

Dinámico al ejemplo de configuración dinámico del túnel IPsec

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Real-Time Resolution for IPsec Tunnel Peer](#)

[Actualización del destino del túnel con el administrador del evento integrado \(EEM\)](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo construir a túnel ipsec de LAN a LAN entre los routers Cisco cuando los ambos extremos tienen IP Address dinámicos pero se configura el Sistema de nombres de dominio (DNS) dinámico (DDNS).

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- VPN de sitio a sitio con un túnel IPsec y el Generic Routing Encapsulation (GRE)
- Interfaz del túnel virtual del IPsec (VTI)
- [Los dn dinámico soportan para el Cisco IOS Software](#)

Consejo: Refiera a la sección [VPN que configura de las](#) Cisco 3900 Series, las 2900 Series, y guía de configuración de software de las 1900 Series y [configurar una interfaz del túnel virtual con el](#) artículo de la [seguridad IP](#) para más información.

Componentes Utilizados

La información en este documento se basa en un router de los Servicios integrados de Cisco 2911 que funcione con la versión 15.2(4)M6a.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Cuando un túnel de LAN a LAN necesita ser establecido, la dirección IP de ambos peers IPsec debe ser sabida. Si uno de los IP Addresses no se sabe porque son dinámicos, por ejemplo uno obtenido vía el DHCP, después una alternativa es utilizar una correspondencia cifrada dinámica. Esto trabaja, pero el túnel se puede traer solamente para arriba por el par que tiene el IP address dinámico puesto que el otro par no sabe dónde encontrar a su par.

Para más información sobre dinámico a los parásitos atmosféricos, refiera a [configurar el IPsec dinámica a estática de router a router con NAT](#).

Configurar

Real-Time Resolution for IPsec Tunnel Peer

El ® del Cisco IOS introdujo una nueva función en la versión 12.3(4)T que permite que el nombre de dominio completo (FQDN) del peer IPsec sea especificado. Cuando hay el tráfico que hace juego una lista de acceso crypto, el IOS de Cisco después resuelve el FQDN y obtiene la dirección IP del par. Entonces intenta traer para arriba el túnel.



Nota: Hay una limitación en esta característica: La resolución de los nombres DNS para los peers IPsec remotos trabajará solamente si se utilizan como iniciador. El primer paquete que debe ser cifrado accionará una búsqueda de DNS; después de que la búsqueda de DNS sea completa, los paquetes subsiguientes accionarán el Internet Key Exchange (IKE). La resolución en tiempo real no trabajará en el respondedor.

Para dirigir la limitación y poder iniciar el túnel de cada sitio, usted tendrá una entrada de la correspondencia cifrada dinámica en ambo Routers así que usted puede asociar las conexiones IKE entrantes al crypto dinámico. Esto es necesario puesto que la Entrada estática con la característica en tiempo real de la resolución no trabaja 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: Puesto que usted no sabe qué dirección IP utilizará el FQDN, usted necesita utilizar una clave previamente compartida del comodín: 0.0.0.0 0.0.0.0

Actualización del destino del túnel con el administrador del evento integrado (EEM)

Usted puede también VTI para lograr esto. La configuración básica se muestra aquí:

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 Tunnell
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 Tunnell  
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 previa existe con un FQDN como el destino del túnel, el **comando show run** muestra la dirección IP en vez del nombre. Esto es porque sucede la resolución apenas una vez:

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

```
Current configuration : 130 bytes  
!  
interface Tunnell  
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 Tunnell  
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 alternativa para esto es configurar un applet para resolver el destino del túnel cada minuto:

router A

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

```
Current configuration : 130 bytes  
!  
interface Tunnell  
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
```

router B

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

```
Current configuration : 130 bytes  
!  
interface Tunnell  
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
```

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
Tunnell 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
Tunnell 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: Tunnell
```

```
Crypto map tag: Tunnell-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 = {Tunnell, }
```

```
conn id: 2002, flow_id: AIM-VPN/BPII-PLUS:2, crypto map: Tunnell-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: Tunnell-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: Tunnell

Crypto map tag: Tunnell-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: Tunnell-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: Tunnell-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 que usted cambie el expediente DNS para b.cisco.com en el servidor DNS de 209.165.201.1 a 209.165.202.129, el EEM hará al router A de la causa para realizar y el túnel 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
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
```

Troubleshooting

Usted puede referir al [IPSec IOS y a los debugs IKE - el modo principal IKEv1 que resuelve problemas](#) para el troubleshooting común IKE/IPsec.

Información Relacionada

- [Real-Time Resolution for IPsec Tunnel Peer](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)