

# Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este documento fornece uma configuração de exemplo para Dynamic Multipoint VPN (DMVPN) que usa Generic Routing Encapsulation (GRE) sobre a IPsec com Open Shortest Path First (OSPF), Tradução de Endereço de Rede (NAT) e Cisco IOS® Firewall.

## [Pré-requisitos](#)

### [Requisitos](#)

Antes de um GRE multiponto (mGRE) e do túnel de IPsec pode ser estabelecido, você deve definir uma política do Internet Key Exchange (IKE) usando o **comando `crypto isakmp policy`**.

**Nota:** Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

### [Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Release 12.2(15)T1 de Cisco IOS® no roteador de hub e no Cisco IOS Software Release 12.3(1.6) no Roteadores do spoke
- Cisco 3620 como roteador de hub, dois Cisco 1720 Routers e um Cisco 3620 Router como roteadores spoke

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.

### [Convenções](#)

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

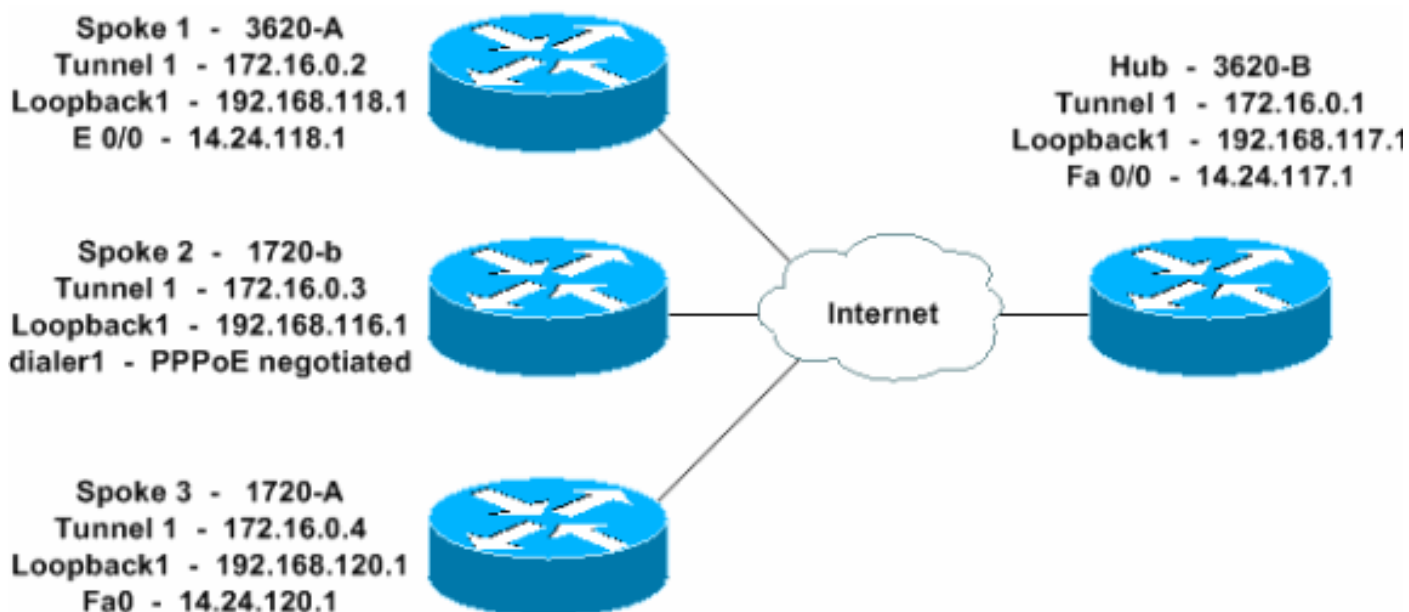
## Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Nota:** Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede.



## Configurações

Este documento utiliza estas configurações.

- [Hub - 3620-B](#)
- [Spoke 1 - 3620-A](#)
- [Spoke 2 - 1720-b](#)
- [Pontos remotos 3 - 1720-A](#)

### Hub - 3620-B

```
W2N-6.16-3620-B#write terminalBuilding
configuration...Current configuration : 2613 bytes!version
12.2service timestamps debug datetime msecservice timestamps
log datetime msecno service password-encryption!hostname W2N-
6.16-3620-B!logging queue-limit 100!memory-size iomem 10ip
subnet-zero!!ip cefno ip domain lookup!!--- This is the Cisco
IOS Firewall configuration and what to inspect. !--- This is
applied outbound on the external interface.ip inspect name
in2out rcmdip inspect name in2out ftpip inspect name in2out
tftpip inspect name in2out tcp timeout 43200ip inspect name
in2out httpip inspect name in2out udpip 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.crypto isakmp key
dmvpnkey address 0.0.0.0 0.0.0.0crypto 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 bufferno 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 overloadip http serverno ip http
secure-serverip classlessip route 0.0.0.0 0.0.0.0 14.24.1.1ip
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 needed.access-list 100 permit udp any host
14.24.117.1 eq 500access-list 100 permit esp any host
14.24.117.1access-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 0.0.0.255access-list
110 deny ip 192.168.117.0 0.0.0.255 192.168.116.0
0.0.0.255access-list 110 deny ip 192.168.117.0 0.0.0.255
192.168.120.0 0.0.0.255access-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 0line aux 0line vty
0 4 login!!endW2N-6.16-3620-B#

```

## Spoke 1 - 3620-A

```

W2N-6.16-3620-A#write terminalBuilding
configuration...Current configuration : 2678 bytes!version
12.2service 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.binlogging queue-limit 100!memory-size iomem 15ip
subnet-zero!!ip cefno ip domain lookup!--- This is the Cisco
IOS Firewall configuration and what to inspect. !--- This is
applied outbound on the external interface.ip inspect name
in2out rcmdip inspect name in2out tftpip inspect name in2out
udpip inspect name in2out tcp timeout 43200ip inspect name

```

```

in2out realaudioip inspect name in2out vdoliveip inspect name
in2out netshowip 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 bufferno 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 Tunnell1 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
overloadip http serverno ip http secure-serverip classlessip
route 0.0.0.0 0.0.0.0 14.24.1.1ip 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
500access-list 100 permit esp any host 14.24.118.1access-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 0.0.0.255access-list 110 deny ip 192.168.118.0
0.0.0.255 192.168.116.0 0.0.0.255access-list 110 deny ip
192.168.118.0 0.0.0.255 192.168.120.0 0.0.0.255access-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
0line aux 0line vty 0 4 login!!endW2N-6.16-3620-A#

```

## Spoke 2 - 1720-b

```

1720-b#write terminalBuilding configuration...Current
configuration : 2623 bytes!version 12.2service timestamps
debug uptimeservice timestamps log uptime no service password-
encryption!hostname 1720-b!logging queue-limit 100enable
password cisco!username 7206-B password 0 ciscoip subnet-
zero!!no ip domain lookup!ip cef!--- This is the Cisco IOS
Firewall configuration and what to inspect. !--- This is
applied outbound on the external interface.ip inspect name

```

```

in2out rcmdip inspect name in2out tftpip inspect name in2out
udpip inspect name in2out tcp timeout 43200ip inspect name
in2out realaudioip inspect name in2out vdoliveip inspect name
in2out netshowip audit po max-events 100vpdn-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 overloadip
classlessip route 0.0.0.0 0.0.0.0 14.24.1.1ip route 0.0.0.0
0.0.0.0 Dialer1no ip http serverno 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 500access-list 100 permit
esp any host 14.24.116.1access-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
0.0.0.255access-list 110 deny ip 192.168.116.0 0.0.0.255
192.168.118.0 0.0.0.255access-list 110 deny ip 192.168.116.0
0.0.0.255 192.168.120.0 0.0.0.255access-list 110 permit ip
192.168.116.0 0.0.0.255 anydialer-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 0line aux 0line vty 0 4 login!no
scheduler allocateend1720-b#

```

### Pontos remotos 3 - 1720-A

```

W2N-6.16-1720-A#write terminalBuilding
configuration...Current configuration : 2303 bytes!version
12.2service timestamps debug datetime msecservice timestamps
log datetime msecno service password-encryption!hostname W2N-
6.16-1720-A!logging queue-limit 100!memory-size iomem 25ip
subnet-zero!!no ip domain lookup!ip cef!--- This is the Cisco
IOS Firewall configuration and what to inspect. !--- This is

```

```

applied outbound on the external interface.ip inspect name
in2out rcmdip inspect name in2out tftpip inspect name in2out
udpip inspect name in2out tcp timeout 43200ip inspect name
in2out realaudioip inspect name in2out vdoliveip inspect name
in2out netshowip audit notify logip 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 overloadip
classlessip route 0.0.0.0 0.0.0.0 14.24.1.1ip route 2.0.0.0
255.0.0.0 14.24.121.1no ip http serverno 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 500access-list
100 permit esp any host 14.24.116.1access-list 100 permit gre
any host 14.24.116.1 access-list 100 deny ip any anyaccess-
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
0.0.0.255access-list 110 deny ip 192.168.120.0 0.0.0.255
192.168.117.0 0.0.0.255access-list 110 deny ip 192.168.120.0
0.0.0.255 192.168.118.0 0.0.0.255access-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 0line aux 0line vty
0 4 login!endW2N-6.16-1720-A#

```

## Verificar

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

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **mostre isakmp cripto sa?** Indica o estado para a associação de segurança ISAKMP (SA).
- **active do show crypto engine connections?** Indica o total cifra/decifra pelo SA.
- **mostre IPsec cripto sa?** Indica as estatísticas nos túneis ativo.
- **mostre a rota IP?** Indica a tabela de roteamento.
- **mostre o vizinho OSPF IP?** Informação do vizinho de OSPF dos indicadores em uma base da interface per.
- **mostre o nhrp IP?** Indica o esconderijo do Next Hop Resolution Protocol (NHRP) IP, opcionalmente limitado a dinâmico ou às entradas de cache estático para uma relação específica.

## Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

### Comandos para Troubleshooting

**Nota:** Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

- **IPsec do debug crypto?** Eventos de IPsec dos indicadores.
- **isakmp do debug crypto?** Indica mensagens sobre eventos IKE.
- **motor do debug crypto?** Indica a informação da crypto-engine.

A informação adicional no IPsec do Troubleshooting pode ser encontrada no [Troubleshooting de Segurança IP - compreendendo e usando comandos debug](#).

## Informações Relacionadas

- [Pesquisando defeitos configurações do Cisco IOS Firewall](#)
- [Visão geral de DMVPN e Cisco IOS](#)
- [Negociação IPsec/Protocolos IKE](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)