Configuration d'un tunnel IPSec de routeur entre deux réseaux privés avec NAT et une adresse IP statique

Contenu

Introduction

Cet exemple de configuration décrit les procédures suivantes :

- Chiffrement du trafic entre deux réseaux privés (10.1.1.x et 172.16.1.x).
- Attribution d'une adresse IP statique (adresse externe 200.1.1.25) à un périphérique réseau à l'adresse 10.1.1.3.

Vous devez utiliser des listes de contrôle d'accès (ACLs) pour signaler au routeur qu'il ne doit pas effectuer de traduction d'adresses réseau (NAT) pour le trafic entre réseaux privés, lequel sera alors chiffré et placé dans le tunnel en quittant le routeur. Il existe également un NAT statique pour un serveur interne sur le réseau à l'adresse 10.1.1.x dans cet exemple de configuration. Cet exemple de configuration utilise l'option route-map dans la commande NAT pour arrêter la traduction NAT si le trafic concerné est destiné à passer également par le tunnel chiffré.

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 :

- Logiciel Cisco IOS® Version 12.3(14)T
- Deux routeurs Cisco

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 à Conventions relatives aux conseils techniques Cisco.

Pourquoi l'instruction de refus dans l'ACL spécifie-t-elle le trafic NAT ?

Lorsque vous utilisez Cisco IOS IPsec ou un VPN, cela équivaut en quelque sorte à remplacer un réseau par un tunnel. Dans ce diagramme, vous remplacez le nuage Internet par un tunnel IPsec de Cisco IOS allant de 200.1.1.1 à 100.1.1.1. Apportez de la transparence à ce réseau pour les deux réseaux LAN privés joints ensemble par tunnel. C'est la raison pour laquelle vous ne souhaiterez généralement pas utiliser le NAT pour le trafic allant d'un réseau local privé au réseau local privé distant. Vous souhaitez voir les paquets provenant du réseau du routeur 2 avec une adresse IP source du réseau 10.1.1.0/24 au lieu de 200.1.1.1, lorsque les paquets atteignent le coeur de réseau du routeur 3.

Référez-vous à la commande NAT de l'opération pour plus d'informations sur la façon configurer un NAT. Ce document montre que le NAT s'effectue avant le contrôle crypto, quand le paquet va de l'intérieur vers l'extérieur. C'est pourquoi vous devez spécifier cette information dans la configuration.

```
ip nat inside source list 122 interface Ethernet0/1 overload
```

```
access-list 122 deny ip 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
```

Note: Il est également possible de construire le tunnel et de continuer à utiliser NAT. Vous spécifiez dans ce scénario le trafic NAT comme étant un « trafic intéressant pour IPsec » (appelé ACL 101 dans d'autres sections de ce document). Référez-vous à Configuration d'un tunnel IPsec entre les routeurs avec des sous-réseaux LAN en double pour plus d'informations sur la façon de construire un tunnel avec le NAT actif.

Qu'en est-il du NAT statique, pourquoi je n'arrive pas à atteindre

cette adresse via le tunnel IPsec ?

Cette configuration inclut également un NAT linéaire statique pour un serveur à l'adresse 10.1.1.3. Il est traduit à l'adresse 200.1.1.25 afin que les internautes puissent y accéder. Émettez la commande suivante :

```
ip nat inside source static 10.1.1.3 200.1.1.25
```

Ce NAT statique empêche les utilisateurs sur le réseau à l'adresse 172.16.1.x d'atteindre l'adresse 10.1.1.3 par l'intermédiaire du tunnel chiffré. C'est pourquoi vous devez refuser la traduction NAT du trafic chiffré avec l'ACL 122. Toutefois, la commande NAT statique a priorité sur la déclaration NAT générique pour toutes les connexions en provenance et à destination de 10.1.1.3. La déclaration NAT statique n'empêche pas spécialement la traduction du trafic chiffré. Les réponses de 10.1.1.3 sont traduites à 200.1.1.25 lorsqu'un utilisateur sur le réseau 172.16.1.x se connecte à l'adresse 10.1.1.3. Elles ne sont donc pas renvoyées par l'intermédiaire d'un tunnel chiffré (la traduction NAT se produit avant le chiffrement).

Vous devez refuser la traduction NAT du trafic chiffré (y compris pour un NAT statique linéaire) à l'aide d'une commande **route-map** sur la déclaration NAT statique.

Note: L'option **route-map** sur un NAT statique est seulement prise en charge à partir de la version 12.2(4)T du logiciel Cisco IOS et supérieure. Référez-vous à NAT — Capacité d'utiliser des mappages de route avec les traductions statiques pour information les informations complémentaires.

Vous devez émettre ces commandes supplémentaires pour permettre l'accès chiffré à l'hôte traduit de manière statique sur 10.1.1.3 :

```
ip nat inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
access-list 150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
```

Ces déclarations signalent au routeur qu'il doit uniquement appliquer le NAT statique au trafic correspondant à l'ACL 150. L'ACL 150 indique que la traduction NAT ne doit pas s'appliquer à un trafic issu de l'adresse 10.1.1.3 et destiné à atteindre 172.16.1.x par l'intermédiaire d'un tunnel chiffré. Cependant, elle peut s'appliquer à tous les autres trafics provenant de l'adresse 10.1.1.3 (trafic Internet).

Configurez

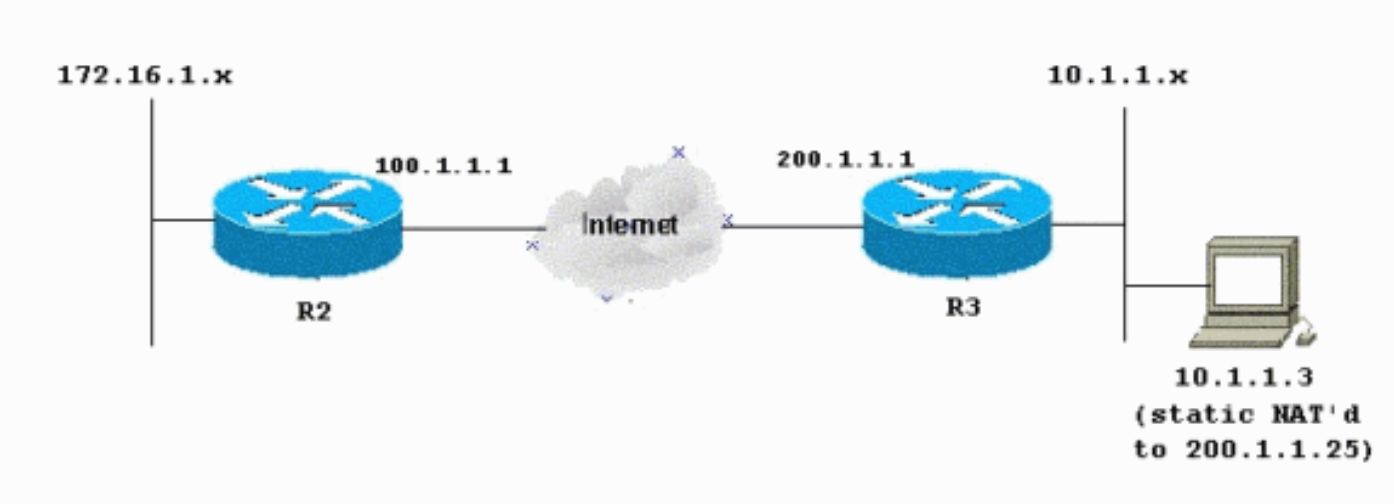
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Note: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus

d'informations sur les commandes utilisées dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes :

- Routeur 2
- Routeur 3

R2 - Configuration du routeur

```
R2#write terminal
Building configuration...
Current configuration : 1412 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
!
crypto isakmp policy 10
 authentication pre-share
!
```

```
crypto isakmp key ciscokey address 200.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
 set peer 200.1.1.1
 set transform-set myset
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: match address
101
!
!
!
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 100.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 crypto map myvpn
!
ip classless
ip route 0.0.0.0 0.0.0.0 100.1.1.254
!
ip http server
no ip http secure-server
!
!--- Except the private network from the NAT process: ip
nat inside source list 175 interface Ethernet1/0
overload
!
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: access-list 101
permit ip 172.16.1.0 0.0.0.255 10.1.1.0 0.0.0.255
!--- Except the private network from the NAT process:
access-list 175 deny   ip 172.16.1.0 0.0.0.255 10.1.1.0
0.0.0.255
access-list 175 permit ip 172.16.1.0 0.0.0.255 any
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

R3 - Configuration du routeur

```
R3#write terminal
Building configuration...
Current configuration : 1630 bytes
!
version 12.3
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone EST 0
ip subnet-zero
no ip domain lookup
!
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key ciscokey address 100.1.1.1
!
!
crypto ipsec transform-set myset esp-3des esp-md5-hmac
!
crypto map myvpn 10 ipsec-isakmp
 set peer 100.1.1.1
 set transform-set myset
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: match address
101
!
!
!
interface Ethernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
interface Ethernet1/0
 ip address 200.1.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 crypto map myvpn
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.1.1.254
!
no ip http server
no ip http secure-server
!
!--- Except the private network from the NAT process: ip
nat inside source list 122 interface Ethernet1/0
overload
!--- Except the static-NAT traffic from the NAT process
if destined !--- over the encrypted tunnel: ip nat
inside source static 10.1.1.3 200.1.1.25 route-map nonat
!
access-list 101 permit ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255
!--- Except the private network from the NAT process:
access-list 122 deny   ip 10.1.1.0 0.0.0.255 172.16.1.0
0.0.0.255
```

```
access-list 122 permit ip 10.1.1.0 0.0.0.255 any
!--- Except the static-NAT traffic from the NAT process
if destined !--- over the encrypted tunnel: access-list
150 deny   ip host 10.1.1.3 172.16.1.0 0.0.0.255
access-list 150 permit ip host 10.1.1.3 any
!
route-map nonat permit 10
 match ip address 150
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

Vérifiez

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

Dépannez

Utilisez cette section pour dépanner votre configuration.

Référez-vous à la section Dépannage de sécurité IP - Comprendre et utiliser les commandes de débogage pour de plus amples informations.

Dépannage des commandes

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Note: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug crypto ipsec SA** — Affiche les négociations IPSecs du Phase 2.
- **debug crypto isakmp SA** — Voyez les négociations ISAKMP du Phase 1.
- **debug crypto engine** — Affiche les sessions chiffrées.

Informations connexes

- Négociation IPSec/Protocole IKE - Cisco Systems
- Support et documentation techniques - Cisco Systems