

Exemple de configuration DMVPN et Easy VPN Server avec les profils ISAKMP

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifier](#)

[Dépanner](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit comment configurer le VPN multipoint dynamique (DMVPN) et l'Easy VPN avec Xauth sur le même routeur. Cette installation s'assure que les DMVPN en étoile sont adressés dynamiquement. Les profils Internet Security Association and Key Management Protocol (ISAKMP) permettent de séparer les méthodes d'authentification des DMVPN en étoile ou des clients Easy VPN adressés dynamiquement.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

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

- Routeurs de Cisco 2691 et 3725 qui exécutent des versions de logiciel 12.3(3) et 12.3(3)a de Cisco IOS®

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

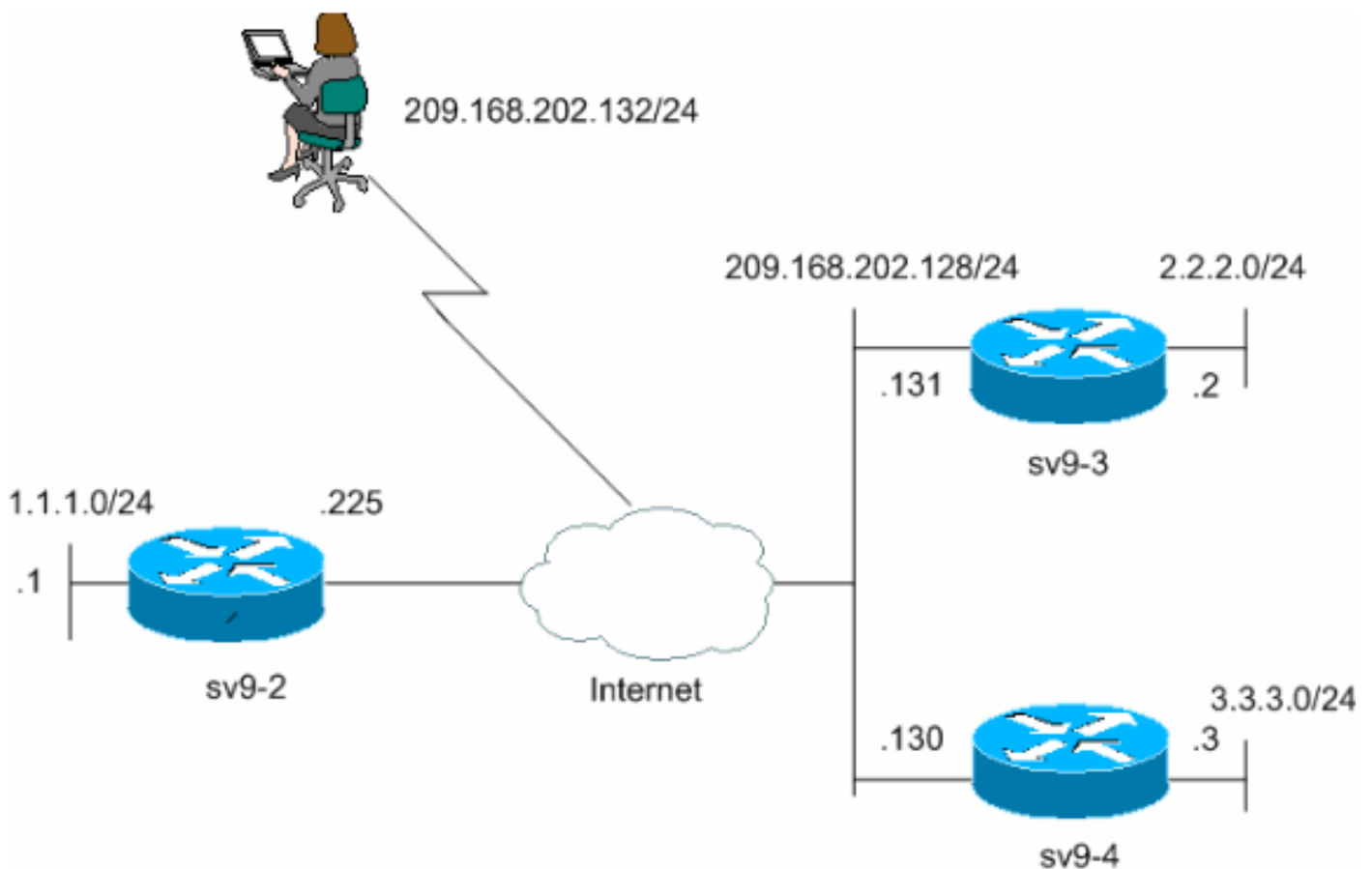
Configurer

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

Remarque: Utilisez l'outil [Command Lookup Tool](#) (clients [enregistrés](#) seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Diagramme du réseau

Ce document utilise cette configuration du réseau.



Configurations

Ce document utilise les configurations suivantes.

- [configuration du hub sv9-2](#)
- [configuration en étoile sv9-3](#)
- [configuration en étoile sv9-4](#)

configuration du hub sv9-2

```
sv9-2#show run
Building configuration...

Current configuration : 2876 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sv9-2
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
username cisco password 0 cisco
aaa new-model
!
!
!--- Xauth is configured for local authentication. aaa
authentication login userauthen local
aaa authorization network hw-client-groupname local
aaa session-id common
ip subnet-zero
!
!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!
!--- Keyring that defines the wildcard pre-shared key.
crypto keyring dmvpnsokes
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!

!--- Create an ISAKMP policy for Phase 1 negotiations.
!--- This policy is for DMVPN spokes. crypto isakmp
policy 10
hash md5
authentication pre-share
!

!--- Create an ISAKMP policy for Phase 1 negotiations.
!--- This policy is for Easy VPN Clients. crypto isakmp
policy 20
hash md5
authentication pre-share
group 2
!

!--- VPN Client configuration for group "hw-client-
groupname" !--- (this name is configured in the VPN
```

```
Client). crypto isakmp client configuration group hw-
client-groupname
key hw-client-password
dns 1.1.11.10 1.1.11.11
wins 1.1.11.12 1.1.11.13
domain cisco.com
pool dynpool

!--- Profile for VPN Client connections, matches the !--
- "hw-client-group" group and defines the XAuth
properties. crypto isakmp profile VPNclient
match identity group hw-client-groupname
client authentication list userauthen
isakmp authorization list hw-client-groupname
client configuration address respond

!--- Profile for LAN-to-LAN connection, references !---
the wildcard pre-shared key and a wildcard !--- identity
(this is what is broken in !--- Cisco bug ID CSCea77140)
!--- and no XAuth. crypto isakmp profile DMVPN
keyring dmvpnsokes
match identity address 0.0.0.0
!
!

!--- Create the Phase 2 policy for actual data
encryption. crypto ipsec transform-set strong esp-3des
esp-md5-hmac
mode transport
!

!--- Create an IPsec profile to be applied dynamically
to the !--- generic routing encapsulation (GRE) over
IPsec tunnels. crypto ipsec profile cisco
set security-association lifetime seconds 120
set transform-set strong
set isakmp-profile DMVPN
!
!

!--- This dynamic crypto map references the ISAKMP !---
Profile VPN Client above. !--- Reverse route injection
is used to provide the !--- DMVPN networks access to any
Easy VPN Client networks. crypto dynamic-map dynmap 10
set isakmp-profile VPNclient
reverse-route
set transform-set strong
!
!

!--- Crypto map only references the dynamic crypto map
above. crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
!
!
!
!
!
!
!
!
```

```
no voice hpi capture buffer
no voice hpi capture destination
!
!
!
!
!
!
!
!--- Create a GRE tunnel template which is applied to !-
-- all the dynamically created GRE tunnels. interface
Tunnel0
ip address 192.168.1.1 255.255.255.0
no ip redirects
ip mtu 1440
ip nhrp authentication cisco123
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp holdtime 300
no ip split-horizon eigrp 90
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile cisco
!
interface FastEthernet0/0
ip address 209.168.202.225 255.255.255.0
duplex auto
speed auto
crypto map dynmap
!
interface FastEthernet0/1
ip address 1.1.1.1 255.255.255.0
duplex auto
speed auto
!
interface BRI1/0
no ip address
shutdown
!
interface BRI1/1
no ip address
shutdown
!
interface BRI1/2
no ip address
shutdown
!
interface BRI1/3
no ip address
shutdown
!
!--- Enable a routing protocol to send and receive !--
dynamic updates about the private networks. router eigrp
90
redistribute static
network 1.1.1.0 0.0.0.255
network 192.168.1.0
no auto-summary
!
ip local pool dynpool 1.1.11.60 1.1.11.80
ip http server
no ip http secure-server
```

```
ip classless
!
!
!
!
!
!
!
!
!
!
!
line con 0
exec-timeout 0 0
transport preferred all
transport output all
escape-character 27
line aux 0
transport preferred all
transport output all
line vty 0 4
password cisco
transport preferred all
transport input all
transport output all
!
!
end
```

configuration en étoile sv9-3

```
sv9-3#show run
Building configuration...

Current configuration : 2052 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sv9-3
!
boot-start-marker
boot system flash:c3725-ik9o3s-mz.123-3.bin
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!
!--- Create an ISAKMP policy for Phase 1 negotiations.
crypto isakmp policy 10
```

```
hash md5
authentication pre-share
!--- Add dynamic pre-shared keys for all remote VPN
routers. crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0
!
!
!--- Create the Phase 2 policy for actual data
encryption. crypto ipsec transform-set strong esp-3des
esp-md5-hmac
mode transport
!
!--- Create an IPsec profile to be applied dynamically
to the !--- GRE over IPsec tunnels. crypto ipsec profile
cisco
set security-association lifetime seconds 120
set transform-set strong
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
!--- Create a GRE tunnel template which is applied to !-
-- all the dynamically created GRE tunnels. interface
Tunnel0
ip address 192.168.1.3 255.255.255.0
no ip redirects
ip mtu 1440
ip nhrp authentication cisco123
ip nhrp map multicast dynamic
ip nhrp map 192.168.1.1 209.168.202.225
ip nhrp map multicast 209.168.202.225
ip nhrp network-id 1
ip nhrp holdtime 300
ip nhrp nhs 192.168.1.1
no ip split-horizon eigrp 90
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile cisco
!
interface FastEthernet0/0
ip address 209.168.202.130 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 3.3.3.3 255.255.255.0
duplex auto
speed auto
!
interface BRI1/0
no ip address
shutdown
!
interface BRI1/1
no ip address
shutdown
!
interface BRI1/2
no ip address
shutdown
!
```

```
interface BRI1/3
no ip address
shutdown
!
!--- Enable a routing protocol to send and receive !---
dynamic updates about the private networks. router eigrp
90
network 3.3.3.0 0.0.0.255
network 192.168.1.0
no auto-summary
!
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 209.168.202.225
ip route 2.2.2.0 255.255.255.0 Tunnel0
!
!
line con 0
exec-timeout 0 0
transport preferred all
transport output all
escape-character 27
line aux 0
transport preferred all
transport output all
line vty 0 4
login
transport preferred all
transport input all
transport output all
!
!
end
```

configuration en étoile sv9-4

```
sv9-4#show run
Building configuration...

Current configuration : 1992 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname sv9-4
!
boot-start-marker
boot system flash:c2691-jk9o3s-mz.123-3a.bin
boot-end-marker
!
enable password cisco
!
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
```



```
ip ssh break-string
no ftp-server write-enable
!
!
!
!--- Create an ISAKMP policy for Phase 1 negotiations.
crypto isakmp policy 10
hash md5
authentication pre-share
!--- Add dynamic pre-shared keys for all remote VPN
routers. crypto isakmp key cisco123 address 0.0.0.0
0.0.0.0
!
!
!--- Create the Phase 2 policy for actual data
encryption. crypto ipsec transform-set strong esp-3des
esp-md5-hmac
mode transport
!
!--- Create an IPsec profile apply dynamically to the !-
-- GRE over IPsec tunnels. crypto ipsec profile cisco
set security-association lifetime seconds 120
set transform-set strong
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
!--- Create a GRE tunnel template which is applied to !-
-- all the dynamically created GRE tunnels. interface
Tunnel0
ip address 192.168.1.2 255.255.255.0
no ip redirects
ip mtu 1440
ip nhrp authentication cisco123
ip nhrp map multicast dynamic
ip nhrp map 192.168.1.1 209.168.202.225
ip nhrp map multicast 209.168.202.225
ip nhrp network-id 1
ip nhrp holdtime 300
ip nhrp nhs 192.168.1.1
no ip split-horizon eigrp 90
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel key 0
tunnel protection ipsec profile cisco
!
interface FastEthernet0/0
ip address 209.168.202.131 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 2.2.2.2 255.255.255.0
duplex auto
speed auto
!
!--- Enable a routing protocol to send and receive !---
dynamic updates about the private networks. router eigrp
90
network 2.2.2.0 0.0.0.255
network 192.168.1.0
no auto-summary
```

```
!  
ip http server  
no ip http secure-server  
ip classless  
ip route 0.0.0.0 0.0.0.0 209.168.202.225  
!  
!  
dial-peer cor custom  
!  
!  
line con 0  
exec-timeout 0 0  
transport output lat pad v120 lapb-ta mop telnet rlogin  
udptn ssh  
escape-character 27  
line aux 0  
transport output lat pad v120 lapb-ta mop telnet rlogin  
udptn ssh  
line vty 0 4  
login  
transport input lat pad v120 lapb-ta mop telnet rlogin  
udptn ssh  
transport output lat pad v120 lapb-ta mop telnet rlogin  
udptn ssh  
!  
!  
end
```

Vérifier

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

Les commandes de debug qui fonctionnent sur le routeur concentrateur confirment que les paramètres corrects sont appariés pour le rai et les connexions client VPN. Exécutez ces commandes de **débogage**.

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**.

Remarque: Référez-vous aux [informations importantes sur les commandes de débogage](#) avant d'utiliser les commandes de **débogage**.

- **debug crypto isakmp**—Affichage de messages d'événements IKE.
- **debug crypto ipsec** — Affiche des informations au sujet des événements d'IPsec.

```
sv9-4#show run
```

```
Building configuration...
```

```
Current configuration : 1992 bytes
```

```
!  
version 12.3  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname sv9-4
```

```
!  
boot-start-marker  
boot system flash:c2691-jk9o3s-mz.123-3a.bin  
boot-end-marker  
!  
enable password cisco  
!  
no aaa new-model  
ip subnet-zero  
!  
!  
no ip domain lookup  
!  
ip audit notify log  
ip audit po max-events 100  
ip ssh break-string  
no ftp-server write-enable  
!  
!  
!  
!--- Create an ISAKMP policy for Phase 1 negotiations. crypto isakmp policy 10  
hash md5  
authentication pre-share  
!--- Add dynamic pre-shared keys for all remote VPN routers. crypto isakmp key cisco123 address  
0.0.0.0 0.0.0.0  
!  
!  
!--- Create the Phase 2 policy for actual data encryption. crypto ipsec transform-set strong  
esp-3des esp-md5-hmac  
mode transport  
!  
!--- Create an IPsec profile apply dynamically to the !--- GRE over IPsec tunnels. crypto ipsec  
profile cisco  
set security-association lifetime seconds 120  
set transform-set strong  
!  
!  
no voice hpi capture buffer  
no voice hpi capture destination  
!  
!  
!--- Create a GRE tunnel template which is applied to !--- all the dynamically created GRE  
tunnels. interface Tunnel0  
interface Tunnel0  
ip address 192.168.1.2 255.255.255.0  
no ip redirects  
ip mtu 1440  
ip nhrp authentication cisco123  
ip nhrp map multicast dynamic  
ip nhrp map 192.168.1.1 209.168.202.225  
ip nhrp map multicast 209.168.202.225  
ip nhrp network-id 1  
ip nhrp holdtime 300  
ip nhrp nhs 192.168.1.1  
no ip split-horizon eigrp 90  
tunnel source FastEthernet0/0  
tunnel mode gre multipoint  
tunnel key 0  
tunnel protection ipsec profile cisco  
!  
interface FastEthernet0/0  
ip address 209.168.202.131 255.255.255.0  
duplex auto  
speed auto  
!
```

```
interface FastEthernet0/1
ip address 2.2.2.2 255.255.255.0
duplex auto
speed auto
!
!--- Enable a routing protocol to send and receive !--- dynamic updates about the private
networks. router eigrp 90
network 2.2.2.0 0.0.0.255
network 192.168.1.0
no auto-summary
!
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 209.168.202.225
!
!
dial-peer cor custom
!
!
line con 0
exec-timeout 0 0
transport output lat pad v120 lapb-ta mop telnet rlogin udptn ssh
escape-character 27
line aux 0
transport output lat pad v120 lapb-ta mop telnet rlogin udptn ssh
line vty 0 4
login
transport input lat pad v120 lapb-ta mop telnet rlogin udptn ssh
transport output lat pad v120 lapb-ta mop telnet rlogin udptn ssh
!
!
end
```

Dépanner

Référez-vous au [dépannage de sécurité IP - Comprenant et utilisant des commandes de débogage](#) pour l'information de dépannage supplémentaire.

Informations connexes

- [Aperçu de logiciel DMVPN et de Cisco IOS](#)
- [Négociation IPSec/Protocoles IKE](#)
- [Support et documentation techniques - Cisco Systems](#)