Configuración de Dynamic Multipoint VPN Usando GRE sobre IPsec con OSPF, NAT y Cisco IOS Firewall

Contenido

Introducción

Este documento proporciona una configuración de ejemplo de DMVPN (Dynamic Multipoint VPN) usando GRE (Generic Routing Encapsulation) sobre IPSec con OSPF (Open Shortest Path First), Traducción de Dirección de Red (NAT) y Cisco IOS® Firewall.

Prerequisites

Requirements

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.

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Componentes Utilizados

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

- Cisco IOS® Software Release 12.2(15)T1 en el router hub y Cisco IOS Software Release

12.3(1.6) en los routers spoke

- Cisco 3620 como router de eje de conexión, dos routers Cisco 1720 y un router Cisco 3620 como routers radiales

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). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

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

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

Este documento utiliza esta configuración de red:

Configuraciones

Este documento usa estas configuraciones.

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

Concentrador - 3620-B
<#root> W2N-6.16-3620-B# **write terminal** Building configuration... Current configuration : 2613 bytes

```
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname W2N-6.16-3620-B
!
logging queue-limit 100
!
memory-size iomem 10
ip subnet-zero
!
!
ip cef
no ip domain lookup
!

!--- This is the Cisco IOS Firewall configuration and what to inspect. !--- This is applied outbound o

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 Phas

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
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 inbound interface.

interface Loopback1
 ip address 192.168.117.1 255.255.255.0
 ip nat inside
!

!--- Create a GRE tunnel template to be applied !--- to all the dynamically created 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 1416
 ip nhrp authentication dmvpn
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 ip nhrp holdtime 300
 no ip route-cache
 ip ospf network broadcast
 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 outbound 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.

router ospf 1
 log-adjacency-changes
 network 172.16.0.0 0.0.0.255 area 0
 network 192.168.117.0 0.0.0.255 area 0
!

!--- Except the private network traffic from the NAT process.

ip nat inside source route-map nonat 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. !--- Cisco IOS Firewall opens other inbound access as

access-list 100 permit udp any host 14.24.117.1 eq 500
access-list 100 premit 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


!--- Except the private network traffic from the NAT process.

access-list 110 deny   ip 192.168.117.0 0.0.0.255 192.168.118.0 0.0.0.255
access-list 110 deny   ip 192.168.117.0 0.0.0.255 192.168.116.0 0.0.0.255
access-list 110 deny   ip 192.168.117.0 0.0.0.255 192.168.120.0 0.0.0.255
access-list 110 permit ip 192.168.117.0 0.0.0.255 any
!

!--- Except the private network traffic from the NAT process.

route-map nonat permit 10
 match ip address 110
!
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
```

```
W2N-6.16-3620-B#
```

Spoke 1 - 3620-A

<#root>

```
W2N-6.16-3620-A#
write terminal

Building configuration...

Current configuration : 2678 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname W2N-6.16-3620-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 Cisco IOS Firewall configuration and what to inspect. !--- This is applied outbound o

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 inbound interface.

interface Loopback1
 ip address 192.168.118.1 255.255.255.0
 ip nat inside
!

!--- Create a GRE tunnel template to be applied to !--- all the dynamically created 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 1416
 ip nhrp authentication dmvpn
 ip nhrp map multicast dynamic
 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 route-cache
 ip ospf network broadcast
 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 outbound interface.

interface Ethernet0/0
 ip address 14.24.118.1 255.255.0.0
 ip nat outside
 ip access-group 100 in
 ip inspect in2out out
 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.

router ospf 1
 log-adjacency-changes
 redistribute connected
 network 172.16.0.0 0.0.0.255 area 0
 network 192.168.118.0 0.0.0.255 area 0
!

!--- Except the private network traffic from the NAT process.

ip nat inside source route-map nonat 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
ip route 2.0.0.0 255.0.0.0 14.24.121.1

!
!
!

!--- Allow ISAKMP, ESP, and GRE traffic inbound. !--- Cisco IOS Firewall opens inbound access as needed

access-list 100 permit udp any host 14.24.118.1 eq 500
access-list 100 premit 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


!--- Except the private network traffic from the NAT process.

access-list 110 deny   ip 192.168.118.0 0.0.0.255 192.168.117.0 0.0.0.255
access-list 110 deny   ip 192.168.118.0 0.0.0.255 192.168.116.0 0.0.0.255
access-list 110 deny   ip 192.168.118.0 0.0.0.255 192.168.120.0 0.0.0.255
access-list 110 permit ip 192.168.118.0 0.0.0.255 any
!
```

```
!--- Except the private network traffic from the NAT process.

route-map nonat permit 10
 match ip address 110
!
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

W2N-6.16-3620-A#
```

Spoke 2 - 1720-b

```
<#root>

1720-b#

write terminal

Building configuration...

Current configuration : 2623 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1720-b
!
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 Cisco IOS Firewall configuration and what to inspect. !--- This is applied outbound o

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 inbound interface.

interface Loopback1
 ip address 192.168.116.1 255.255.255.0
 ip nat inside
!

!--- Create a GRE tunnel template to be applied to !--- all the dynamically created 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 1416
```

```
 ip nhrp authentication dmvpn
 ip nhrp map multicast dynamic
 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 route-cache
 ip ospf network broadcast
 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 outbound 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 ospf 1
 log-adjacency-changes
 redistribute connected
 network 172.16.0.0 0.0.0.255 area 0
 network 192.168.116.0 0.0.0.255 area 0
!

!--- Except the private network traffic from the NAT process.

ip nat inside source route-map nonat interface Dialer1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 14.24.1.1
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. !--- Cisco IOS Firewall opens inbound access as needed
```

```
access-list 100 permit udp any host 14.24.116.1 eq 500
access-list 100 premit 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



!--- Except the private network traffic from the NAT process.

access-list 110 deny   ip 192.168.116.0 0.0.0.255 192.168.117.0 0.0.0.255
access-list 110 deny   ip 192.168.116.0 0.0.0.255 192.168.118.0 0.0.0.255
access-list 110 deny   ip 192.168.116.0 0.0.0.255 192.168.120.0 0.0.0.255
access-list 110 permit ip 192.168.116.0 0.0.0.255 any
dialer-list 1 protocol ip permit
!

!--- Except the private network traffic from the NAT process.

route-map nonat permit 10
 match ip address 110
!
!
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

<#root>

```
W2N-6.16-1720-A#

write terminal

Building configuration...

Current configuration : 2303 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname W2N-6.16-1720-A
!
logging queue-limit 100
!
memory-size iomem 25
ip subnet-zero
!
```

```
!
no ip domain lookup
!
ip cef

!--- This is the Cisco IOS Firewall configuration and what to inspect. !--- This is applied outbound o

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 notify log
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 inbound interface.

interface Loopback1
 ip address 192.168.120.1 255.255.255.0
 ip nat inside
!

!--- Create a GRE tunnel template to be applied to !--- all the dynamically created 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 1416
 ip nhrp authentication dmvpn
 ip nhrp map multicast dynamic
 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
 ip ospf network broadcast
 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 outbound 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 ospf 1
 log-adjacency-changes
 redistribute connected
 network 172.16.0.0 0.0.0.255 area 0
 network 192.168.120.0 0.0.0.255 area 0
!

!--- Except the private network traffic from the NAT process.

ip nat inside source route-map nonat interface FastEthernet0 overload
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
no ip http server
no ip http secure-server
!
!
!

!--- Allow ISAKMP, ESP, and GRE traffic inbound. !--- Cisco IOS Firewall opens inbound access as neede

access-list 100 permit udp any host 14.24.116.1 eq 500
access-list 100 premit 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
```

```
!--- Except the private network traffic from the NAT process.

access-list 110 deny   ip 192.168.120.0 0.0.0.255 192.168.116.0 0.0.0.255
access-list 110 deny   ip 192.168.120.0 0.0.0.255 192.168.117.0 0.0.0.255
access-list 110 deny   ip 192.168.120.0 0.0.0.255 192.168.118.0 0.0.0.255
access-list 110 permit ip 192.168.120.0 0.0.0.255 any
!

!--- Except the private network traffic from the NAT process.

route-map nonat permit 10
 match ip address 110
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end

W2N-6.16-1720-A#
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- show crypto isakmp sa—Muestra el estado de la asociación de seguridad ISAKMP (SA).
- show crypto engine connections active—Muestra el total de cifrados/descifrados por SA.
- show crypto ipsec sa — Muestra las estadísticas en los túneles activos.
- show ip route — Muestra la tabla de ruteo.
- show ip ospf neighbor: muestra la información de vecinos OSPF por interfaz.
- 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.

Troubleshoot

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

Comandos para resolución de problemas

Nota: Consulte Información importante sobre los comandos de depuración antes de utilizar este tipo de comandos.

- 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.

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

- Resolución de problemas de configuración de firewall de Cisco IOS
- Información general de DMVPN y Cisco IOS
- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).