

Configuration d'un tunnel IPSec entre routeurs avec sous-réseaux LAN en double

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifiez](#)

[Dépannez](#)

[Dépannage des commandes](#)

[Informations connexes](#)

[Introduction](#)

Ce document donne un exemple de gestion de réseau qui simule le fusionnement de deux sociétés avec le même schéma d'adressage IP. Deux routeurs sont connectés à un tunnel VPN, et les réseaux derrière chaque routeur sont identiques. Pour qu'un site accède à des hôtes de l'autre site, la Traduction d'adresses de réseau (NAT) est utilisée sur les routeurs pour changer les adresses de la source et de la destination selon les différents sous-réseaux.

Note: Cette configuration n'est pas recommandée comme installation permanente parce qu'elle serait embrouillante d'un point de vue de Gestion de réseau.

[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 :

- Routeur A : Version de logiciel 12.3(4)T courante de Cisco IOS® de routeur de Cisco 3640

- Routeur B : Version de logiciel 12.3(5) courante de Cisco IOS® de routeur de Cisco 2621

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](#).

[Informations générales](#)

Dans cet exemple, quand l'hôte 172.16.1.2 au site A accède à la même chose hôte IP-adressé au site B, il connecte à 172.19.1.2 une adresse plutôt qu'à l'adresse réelle de 172.16.1.2. Quand l'hôte au site B aux accès situent A, il connecte à 172.18.1.2 une adresse. NAT sur le routeur A traduit n'importe quelle adresse 172.16.x.x pour ressembler à l'entrée de hôte 172.18.x.x assortie. NAT sur le routeur B change 172.16.x.x pour ressembler à 172.19.x.x.

La crypto fonction sur chaque routeur chiffre le trafic traduit à travers les interfaces série. Notez que NAT se produit *avant* cryptage sur un routeur.

Note: Cette configuration permet seulement aux deux réseaux pour communiquer. Il ne tient pas compte de la connexion Internet. Vous avez besoin de chemins supplémentaires à l'Internet pour la Connectivité aux emplacements autres que les deux sites ; en d'autres termes, vous devez ajouter un routeur ou un Pare-feu différent de chaque côté, avec de plusieurs artères configurées sur les hôtes.

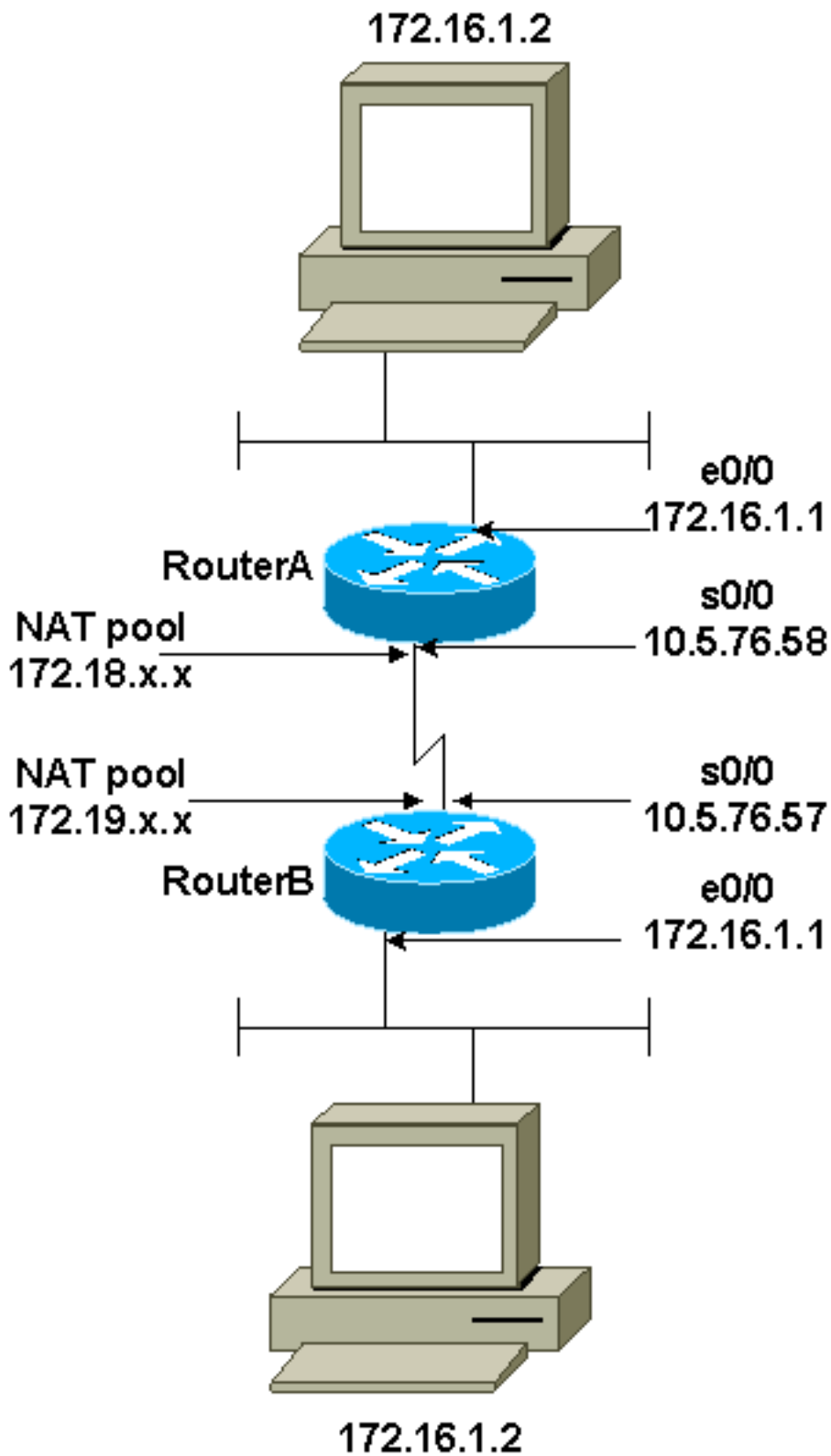
[Configurez](#)

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 suivante :



Configurations

Ce document utilise les configurations suivantes :

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

routeur A

```
Current configuration : 1404 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!
!--- These are the Internet Key Exchange (IKE)
parameters. crypto isakmp policy 10
  encr 3des
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 10.5.76.57
!
!--- These are the IPSec parameters. crypto ipsec
transform-set myset1 esp-3des esp-md5-hmac
!
!
crypto map mymap 10 ipsec-isakmp
  set peer 10.5.76.57
  set transform-set myset1
  !--- Encrypt traffic to the other side. match address
100
!
!
!
interface Serial0/0
  description Interface to Internet
  ip address 10.5.76.58 255.255.0.0
  ip nat outside
  clockrate 128000
  crypto map mymap
!
interface Ethernet0/0
  ip address 172.16.1.1 255.255.255.0
  no ip directed-broadcast
  ip nat inside
  half-duplex
!
!
!--- This is the NAT traffic. ip nat inside source
static network 172.16.0.0 172.18.0.0 /16 no-alias
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
```

```
!  
!--- Encrypt traffic to the other side. access-list 100  
permit ip 172.18.0.0 0.0.255.255 172.19.0.0 0.0.255.255  
!  
control-plane  
!  
!  
line con 0  
line aux 0  
line vty 0 4  
!  
!  
end
```

routeur B

```
Current configuration : 1255 bytes  
!  
version 12.3  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname SV3-15  
!  
boot-start-marker  
boot-end-marker  
!  
!  
memory-size iomem 15  
no aaa new-model  
ip subnet-zero  
!  
!  
!  
ip audit notify log  
ip audit po max-events 100  
!  
!--- These are the IKE parameters. crypto isakmp policy  
10  
  encr 3des  
  hash md5  
  authentication pre-share  
crypto isakmp key cisco123 address 10.5.76.58  
!  
!--- These are the IPSec parameters. crypto ipsec  
transform-set myset1 esp-3des esp-md5-hmac  
!  
crypto map mymap 10 ipsec-isakmp  
  set peer 10.5.76.58  
  set transform-set myset1  
!--- Encrypt traffic to the other side. match address  
100  
!  
!  
interface FastEthernet0/0  
  ip address 172.16.1.1 255.255.255.0  
  ip nat inside  
  duplex auto  
  speed auto  
!  
interface Serial0/0  
  description Interface to Internet
```

```
ip address 10.5.76.57 255.255.0.0
ip nat outside
crypto map mymap
!
!--- This is the NAT traffic. ip nat inside source
static network 172.16.0.0 172.19.0.0 /16 no-alias
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0
!
!--- Encrypt traffic to the other side. access-list 100
permit ip 172.19.0.0 0.0.255.255 172.18.0.0 0.0.255.255
!
!
line con 0
line aux 0
line vty 0 4
!
!
!
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** - Montre les associations de sécurisation de phase 2.
- **show crypto isakmp sa** - Montre les associations de sécurisation de phase 1.
- **traduction nat de show ip** — Affiche les traductions NAT en cours en service.

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.

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

- **debug crypto ipsec** — Affiche les négociations IPSecs 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** - Montre le trafic crypté.

Informations connexes

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