

Configuration de VPN multipoint dynamique à l'aide de GRE sur IPSec avec EIGRP, NAT et CBAC

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit un exemple de configuration pour le VPN DMVPN (Hub and Spoke Dynamic Multipoint VPN) utilisant l'encapsulation de routage générique (GRE) sur IPSec avec le protocole EIGRP (Enhanced Interior Gateway Routing Protocol), la traduction d'adresses réseau (NAT) et le contrôle d'accès basé sur le contexte (CBAC).

[Conditions préalables](#)

[Conditions requises](#)

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

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez [l'outil de recherche de commandes](#) (clients [inscrits](#) seulement).

[Components Used](#)

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 12.3(1.6) sur les routeurs en étoile
- Cisco 3620 comme routeur concentrateur, deux routeurs Cisco 1720 et un routeur Cisco 3620 comme routeur en étoile

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

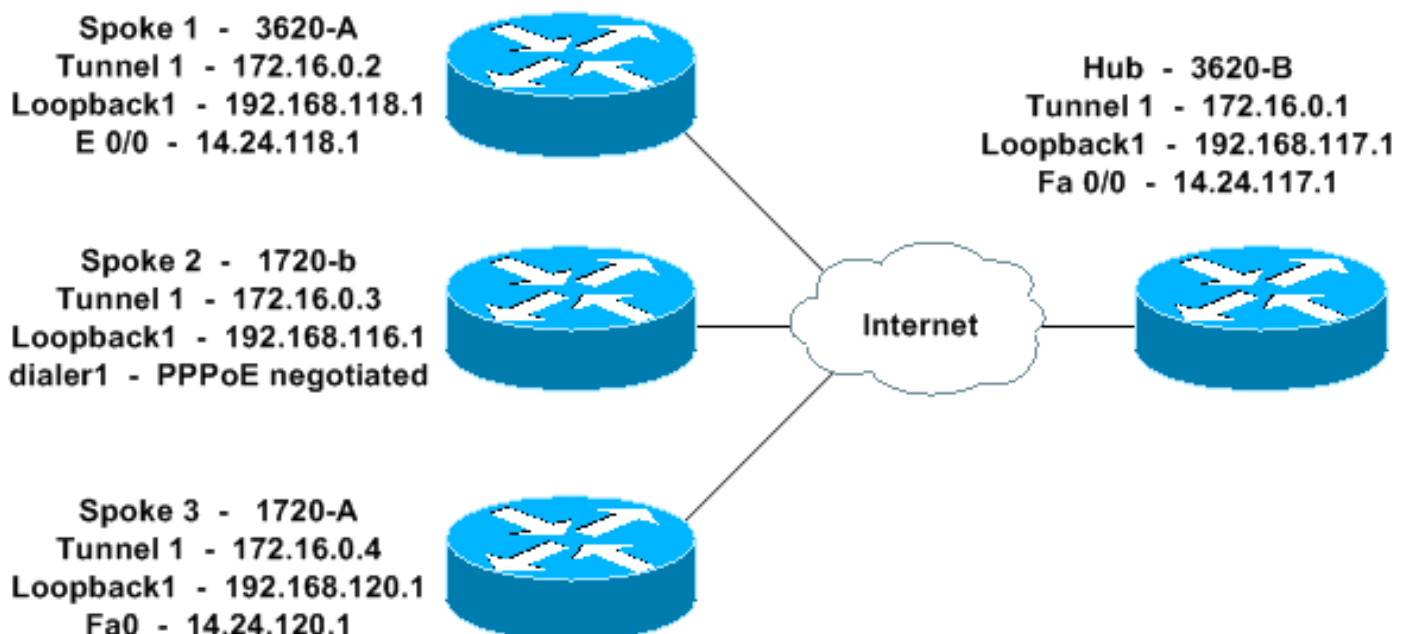
Configuration

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

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez [l'outil de recherche de commandes](#) (clients [inscrits](#) seulement).

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :



Configurations

Ce document utilise les configurations présentées ci-dessous.

- [Concentrateur - 3620-B](#)
- [Spoke 1 - 3620-A](#)

- [Spoke 2 - 1720-b](#)
- [Spoke 3 - 1720-A](#)

Concentrateur - 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 Tunnell
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 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#

```

Vérification

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre

configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show crypto isakmp sa** : affiche l'état de l'association de sécurité ISAKMP (SA).
- **show crypto engine connections active** : affiche le nombre total de chiffrement/déchiffrement par SA.
- **show crypto ipsec sa** : affiche les statistiques sur les tunnels actifs.
- **show ip route** : affiche la table de routage.
- **show ip eigrp neighbor** : affiche les voisins EIGRP.
- **show ip nhrp** - Affiche le cache NHRP (Next Hop Resolution Protocol) IP, éventuellement limité aux entrées de cache dynamique ou statique pour une interface spécifique.
- **show crypto socket** : affiche la table de socket de chiffrement entre NHRP et IPsec.

Dépannage

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

Dépannage des commandes

Note : Avant d'émettre des commandes **debug**, consultez [Informations importantes sur les 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.
- **debug crypto socket** - Affiche des informations sur la table de socket entre NHRP et IPsec.
- **debug nhrp** - Affiche des informations sur les événements NHRP.
- **debug nhrp packet** : affiche des informations sur les paquets NHRP.
- **debug tunnel protection** : affiche des informations sur les tunnels GRE dynamiques.

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

Informations connexes

- [Présentation de DMVPN et de Cisco IOS](#)
- [Page d'assistance IPsec](#)
- [Support et documentation techniques - Cisco Systems](#)