

Configuration d'IPSec entre trois routeurs à l'aide d'adresses privées

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifiez](#)

[Dépannez](#)

[Dépannage des commandes](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit une configuration entièrement engrenée avec trois Routeurs qui utilisent des adresses privées. L'exemple montre ces caractéristiques :

- Protocole ESP (Encapsulating Security Payload) - Norme de chiffrement de données (DES) seulement
- Clés pré-partagées
- Réseaux privés derrière chaque routeur : 192.168.1.0, 192.168.2.0, et 192.168.3.0
- stratégie d'ISAKMP et configuration de crypto map
- Le trafic du tunnel défini avec les commandes de **liste d'accès** et de **route-map**. En plus de la traduction d'adresses de port (TAPOTEMENT), des mappages de route peuvent être appliqués à une traduction d'adresses de réseau statique linéaire (NAT) sur la version de logiciel 12.2(4)T2 et ultérieures de Cisco IOS®. Le pour en savoir plus se rapportent à [NAT - Capacité d'utiliser des mappages de route avec la vue d'ensemble des fonctionnalités statique de traductions](#).

Remarque: La technologie de cryptage est sujette à des contrôles d'exportation. Il est de votre responsabilité de connaître la loi concernant l'exportation de la technologie de cryptage. Si vous avez n'importe quelles questions concernant le contrôle d'exportation, envoyez s'il vous plaît un email à export@cisco.com.

[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 :

- Version du logiciel Cisco IOS 12.3.(7)T.
- Routeurs de Cisco configurés avec IPSec.

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 aux [Conventions relatives aux conseils techniques Cisco](#).

Configurez

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

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'[Outil de recherche de commande](#) ([clients enregistrés](#) seulement).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configurations

Ce document utilise les configurations suivantes :

- [Routeur 1](#)
- [Routeur 2](#)
- [Routeur 3](#)

Routeur 1
Current configuration: ! version 12.3 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname router1

```

!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!

!--- Configure Internet Key Exchange (IKE) policy and !-
-- pre-shared keys for each peer. !--- IKE policy
defined for peers. crypto isakmp policy 4 authentication
pre-share !--- Pre-shared keys for different peers.
crypto isakmp key xxxxxx1234 address 100.228.202.154
crypto isakmp key xxxxxx1234 address 200.154.17.130 !!
!--- IPsec policies: crypto ipsec transform-set encrypt-
des esp-des !! crypto map combined local-address
Serial0 !--- Set the peer, transform-set and encryption
traffic for tunnel peers. crypto map combined 20 ipsec-
isakmp set peer 100.228.202.154 set transform-set
encrypt-des match address 106 crypto map combined 30
ipsec-isakmp set peer 200.154.17.130 set transform-set
encrypt-des match address 105 !! interface Serial0 ip
address 100.232.202.210 255.255.255.252 ip nat outside
serial restart-delay 0 !--- Apply the crypto map to the
interface. crypto map combined ! interface FastEthernet0
ip address 192.168.1.1 255.255.255.0 ip nat inside ! ip
classless ip route 0.0.0.0 0.0.0.0 100.232.202.209 no ip
http server no ip http secure-server ! !--- Define
traffic for NAT. ip nat inside source route-map nonat
interface Serial0 overload !--- Access control list
(ACL) that shows traffic to encrypt over the tunnel.
access-list 105 permit ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255 access-list 106 permit ip
192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 !--- ACL to
avoid the traffic through NAT over the tunnel. access-
list 150 deny ip 192.168.1.0 0.0.0.255 192.168.2.0
0.0.0.255 access-list 150 deny ip 192.168.1.0 0.0.0.255
192.168.3.0 0.0.0.255 !--- ACL to perform NAT on the
traffic that does not go over the tunnel. access-list
150 permit ip 192.168.1.0 0.0.0.255 any !--- Do not
perform NAT on the IPsec traffic. route-map nonat permit
10 match ip address 150 ! control-plane !! line con 0
line aux 0 line vty 0 4 !! end

```

Routeur 2

Current configuration:

```

!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router2
!
boot-start-marker
boot-end-marker
!
!

```

```

clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100
no ftp-server write-enable
!
.
!--- Configure IKE policy and pre-shared keys for each
peer. !--- IKE policy defined for peers. crypto isakmp
policy 4 authentication pre-share !--- Pre-shared keys
for different peers. crypto isakmp key xxxxxx1234
address 100.228.202.154 crypto isakmp key xxxxxx1234
address 100.232.202.210 !! !--- IPsec policies. crypto
ipsec transform-set encrypt-des esp-des !! crypto map
combined local-address Ethernet1 !--- Set the peer,
transform-set and encryption traffic for tunnel peers.
crypto map combined 7 ipsec-isakmp set peer
100.232.202.210 set transform-set encrypt-des match
address 105 crypto map combined 8 ipsec-isakmp set peer
100.228.202.154 set transform-set encrypt-des match
address 106 !!! interface Ethernet0 ip address
192.168.3.1 255.255.255.0 ip nat inside ! interface
Ethernet1 ip address 200.154.17.130 255.255.255.224 ip
nat outside !--- Apply the crypto map to the interface.
crypto map combined ! ip classless ip route 0.0.0.0
0.0.0.0 200.154.17.129 no ip http server no ip http
secure-server !!--- Define traffic for NAT. ip nat
inside source route-map nonat interface Ethernet1
overload !--- ACL shows traffic to encrypt over the
tunnel. access-list 105 permit ip 192.168.3.0 0.0.0.255
192.168.1.0 0.0.0.255 access-list 106 permit ip
192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255 !--- ACL to
avoid the traffic through NAT over the tunnel. access-
list 150 deny ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255 access-list 150 deny ip 192.168.3.0 0.0.0.255
192.168.2.0 0.0.0.255 !--- ACL to perform NAT on the
traffic that does not go over the tunnel. access-list
150 permit ip any any !--- Do not perform NAT on the
IPsec traffic. route-map nonat permit 10 match ip
address 150 !!! control-plane !! line con 0 line aux
0 line vty 0 4 !! end

```

Routeur3 configuration

```

Current configuration:
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname router3
!
boot-start-marker
boot-end-marker
!
!
clock timezone EST 0
no aaa new-model
ip subnet-zero
!
!
ip audit po max-events 100

```

```

no ftp-server write-enable
!

!--- Configure IKE policy and pre-shared keys for each
peer. !--- IKE policy defined for peers. crypto isakmp
policy 4 authentication pre-share !--- Pre-shared keys
for different peers. crypto isakmp key xxxxxx1234
address 100.232.202.210 crypto isakmp key xxxxxx1234
address 200.154.17.130 ! ! !--- IPsec policies: crypto
ipsec transform-set encrypt-des esp-des ! ! !--- Set the
peer, transform-set and encryption traffic for tunnel
peers. crypto map combined local-address Serial0 crypto
map combined 7 ipsec-isakmp set peer 100.232.202.210 set
transform-set encrypt-des match address 106 crypto map
combined 8 ipsec-isakmp set peer 200.154.17.130 set
transform-set encrypt-des match address 105 ! !
interface Serial0 ip address 100.228.202.154
255.255.255.252 ip nat outside serial restart-delay 0 !-
-- Apply the crypto map to the interface. crypto map
combined ! interface FastEthernet0 ip address
192.168.2.1 255.255.255.0 ip nat inside ! ip classless
ip route 0.0.0.0 0.0.0.0 100.228.202.153 no ip http
server no ip http secure-server ! !--- Define traffic
for NAT. ip nat inside source route-map nonat interface
Serial0 overload !--- ACL that shows traffic to encrypt
over the tunnel. access-list 105 permit ip 192.168.2.0
0.0.0.255 192.168.3.0 0.0.0.255 access-list 106 permit
ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 !--- ACL
to avoid the traffic through NAT over the tunnel.
access-list 150 deny ip 192.168.2.0 0.0.0.255
192.168.3.0 0.0.0.255 access-list 150 deny ip
192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255 !--- ACL to
perform NAT on the traffic that does not go over the
tunnel. access-list 150 permit ip 192.168.2.0 0.0.0.255
any !--- Do not perform NAT on the IPsec traffic. route-
map nonat permit 10 match ip address 150 ! ! ! control-
plane ! ! line con 0 line aux 0 line vty 0 4 login ! !
end

```

Vérifiez

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.

- **active de connexions de show crypto engine** — Les expositions ont chiffré et ont déchiffré des paquets entre les pairs d'IPSec.
- **show crypto isakmp sa** — Affiche toutes les associations de sécurité en cours d'IKE (SAS) à un pair.
- **show crypto ipsec sa** — Affiche les configurations utilisées par le courant (IPSec) SAS.

Dépannez

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

Dépannage des commandes

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.

Remarque: Avant d'exécuter les commandes **debug**, référez-vous à la section **Informations importantes sur les commandes Debug**.

Remarque: Ce qui suit met au point doit s'exécuter sur les deux Routeurs d'IPSec (pairs). Effacer SAS doit être fait sur les deux pairs.

- **debug crypto isakmp** — Affiche des erreurs pendant le Phase 1.
- **debug crypto ipsec** — Affiche des erreurs pendant le Phase 2.
- **debug crypto engine** — Affiche des informations du moteur de chiffrement.
- **effacez le crypto connexion-id de connexion** [*emplacement* | *rsm* | *VIP*] — termine une session chiffrée en cours. Les sessions chiffrées se terminent normalement quand les temps de session. Utilisez l'**exposition que les cryptos connexions de Cisco** commandent d'apprendre la valeur de connexion-id.
- **clear crypto isakmp** — Efface le Phase 1 SAS.
- **clear crypto sa** — Efface le Phase 2 SAS.

Informations connexes

- [Page d'assistance IPsec](#)
- [Support technique - Cisco Systems](#)