

# Configuration d'IPSec de routeur à routeur, avec clés partagées et surcharge NAT, entre des réseaux privés

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Informations connexes](#)

## Introduction

Cet exemple de configuration montre comment chiffrer le trafic entre deux réseaux privés (10.50.50.x et 10.103.1.x) à l'aide d'IPSec. Les réseaux se reconnaissent à l'aide de leurs adresses privées.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Components Used

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

- Logiciel Cisco IOS® Version 12.3.1a
- Routeurs Cisco 2691

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 des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

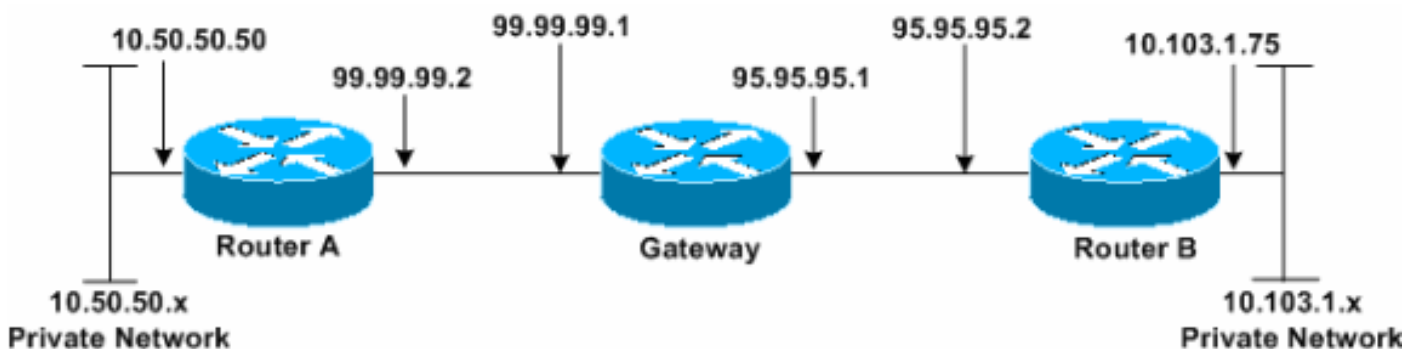
## Configuration

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 suivantes.

- [Router A](#)
- [Router B](#)

### Router A

```
Router_A#write terminal
Building configuration...
Current configuration : 1638 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router_A
!
boot system flash:c2691-ik9o3s-mz.123-1a.bin
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
```

```
no ftp-server write-enable
!
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 95.95.95.2
!
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
!
crypto map rtp 1 ipsec-isakmp
set peer 95.95.95.2
set transform-set rtpset
!--- Include the private network to private network
traffic !--- in the encryption process. match address
115
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface FastEthernet0/0
ip address 99.99.99.2 255.255.255.0
ip nat outside
duplex auto
speed auto
crypto map rtp
!
interface FastEthernet0/1
ip address 10.50.50.50 255.255.255.0
ip nat inside
duplex auto
speed auto
!
!--- Except the private network traffic from the !---
Network Address Translation (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 99.99.99.1
!
!--- Except the private network traffic from the NAT
process. access-list 110 deny ip 10.50.50.0 0.0.0.255
10.103.1.0 0.0.0.255
access-list 110 permit ip 10.50.50.0 0.0.0.255 any
!--- Include the private network to private network
traffic !--- in the encryption process. access-list 115
permit ip 10.50.50.0 0.0.0.255 10.103.1.0 0.0.0.255
!
!--- Except the private network traffic from the NAT
process. route-map nonat permit 10
match ip address 110
!
dial-peer cor custom
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
end

Router_A#
```

## Router B

```
Router_B#write terminal
Building configuration...
Current configuration : 1394 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router_B
!
boot system flash:c2691-ik9o3s-mz.123-1a.bin
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
no ftp-server write-enable
!
crypto isakmp policy 1
hash md5
authentication pre-share
crypto isakmp key cisco123 address 99.99.99.2
!
crypto ipsec transform-set rtpset esp-des esp-md5-hmac
!
crypto map rtp 1 ipsec-isakmp
set peer 99.99.99.2
set transform-set rtpset
!--- Include the private network to private network
traffic !--- in the encryption process. match address
115
!
no voice hpi capture buffer
no voice hpi capture destination
!
interface FastEthernet0/0
ip address 95.95.95.2 255.255.255.0
ip nat outside
duplex auto
speed auto
crypto map rtp
!
interface FastEthernet0/1
ip address 10.103.1.75 255.255.255.0
ip nat inside
duplex auto
speed auto
!
!--- 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 95.95.95.1
!
!--- Except the private network traffic from the NAT
process. access-list 110 deny ip 10.103.1.0 0.0.0.255
10.50.50.0 0.0.0.255
access-list 110 permit ip 10.103.1.0 0.0.0.255 any
```

```
!--- Include the private network to private network
traffic !--- in the encryption process. access-list 115
permit ip 10.103.1.0 0.0.0.255 10.50.50.0 0.0.0.255
!
!--- Except the private network traffic from the NAT
process. route-map nonat permit 10
match ip address 110
!
dial-peer cor custom
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
login
!
end
Router_B#
```

## Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

## Dépannage

### 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'émettre des commandes **debug**, reportez-vous à [Informations importantes sur les commandes de débogage](#).

- **debug crypto ipsec sa** - Affiche les négociations IPSec de la phase 2.
- **debug crypto isakmp sa** - Affiche les négociations ISAKMP (Internet Security Association and Key Management Protocol) de la phase 1.
- **debug crypto engine** : affiche les sessions chiffrées.

## Informations connexes

- [Dépannage de sécurité IP - Comprendre et utiliser les commandes de dépannage](#)
- [Page d'assistance IPsec](#)
- [Support technique - Cisco Systems](#)