

# Configuration d'IPSec en mode entièrement maillé entre deux routeurs

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifiez](#)

[Dépannez](#)

[Dépannage des commandes](#)

[Informations connexes](#)

## **Introduction**

Cette configuration d'échantillon affiche le cryptage plein-engrené entre trois Routeurs par l'utilisation d'un crypto map sur chaque routeur aux réseaux derrière chacun de ses deux pairs.

Le cryptage doit être fait de :

- réseau 160.160.160.x au réseau 170.170.170.x
- réseau 160.160.160.x au réseau 180.180.180.x
- réseau 170.170.170.x au réseau 180.180.180.x

## **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 :

- Versions de logiciel 12.2.7C et 12.2.8(T)4 de Cisco IOS®
- Cisco 2500 et 3600 Routeurs

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 de documents, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

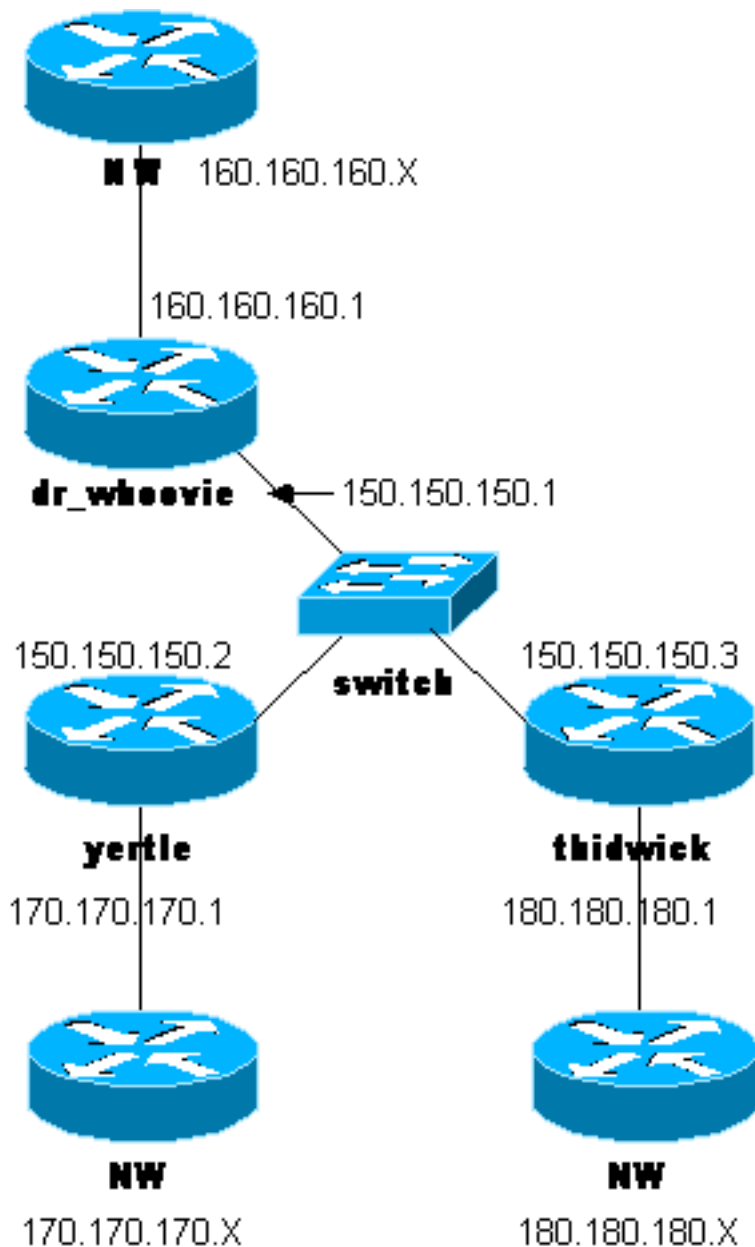
## [Configurez](#)

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

**Note:** 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 indiquée dans le diagramme suivant.



## Configurations

Ce document utilise les configurations suivantes.

- [Configuration de Dr\\_Whoovie](#)
- [Configuration de Yertle](#)
- [Configuration de Thidwick](#)

**Note:** Ces configurations ont été récemment testées avec le code en cours (novembre 2003) dans le document.

### Configuration de Dr\_Whoovie

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

```
hostname dr_whoovie
!
enable secret 5 $1$KxKv$cbqKsZtQTLJLGPn.tErFZ1
enable password ww
!
ip subnet-zero
!
cns event-service server
!
!--- Internet Key Exchange (IKE) Policies: crypto isakmp
policy 1
authentication pre-share
crypto isakmp key cisco123 address 150.150.150.3
crypto isakmp key cisco123 address 150.150.150.2
!
!--- IPSec Policies: crypto ipsec transform-set 170cisco
esp-des esp-md5-hmac
crypto ipsec transform-set 180cisco esp-des esp-md5-hmac
!
crypto map ETH0 17 ipsec-isakmp
set peer 150.150.150.2
set transform-set 170cisco
!--- Include the 160.160.160.x to 170.170.170.x network
!--- in the encryption process. match address 170
crypto map ETH0 18 ipsec-isakmp
set peer 150.150.150.3
set transform-set 180cisco
!--- Include the 160.160.160.x to 180.180.180.x network
!--- in the encryption process. match address 180
!
interface Ethernet0
ip address 150.150.150.1 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no mop enabled
crypto map ETH0
!
interface Ethernet1
no ip address
no ip directed-broadcast
shutdown
!
interface Serial0
ip address 160.160.160.1 255.255.255.0
no ip directed-broadcast
no ip mroute-cache
no fair-queue
!
interface Serial1
no ip address
no ip directed-broadcast
clockrate 4000000
!
ip classless
ip route 170.170.170.0 255.255.255.0 150.150.150.2
ip route 180.180.180.0 255.255.255.0 150.150.150.3
no ip http server
!
!--- Include the 160.160.160.x to 170.170.170.x network
!--- in the encryption process. access-list 170 permit
ip 160.160.160.0 0.0.0.255 170.170.170.0 0.0.0.255
!--- Include the 160.160.160.x to 180.180.180.x network
!--- in the encryption process. access-list 180 permit
```

```
ip 160.160.160.0 0.0.0.255 180.180.180.0 0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

## Configuration de Yertle

```
Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname yertle
!
enable secret 5 $1$me5Q$2kF5zKlPPTvHEBdGiEZ9m/
enable password ww
!
ip subnet-zero
!
cns event-service server
!
!--- IKE Policies: crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco123 address 150.150.150.3
crypto isakmp key cisco123 address 150.150.150.1
!
!--- IPSec Policies: crypto ipsec transform-set 160cisco
esp-des esp-md5-hmac
crypto ipsec transform-set 180cisco esp-des esp-md5-hmac
!
crypto map ETH0 16 ipsec-isakmp
set peer 150.150.150.1
set transform-set 160cisco
!--- Include the 170.170.170.x to 160.160.160.x network
!--- in the encryption process. match address 160
crypto map ETH0 18 ipsec-isakmp
set peer 150.150.150.3
set transform-set 180cisco
!--- Include the 170.170.170.x to 180.180.180.x network
!--- in the encryption process. match address 180
!
interface Ethernet0
ip address 150.150.150.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no mop enabled
crypto map ETH0
!
interface Serial0
no ip address
no ip directed-broadcast
no ip mroute-cache
```

```

shutdown
no fair-queue
!
interface Serial1
ip address 170.170.170.1 255.255.255.0
no ip directed-broadcast
!
ip classless
ip route 160.160.160.0 255.255.255.0 150.150.150.1
ip route 180.180.180.0 255.255.255.0 150.150.150.3
no ip http server
!
!--- Include the 170.170.170.x to 160.160.160.x network
!--- in the encryption process. access-list 160 permit
ip 170.170.170.0 0.0.0.255 160.160.160.0 0.0.0.255
!--- Include the 170.170.170.x to 180.180.180.x network
!--- in the encryption process. access-list 180 permit
ip 170.170.170.0 0.0.0.255 180.180.180.0 0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end

```

## Configuration de Thidwick

```

Current configuration:
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname thidwick
!
enable secret 5 $l$Pcpo$fj4FNS1dEDY9lGg3Ne6FK1
enable password ww
!
ip subnet-zero
!
isdn switch-type basic-5ess
isdn voice-call-failure 0
cns event-service server
!
!--- IKE Policies: crypto isakmp policy 1
authentication pre-share
crypto isakmp key cisco123 address 150.150.150.1
crypto isakmp key cisco123 address 150.150.150.2
!
!--- IPSec Policies: crypto ipsec transform-set 160cisco
esp-des esp-md5-hmac
crypto ipsec transform-set 170cisco esp-des esp-md5-hmac
!
crypto map ETH0 16 ipsec-isakmp
set peer 150.150.150.1
set transform-set 160cisco
!--- Include the 180.180.180.x to 160.160.160.x network

```

```

!--- in the encryption process. match address 160
crypto map ETH0 17 ipsec-isakmp
set peer 150.150.150.2
set transform-set 170cisco
!--- Include the 180.180.180.x to 170.170.170.x network
!--- in the encryption process. match address 170
!
interface Ethernet0
ip address 150.150.150.3 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no mop enabled
crypto map ETH0
!
interface Serial0
no ip address
no ip directed-broadcast
no ip mroute-cache
no fair-queue
clockrate 4000000
!
interface Serial1
ip address 180.180.180.1 255.255.255.0
no ip directed-broadcast
clockrate 4000000
!
interface BRI0
no ip address
no ip directed-broadcast
shutdown
isdn switch-type basic-5ess
!
ip classless
ip route 160.160.160.0 255.255.255.0 150.150.150.1
ip route 170.170.170.0 255.255.255.0 150.150.150.2
no ip http server
!
!--- Include the 180.180.180.x to 160.160.160.x network
!--- in the encryption process. access-list 160 permit
ip 180.180.180.0 0.0.0.255 160.160.160.0 0.0.0.255
!--- Include the 180.180.180.x to 170.170.170.x network
!--- in the encryption process. access-list 170 permit
ip 180.180.180.0 0.0.0.255 170.170.170.0 0.0.0.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
!
line con 0
transport input none
line aux 0
line vty 0 4
password ww
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.

- **show crypto ipsec sa** — Affiche les configurations utilisées par [les associations de sécurité en cours d'IPSec].
- **show crypto isakmp sa** — Affiche toutes les associations de sécurité en cours d'IKE à un pair.

## [Dépannez](#)

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

### [Dépannage des commandes](#)

**Note:** Avant d'émettre des commandes de **débogage**, référez-vous aux [informations importantes sur des commandes de debug](#).

- **debug crypto ipsec** — Affiche les négociations IPsec de la phase 2.
- **debug crypto isakmp** — Affiche les négociations de Protocole ISAKMP (Internet Security Association and Key Management Protocol) de la phase 1.
- **debug crypto engine** — Affiche le trafic qui est chiffré.
- **clear crypto isakmp** — Autorise les associations de sécurité liées à la phase 1.
- **clear crypto sa** — Autorise les associations de sécurité liées à la phase 2.

## [Informations connexes](#)

- [Page d'assistance IPsec](#)
- [Sécurité des réseaux de configuration d'IPSec](#)
- [Configurer le protocole de sécurité IKE](#)
- [Support technique - Cisco Systems](#)