

Configuration VPN multipoint dynamique à l'aide de GRE sur IPsec avec OSPF, NAT et pare-feu Cisco IOS

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifier](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Informations connexes](#)

Introduction

Ce document fournit un exemple de configuration du VPN multipoint dynamique (DMVPN) par l'utilisation de l'Encapsulation de routage générique (GRE) pour IPsec avec l'Open Shortest Path First (OSPF), la Traduction d'adresses réseau (NAT), et le pare-feu Cisco IOS®.

Conditions préalables

Exigences

Avant de pouvoir établir un tunnel multipoint GRE (mGRE) et IPsec, vous devez définir une stratégie IKE (Internet Key Exchange) à l'aide de la commande `crypto isakmp policy`.

Remarque : utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco IOS® version 12.2(15)T1 sur le routeur concentrateur et logiciel Cisco IOS

version 12.3(1.6) sur les routeurs satellites

- Cisco 3620 comme routeur concentrateur, deux routeurs Cisco 1720 et un routeur Cisco 3620 comme routeurs satellites

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux [Conventions relatives aux conseils techniques Cisco](#).

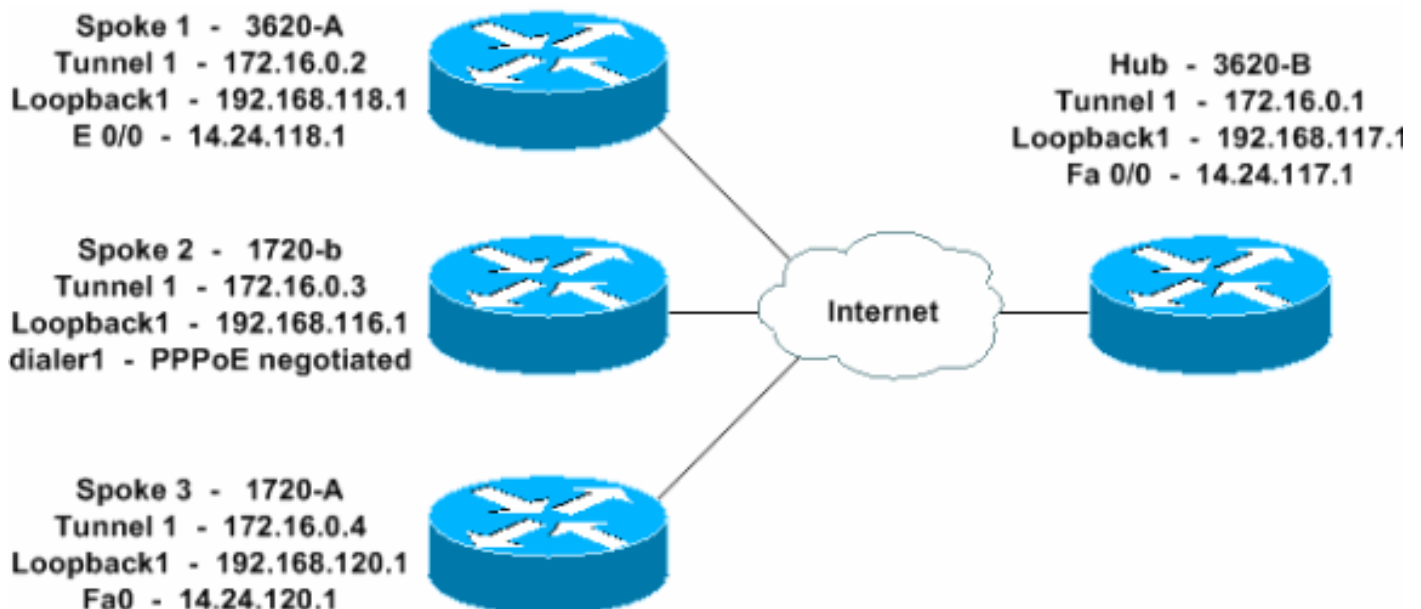
Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise cette configuration du réseau.



Configurations

Ce document utilise les configurations suivantes.

- [Concentrateur - 3620-B](#)

- [Satellite 1 - 3620-A](#)
- [Satellite 2 - 1720-b](#)
- [Satellite 3 - 1720-A](#)

Concentrateur - 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 on
```

```
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
```

```
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 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

!--- 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#

Satellite 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 on

```
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 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  
  
!--- 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#
```

Satellite 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 on

```
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 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

!--- 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#

```

Satellite 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 on

```
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 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

!--- 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#

```

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\) prend en charge certaines commandes show](#). Utilisez l'OIT pour afficher une analyse de la sortie de la commande show .

- show crypto isakmp sa : affiche l'état de l'association de sécurité ISAKMP.
- show crypto engine connections active : affiche le total des chiffrements/déchiffrements par SA.

- show crypto ipsec sa : affiche les statistiques sur les tunnels actifs.
- show ip route : affiche la table de routage.
- show ip ospf neighbor : affiche les informations de voisinage OSPF par interface.
- show ip nhrp : affiche le cache NHRP (IP Next Hop Resolution Protocol), éventuellement limité aux entrées de cache dynamiques ou statiques pour une interface spécifique.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

Remarque : Consultez les renseignements importants sur les commandes de débogage avant d'entrer des commandes de débogage.

- debug crypto ipsec — Affiche des événements IPsec.
- debug crypto isakmp—Affichage de messages d'événements IKE.
- debug crypto engine — Affiche des informations du moteur de chiffrement.

Vous trouverez les informations supplémentaires pour dépanner IPSec à la section [Dépannage de sécurité IP - Présentation et utilisation des commandes de débogage](#).

Informations connexes

- [Dépannage des configurations de Cisco IOS Firewall](#)
- [Présentation de DMVPN et de Cisco IOS](#)
- [Négociation IPSec/Protocoles IKE](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.