Configurar el VPN de múltiples puntos dinámico usando el GRE sobre IPSec con el EIGRP, el NAT, y el CBAC

Contenido

Introducción

Este documento ofrece un ejemplo de configuración de una VPN multipunto dinámica (DMVPN) para el concentrador y el radio utilizando la encapsulación de ruteo genérico (GRE) sobre IPSec con el Protocolo de ruteo de gateway interior mejorado (EIGRP), la Traducción de dirección de red (NAT) y el Control de acceso basado en contexto (CBAC).

prerrequisitos

Requisitos

Antes de que un GRE multipunto (mGRE) y un túnel IPSec puedan establecerse, deberá definir una política de intercambio de claves de Internet (IKE) mediante el comando crypto isakmp policy.

Note: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes registrados).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software Release 12.2(15)T1 de Cisco IOS® en el router de eje de conexión y 12.3(1.6) en los routeres radiales
- Cisco 3620 como router de eje de conexión, dos routers Cisco 1720 y un router Cisco 3620 como routers radiales

La información que se presenta en este documento se originó a partir de dispositivos dentro de 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 un comando antes de ejecutarlo.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

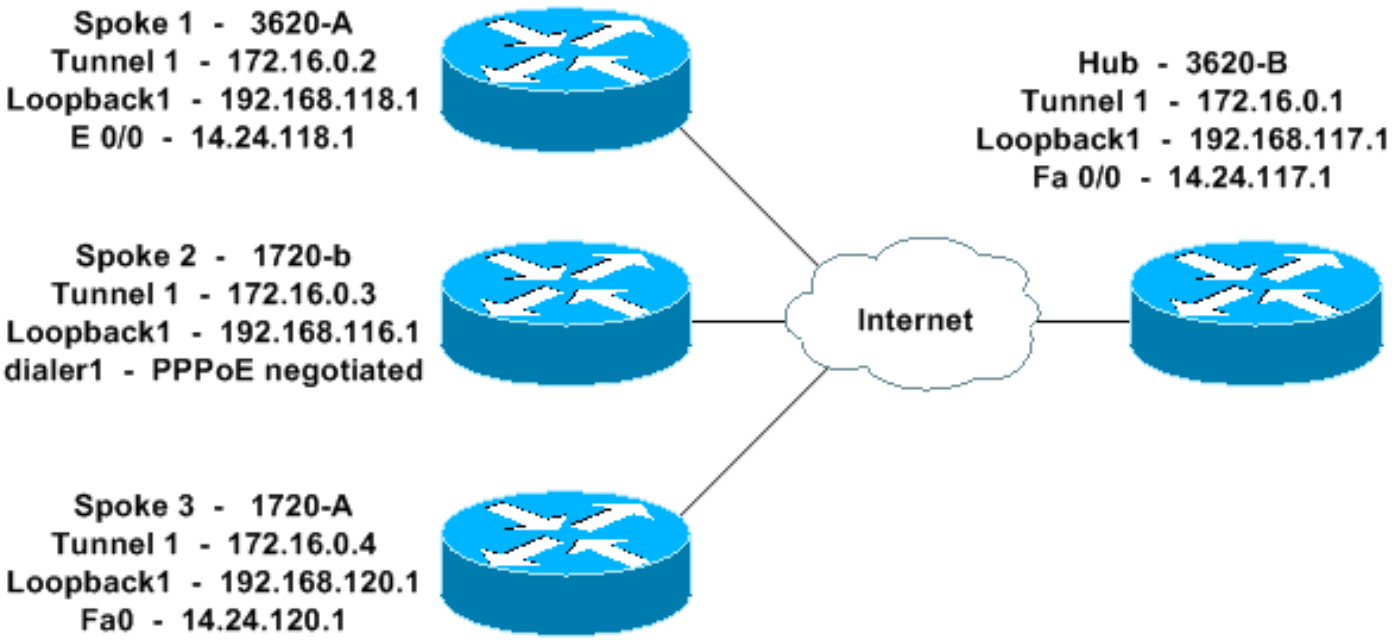
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Note: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes registrados).

Diagrama de la red

Este documento utiliza la instalación de red que se muestra en el siguiente diagrama.



Configuraciones

Este documento usa las configuraciones detalladas a continuación.

- Concentrador - 3620-B

- Spoke 1 - 3620-A
- Spoke 2 - 1720-b
- Spoke 3 – 1720-A

Concentrador - 3620-B

```
3620-B#write terminal
Building configuration...

Current configuration : 2607 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 3620-B
!
logging queue-limit 100
!
memory-size iomem 10
ip subnet-zero
!
!
ip cef
no ip domain lookup
!
!--- This is the CBAC configuration and what to inspect.
!--- This will be applied outbound on the external
interface. ip inspect name in2out rcmd ip inspect name
in2out ftp ip inspect name in2out tftp ip inspect name
in2out tcp timeout 43200 ip inspect name in2out http ip
inspect name in2out udp ip audit po max-events 100 ! ! !
!--- Create an Internet Security Association and Key
Management !--- Protocol (ISAKMP) policy for Phase 1
negotiations. ! crypto isakmp policy 5 authentication
pre-share group 2 !--- Add dynamic pre-shared key. !---
Here "dmvpn" is the word that is used as the key. crypto
isakmp key dmvpnkey address 0.0.0.0 0.0.0.0 crypto
isakmp nat keepalive 20 ! ! !--- Create the Phase 2
policy for actual data encryption. crypto ipsec
transform-set dmvpnset esp-3des esp-sha-hmac ! !---
Create an IPSec profile to be applied dynamically !---
to the GRE over IPSec tunnels. crypto ipsec profile
dmvpnprof set transform-set dmvpnset ! ! no voice hpi
capture buffer no voice hpi capture destination ! ! mta
receive maximum-recipients 0 ! ! !--- This is the inside
interface. interface Loopback1 ip address 192.168.117.1
255.255.255.0 ip nat inside ! !--- This is the mGRE
interface for dynamic GRE tunnels. interface Tunnel1
description MULTI-POINT GRE TUNNEL for BRANCHES
bandwidth 1000 ip address 172.16.0.1 255.255.255.0 no ip
redirects ip mtu 1400 ip nhrp authentication dmvpn ip
nhrp map multicast dynamic ip nhrp network-id 99 ip nhrp
holdtime 300 no ip split-horizon eigrp 1 no ip mroute-
cache delay 1000 tunnel source FastEthernet0/0 tunnel
mode gre multipoint tunnel key 100000 tunnel protection
ipsec profile dmvpnprof ! !--- This is the outside
interface. interface FastEthernet0/0 ip address
14.24.117.1 255.255.0.0 ip nat outside ip access-group
100 in ip inspect in2out out no ip mroute-cache duplex
auto speed auto ! interface Serial0/0 no ip address
```

```
shutdown clockrate 2000000 no fair-queue ! interface
FastEthernet0/1 no ip address no ip mroute-cache duplex
auto speed auto ! !--- Enable a routing protocol to
send/receive dynamic !--- updates about the private
networks over the tunnels. router eigrp 1 network
172.16.0.0 0.0.0.255 network 192.168.117.0 no auto-
summary ! !--- Perform NAT on local traffic !--- going
directly out FastEthernet0/0. ip nat inside source list
110 interface FastEthernet0/0 overload ip http server no
ip http secure-server ip classless ip route 0.0.0.0
0.0.0.0 14.24.1.1 ip route 2.0.0.0 255.0.0.0 14.24.121.1
! ! ! !--- Allow ISAKMP, ESP, and GRE traffic inbound.
!--- CBAC will open other inbound access as needed.
access-list 100 permit udp any host 14.24.117.1 eq 500
access-list 100 permit esp any host 14.24.117.1 access-
list 100 permit gre any host 14.24.117.1 access-list 100
deny ip any any access-list 110 permit ip 192.168.117.0
0.0.0.255 any ! ! call rsvp-sync ! ! mgcp profile
default ! dial-peer cor custom ! ! line con 0 exec-
timeout 0 0 line aux 0 line vty 0 4 login ! ! end 3620-
B#
```

Spoke 1 - 3620-A

```
3620-A#write terminal
Building configuration...

Current configuration : 2559 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3620-A
!
boot system flash slot0:c3620-ik9o3s7-mz.122-15.T1.bin
logging queue-limit 100
!
memory-size iomem 15
ip subnet-zero
!
!
ip cef
no ip domain lookup
!
!--- This is the CBAC configuration and what to inspect.
!--- This will be applied outbound on the external
interface. ip inspect name in2out rcmd ip inspect name
in2out tftp ip inspect name in2out udp ip inspect name
in2out tcp timeout 43200 ip inspect name in2out
realaudio ip inspect name in2out vdolive ip inspect name
in2out netshow ip audit po max-events 100 ! ! ! !---
Create an ISAKMP policy for !--- Phase 1 negotiations.
crypto isakmp policy 5 authentication pre-share group 2
!--- Add dynamic pre-shared key. crypto isakmp key
dmvpnkey address 0.0.0.0 0.0.0.0 ! ! !--- Create the
Phase 2 policy for actual data encryption. crypto ipsec
transform-set dmvpnset esp-3des esp-sha-hmac ! !---
Create an IPSec profile to be applied dynamically !---
to the GRE over IPSec tunnels. crypto ipsec profile
dmvpnprof set transform-set dmvpnset ! ! no voice hpi
capture buffer no voice hpi capture destination ! ! mta
```

```
receive maximum-recipients 0 ! ! !--- This is the inside
interface. interface Loopback1 ip address 192.168.118.1
255.255.255.0 ip nat inside ! !--- This is the mGRE
interface for dynamic GRE tunnels. interface Tunnel1
description HOST DYNAMIC TUNNEL bandwidth 1000 ip
address 172.16.0.2 255.255.255.0 no ip redirects ip mtu
1400 ip nhrp authentication dmvpn ip nhrp map 172.16.0.1
14.24.117.1 ip nhrp map multicast 14.24.117.1 ip nhrp
network-id 99 ip nhrp holdtime 300 ip nhrp nhs
172.16.0.1 no ip mroute-cache delay 1000 tunnel source
Ethernet0/0 tunnel mode gre multipoint tunnel key 100000
tunnel protection ipsec profile dmvpnprof ! !--- This is
the outside interface. interface Ethernet0/0 ip address
14.24.118.1 255.255.0.0 ip nat outside ip inspect in2out
out ip access-group 100 in no ip mroute-cache half-
duplex ! interface Ethernet0/1 no ip address half-duplex
! interface Ethernet0/2 no ip address shutdown half-
duplex ! interface Ethernet0/3 no ip address shutdown
half-duplex ! !--- Enable a routing protocol to
send/receive dynamic !--- updates about the private
networks over the tunnel. router eigrp 1 network
172.16.0.0 0.0.0.255 network 192.168.118.0 no auto-
summary ! !--- Perform NAT on local traffic !--- going
directly out Ethernet0/0. ip nat inside source list 110
interface Ethernet0/0 overload ip http server no ip http
secure-server ip classless ip route 0.0.0.0 0.0.0.0
14.24.1.1 ! ! !--- Allow ISAKMP, ESP, and GRE traffic
inbound. !--- CBAC will open inbound access as needed.
access-list 100 permit udp any host 14.24.118.1 eq 500
access-list 100 permit esp any host 14.24.118.1 access-
list 100 permit gre any host 14.24.118.1 access-list 100
deny ip any any access-list 110 permit ip 192.168.118.0
0.0.0.255 any ! ! call rsvp-sync ! ! mgcp profile
default ! dial-peer cor custom ! ! line con 0 exec-
timeout 0 0 line aux 0 line vty 0 4 login ! ! end 3620-
A#
```

Spoke 2 - 1720-b

```
1720-b#write terminal
Building configuration...

Current configuration : 2543 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1720-b
!
boot system flash flash:c1700-ny-mz.122-8.YJ
logging queue-limit 100
enable password cisco
!
username 7206-B password 0 cisco
ip subnet-zero
!
!
no ip domain lookup
!
ip cef
!--- This is the CBAC configuration and what to inspect.
```

```
!--- This will be applied outbound on the external
interface. ip inspect name in2out rcmd ip inspect name
in2out tftp ip inspect name in2out udp ip inspect name
in2out tcp timeout 43200 ip inspect name in2out
realaudio ip inspect name in2out vdolive ip inspect name
in2out netshow ip audit po max-events 100 ! ! vpdn-group
1 request-dialin protocol pppoe ! ! !--- Create an
ISAKMP policy for !--- Phase 1 negotiations. crypto
isakmp policy 5 authentication pre-share group 2 !---
Add dynamic pre-shared key. crypto isakmp key dmvpnkey
address 0.0.0.0 0.0.0.0 ! ! !--- Create the Phase 2
policy for actual data encryption. crypto ipsec
transform-set dmvpnset esp-3des esp-sha-hmac ! !---
Create an IPSec profile to be applied dynamically !---
to the GRE over IPSec tunnels. crypto ipsec profile
dmvpnprof set transform-set dmvpnset ! ! !--- This is
the inside interface. interface Loopback1 ip address
192.168.116.1 255.255.255.0 ip nat inside ! !--- This is
the mGRE interface for dynamic GRE tunnels. interface
Tunnel1 description HOST DYNAMIC TUNNEL bandwidth 1000
ip address 172.16.0.3 255.255.255.0 no ip redirects ip
mtu 1400 ip nhrp authentication dmvpn ip nhrp map
172.16.0.1 14.24.117.1 ip nhrp map multicast 14.24.117.1
ip nhrp network-id 99 ip nhrp holdtime 300 ip nhrp nhs
172.16.0.1 no ip mroute-cache delay 1000 tunnel source
Dialer1 tunnel mode gre multipoint tunnel key 100000
tunnel protection ipsec profile dmvpnprof ! interface
Ethernet0 no ip address half-duplex ! interface
FastEthernet0 no ip address no ip mroute-cache speed
auto pppoe enable pppoe-client dial-pool-number 1 ! !---
This is the outside interface. interface Dialer1 ip
address 2.2.2.10 255.255.255.0 ip inspect in2out out ip
access-group 100 in encapsulation ppp dialer pool 1
dialer-group 1 ppp authentication pap chap callin ! !---
Enable a routing protocol to send/receive dynamic !---
updates about the private networks. router eigrp 1
network 172.16.0.0 0.0.0.255 network 192.168.116.0 no
auto-summary ! !--- Perform NAT on local traffic !---
going directly out Dialer1. ip nat inside source list
110 interface Dialer1 overload ip classless ip route
0.0.0.0 0.0.0.0 Dialer1 no ip http server no ip http
secure-server ! ! ! !--- Allow ISAKMP, ESP, and GRE
traffic inbound. !--- CBAC will open inbound access as
needed. access-list 100 permit udp any host 14.24.116.1
eq 500 access-list 100 permit esp any host 14.24.116.1
access-list 100 permit gre any host 14.24.116.1 access-
list 100 deny ip any any access-list 110 permit ip
192.168.116.0 0.0.0.255 any dialer-list 1 protocol ip
permit ! ! ! line con 0 exec-timeout 0 0 line aux 0 line
vty 0 4 login ! no scheduler allocate end 1720-b#
```

Spoke 3 – 1720-A

```
1720-A#write terminal
Building configuration...

Current configuration : 1770 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
```

```
hostname 1720-A
!
logging queue-limit 100
!
memory-size iomem 25
ip subnet-zero
!
!
!
ip cef
!--- This is the CBAC configuration and what to inspect.
!--- This will be applied outbound on the external
interface. ip inspect name in2out rcmd ip inspect name
in2out tftp ip inspect name in2out udp ip inspect name
in2out tcp timeout 43200 ip inspect name in2out
realaudio ip inspect name in2out vdolive ip inspect name
in2out netshow ip audit po max-events 100 ! ! !---
Create an ISAKMP policy for !--- Phase 1 negotiations.
crypto isakmp policy 5 authentication pre-share group 2
!--- Add dynamic pre-shared key. crypto isakmp key
dmvpnkey address 0.0.0.0 0.0.0.0 ! ! !--- Create the
Phase 2 policy for actual data encryption. crypto ipsec
transform-set dmvpnset esp-3des esp-sha-hmac ! !---
Create an IPSec profile to be applied dynamically !---
to the GRE over IPSec tunnels. crypto ipsec profile
dmvpnprof set transform-set dmvpnset ! ! !--- This is
the inside interface. interface Loopback1 ip address
192.168.120.1 255.255.255.0 ip nat inside ! !--- This is
the mGRE interface for dynamic GRE tunnels. interface
Tunnel1 description HOST DYNAMIC TUNNEL bandwidth 1000
ip address 172.16.0.4 255.255.255.0 no ip redirects ip
mtu 1400 ip nhrp authentication dmvpn ip nhrp map
172.16.0.1 14.24.117.1 ip nhrp map multicast 14.24.117.1
ip nhrp network-id 99 ip nhrp holdtime 300 ip nhrp nhs
172.16.0.1 no ip mroute-cache delay 1000 tunnel source
FastEthernet0 tunnel mode gre multipoint tunnel key
100000 tunnel protection ipsec profile dmvpnprof !
interface Ethernet0 no ip address no ip mroute-cache
half-duplex ! !--- This is the outside interface.
interface FastEthernet0 ip address 14.24.120.1
255.255.0.0 ip nat outside ip inspect in2out out ip
access-group 100 in no ip mroute-cache speed auto ! !---
Enable a routing protocol to send/receive dynamic !---
updates about the private networks. router eigrp 1
network 172.16.0.0 0.0.0.255 network 192.168.120.0 no
auto-summary ! !--- Perform NAT on local traffic !---
going directly out FastEthernet0. ip nat inside source
list 110 interface FastEthernet0 overload ip classless
ip route 0.0.0.0 0.0.0.0 14.24.1.1 no ip http server no
ip http secure-server ! ! ! !--- Allow ISAKMP, ESP, and
GRE traffic inbound. !--- CBAC will open inbound access
as needed. access-list 100 permit udp any host
14.24.116.1 eq 500 access-list 100 permit esp any host
14.24.116.1 access-list 100 permit gre any host
14.24.116.1 access-list 100 deny ip any any access-list
110 permit ip 192.168.120.0 0.0.0.255 any ! ! ! line con
0 exec-timeout 0 0 line aux 0 line vty 0 4 login ! no
scheduler allocate end 1720-A#
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración

esté funcionando correctamente.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

- **muestre isakmp crypto sa** — Visualiza el estado para la asociación de seguridad ISAKMP (SA).
- **active del show crypto engine connections** — Visualiza el total cifra/desencripta por el SA.
- show crypto ipsec sa — Muestra las estadísticas en los túneles activos.
- show ip route — Muestra la tabla de ruteo.
- show ip eigrp neighbor—Muestra los vecinos EIGRP.
- show ip nhrp — Muestra la memoria caché del Protocolo de resolución de salto siguiente (NHRP) de IP, opcionalmente limitado a entradas de caché estáticas o dinámicas para un determinada interfaz.
- show crypto socket—Muestra la tabla de zócalo de criptografía entre NHRP e IPSec.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

Note: Antes de ejecutar un comando debug, consulte Información Importante sobre Comandos Debug.

- debug crypto ipsec — Muestra eventos de IPSec.
- debug crypto isakmp — Muestra mensajes acerca de eventos IKE.
- debug crypto engine — Muestra información del motor de criptografía.
- debug crypto socket—Muestra información sobre la tabla de zócalo entre NHRP e IPSec.
- debug nhrp packet—Muestra información sobre paquetes NHRP.
- debug nhrp packet—Muestra información sobre paquetes NHRP.
- debug tunnel protection—Muestra información acerca de los túneles GRE dinámicos.

Puede encontrar información adicional sobre la resolución de problemas de IPSec en Resolución de problemas de seguridad IP – Introducción y uso de los comandos de depuración.

Información Relacionada

- Información general de DMVPN y Cisco IOS
- Página de soporte de IPSec
- Soporte Técnico y Documentación - Cisco Systems