Ejemplo de Configuración de Túnel IPsec Dinámico a Dinámico

Contenido

Introducción

Este documento describe cómo construir un túnel IPsec de LAN a LAN entre routers Cisco cuando ambos extremos tienen direcciones IP dinámicas pero se configura el sistema de nombres de dominio dinámico (DDNS).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- VPN de sitio a sitio con túnel IPSec y encapsulación de routing genérico (GRE)
- Interfaz de túnel virtual (VTI) IPsec
- Soporte DNS Dinámico para Cisco IOS Software

Consejo: Consulte la sección Configuración de VPN de la Guía de Configuración de Software de las Series 3900, 2900 y 1900 de Cisco y el artículo Configuración de una Interfaz de Túnel Virtual con Seguridad IP para obtener más información.

Componentes Utilizados

La información de este documento se basa en un Cisco 2911 Integrated Services Router que ejecuta la versión 15.2(4)M6a.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

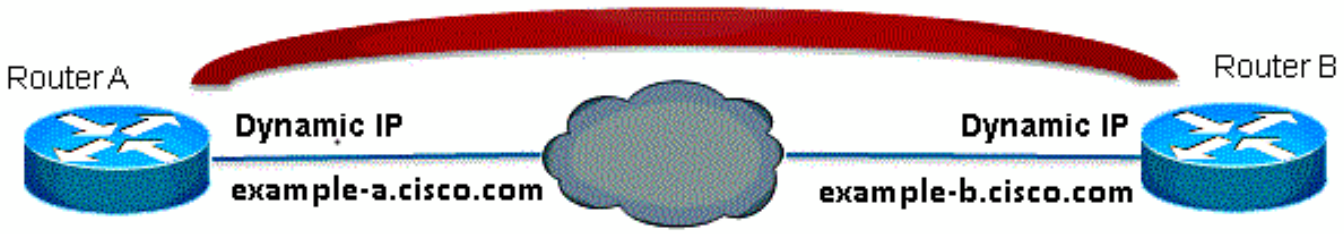
Cuando se necesita establecer un túnel de LAN a LAN, se debe conocer la dirección IP de ambos pares IPSec. Si una de las direcciones IP no se conoce porque es dinámica, como la obtenida a través de DHCP, entonces una alternativa es utilizar un mapa criptográfico dinámico. Esto funciona, pero el túnel sólo puede ser activado por el par que tiene la dirección IP dinámica ya que el otro par no sabe dónde encontrar su par.

Para obtener más información sobre dinámica a estática, refiérase a Configuración de IPSec Dinámico a Estático de Router a Router con NAT.

Configurar

Real-Time Resolution for IPsec Tunnel Peer

Cisco IOS® introdujo una nueva función en la versión 12.3(4)T que permite especificar el nombre de dominio completo (FQDN) del par IPSec. Cuando hay tráfico que coincide con una lista de acceso crypto, Cisco IOS resuelve el FQDN y obtiene la dirección IP del par. Luego intenta abrir el túnel.



Nota: Hay una limitación en esta función: la resolución de nombres DNS para peers IPsec remotos funcionará sólo si se utilizan como iniciadores. El primer paquete que se cifrará activará una búsqueda de DNS; una vez finalizada la búsqueda de DNS, los paquetes subsiguientes activarán el intercambio de claves de Internet (IKE). La resolución en tiempo real no funcionará en el respondedor.

Para abordar la limitación y poder iniciar el túnel desde cada sitio, tendrá una entrada de mapa criptográfico dinámico en ambos routers para que pueda asignar las conexiones IKE entrantes a la criptografía dinámica. Esto es necesario ya que la entrada estática con la función de resolución en tiempo real no funciona cuando actúa como respondedor.

Router 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
```

Router 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
```

> **Nota**: Dado que no sabe qué dirección IP utilizará el FQDN, debe utilizar una clave precompartida comodín: 0.0.0.0 0.0.0.0

Actualización de destino del túnel con Embedded Event Manager (EEM)

También puede VTI para lograr esto. Aquí se muestra la configuración básica:

Router 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
```

Router 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
```

Una vez que la configuración anterior está en funcionamiento con un FQDN como destino del túnel, el comando **show run** muestra la dirección IP en lugar del nombre. Esto se debe a que la resolución se produce una sola 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
```

Una solución temporal para esto es configurar un applet para resolver el destino del túnel cada minuto:

Router A

```
event manager applet change-tunnel-dest
event timer cron name TAC cron-entry "* * * * *"
action 1.0 cli command "enable"
action 1.1 cli command "configure terminal"
action 1.2 cli command "interface tunnel1"
action 1.3 cli command "tunnel destination example-b.cisco.com"
```

Router B

```
event manager applet change-tunnel-dest
event timer cron name TAC cron-entry "* * * * *"
action 1.0 cli command "enable"
```

```
action 1.1 cli command "configure terminal"
action 1.2 cli command "interface tunnel1"
action 1.3 cli command "tunnel destination example-a.cisco.com"
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

```
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:
```

Después de cambiar el registro DNS para b.cisco.com en el servidor DNS de 209.165.201.1 a 209.165.202.129, el EEM hará que el router A se dé cuenta y el túnel se restablecerá con la nueva dirección IP correcta.

```
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
```

Troubleshoot

Puede hacer referencia a debugs de IOS IPSec e IKE - Resolución de problemas del modo principal de IKEv1 para la resolución de problemas comunes de IKE/IPsec.

Información Relacionada

- Real-Time Resolution for IPsec Tunnel Peer
- Soporte Técnico y Documentación - Cisco Systems