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

Contenu

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.

Remarque : Cette configuration n'est pas recommandée en tant que configuration permanente car elle risque de prêter à confusion du point de vue de la gestion du réseau.

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 :

- Routeur A : Routeur Cisco 3640 utilisant le logiciel Cisco IOS®, version 12.3(4)T

- Routeur B : Routeur Cisco 2621 avec Cisco IOS®, version de logiciel 12.3(5)

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.

Informations générales

Dans cet exemple, lorsque l'hôte 172.16.1.2 du site A accède au même hôte à adresse IP sur le site B, il se connecte à une adresse 172.19.1.2 plutôt qu'à l'adresse 172.16.1.2 réelle. Lorsque l'hôte du site B accède au site A, il se connecte à une adresse 172.18.1.2. La NAT sur le routeur A traduit toute adresse 172.16.x.x pour ressembler à l'entrée d'hôte 172.18.x.x correspondante. La NAT sur le routeur B modifie l'adresse 172.16.x.x pour ressembler à 172.19.x.x.

La fonction de chiffrement sur chaque routeur chiffre le trafic traduit sur les interfaces en série. Notez que la NAT survient *avant le chiffrement sur un routeur.*

Remarque : cette configuration permet uniquement aux deux réseaux de communiquer. Or, il ne permet pas la connectivité Internet. Vous avez besoin de chemins supplémentaires vers Internet pour assurer la connectivité à des emplacements autres que les deux sites; autrement dit, vous devez ajouter un autre routeur ou pare-feu de chaque côté, avec plusieurs itinéraires configurés sur les hôtes.

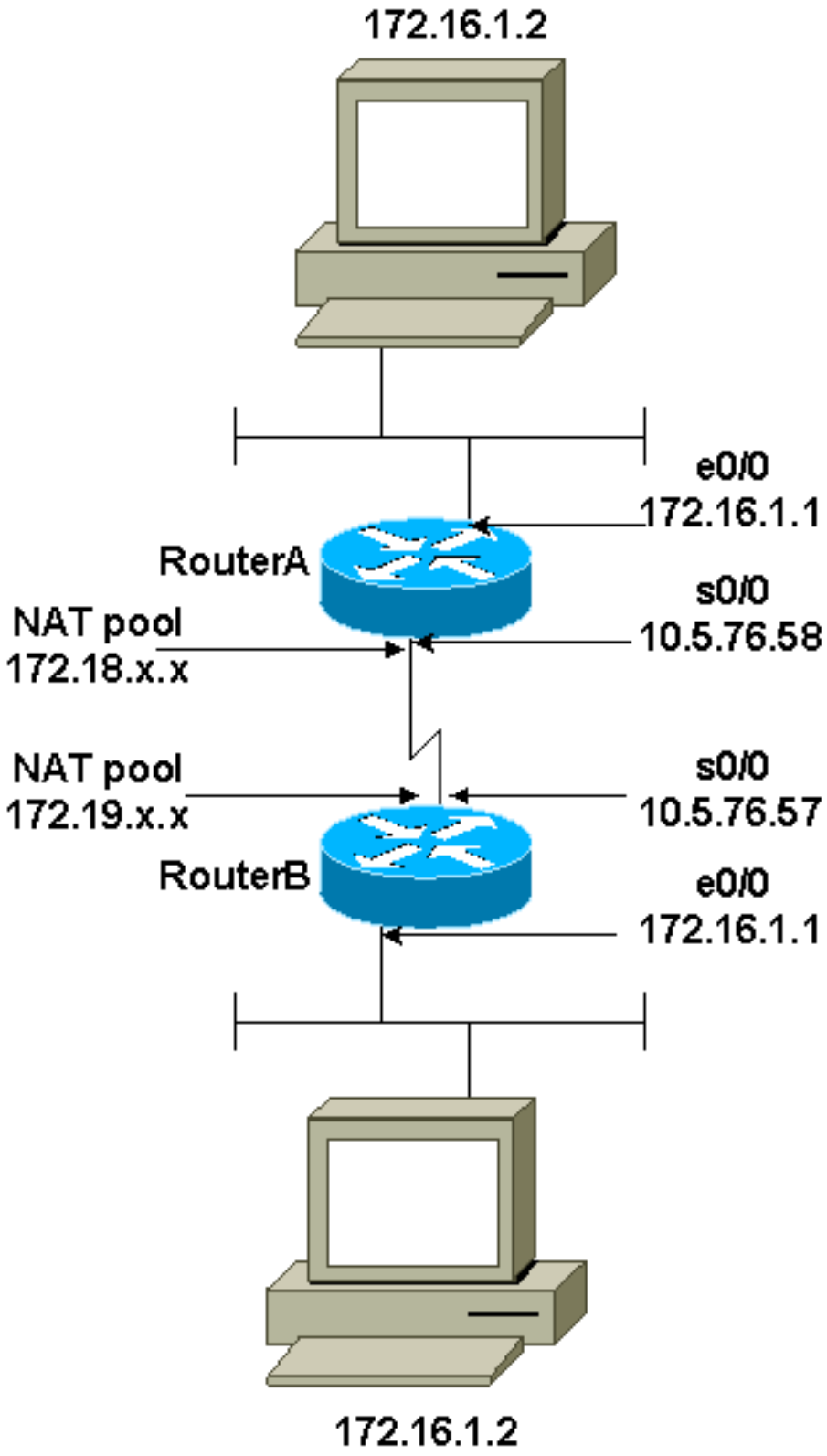
Configuration

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 suivante :



Configurations

Ce document utilise les configurations suivantes :

- Router A
- Router B

Router 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
```

Router 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
```

Vérification

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.**
- **show ip nat translation : Cette commande affiche les NAT actuellement utilisées.**

Dépannage

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'émettre des commandes **debug**, reportez-vous à Informations importantes sur les commandes de débogage.

- **debug crypto ipsec : Cette commande affiche les négociations IPSec de la phase 2.**
- **debug crypto isakmp : Cette commande affiche les négociations 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
- Configuration de la sécurité des réseaux IPSec
- Configuration du protocole IKE (Internet Key Exchange)
- Support technique - Cisco Systems