar uma interface de túnel virtual com o artigo da Segurança IP para mais informação.

Componentes Utilizados

A informação neste documento é baseada em um roteador dos Serviços integrados de Cisco 2911 que execute a versão 15.2(4)M6a.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Quando um túnel de LAN para LAN precisa de ser estabelecido, o endereço IP de Um ou Mais Servidores Cisco ICM NT de ambos os ipsec peer deve ser sabido. Se um dos endereços IP de Um ou Mais Servidores Cisco ICM NT não é sabido porque é dinâmico, como um obtido através do DHCP, a seguir de uma alternativa é usar um mapa cripto dinâmico. Isto trabalha, mas o túnel pode somente ser trazido acima pelo par que tem o IP address dinâmico desde que o outro par não sabe onde encontrar seu par.

Para obter mais informações sobre de dinâmico à estática, refira configurar o IPSec dinâmico a estático de roteador a roteador com NAT.

Configurar

Definição do tempo real para o par do túnel de IPsec

O ® do Cisco IOS introduziu uns novos recursos na versão 12.3(4)T que permite que o nome de domínio totalmente qualificado (FQDN) do ipsec peer seja especificado. Quando há o tráfego que combina uma lista de acessos cripto, Cicso IO a seguir resolve o FQDN e obtém o endereço IP de Um ou Mais Servidores Cisco ICM NT do par. Tenta então trazer acima o túnel.

Note: Há uma limitação nesta característica: A definição dos nomes de DNS para ipsec peer

remotos trabalhará somente se são usados como um iniciador. O primeiro pacote que deve ser cifrada provocará uma pesquisa de DNS; depois que a pesquisa de DNS está completa, os pacotes subsequente provocarão o Internet Key Exchange (IKE). A definição do tempo real não trabalhará no que responde.

A fim endereçar a limitação e poder iniciar o túnel de cada local, você terá uma entrada do mapa cripto dinâmico em ambo o Roteadores assim que você pode traçar conexões IKE de entrada ao cripto dinâmico. Isto é necessário desde que a entrada estática com a característica da definição do tempo real não trabalha quando atua como um que responde.

Roteador 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
```

roteador 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
```

> **Note**: Desde que você não sabe que endereço IP de Um ou Mais Servidores Cisco ICM NT o FQDN estará usando, você precisa de usar uma chave pré-compartilhada do convite: 0.0.0.0 0.0.0.0

Atualização do destino de túnel com o gerente encaixado do evento (EEM)

Você pode igualmente VTI a fim realizar este. A configuração básica é mostrada aqui:

Roteador 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
```

roteador 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
```

Uma vez que a configuração precedente é no lugar com um FQDN como o destino de túnel, o **comando show run** mostra o endereço IP de Um ou Mais Servidores Cisco ICM NT em vez do nome. Isto é porque a definição acontece apenas uma vez:

```
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
end

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
```

Uma ação alternativa para esta é configurar um applet a fim resolver o destino de túnel cada minuto:

Roteador 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
```

roteador 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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

```
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 up

RouterA(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 ACTIVE

RouterA(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:
```

Depois que você muda o registro DNS para b.cisco.com no servidor DNS de 209.165.201.1 a 209.165.202.129, o EEM fará o roteador A da causa para realizar e o túnel restabelecerá com o endereço IP de Um ou Mais Servidores Cisco ICM NT novo correto.

```
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
end

Router1841A#show cry isa sa
dst src state conn-id slot status
209.165.200.225 209.165.202.129 QM_IDLE 3 0 ACTIVE
```

Troubleshooting

Você pode referir o IPsec IO e o IKE debuga - o modo principal IKEv1 que pesquisa defeitos para o Troubleshooting comum IKE/IPsec.

Informações Relacionadas

- Definição do tempo real para o par do túnel de IPsec
- Suporte Técnico e Documentação - Cisco Systems