Vérifier et dépanner les opérations NAT de base

Contenu

Introduction

Ce document décrit comment résoudre les problèmes de connectivité IP dans un environnement NAT.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous à Conventions des conseils techniques Cisco.

Problème

Ce document résout ces problèmes :

- Peut envoyer une requête ping à un routeur, mais pas à un autre routeur
- Les périphériques externes au réseau ne peuvent pas communiquer avec les routeurs

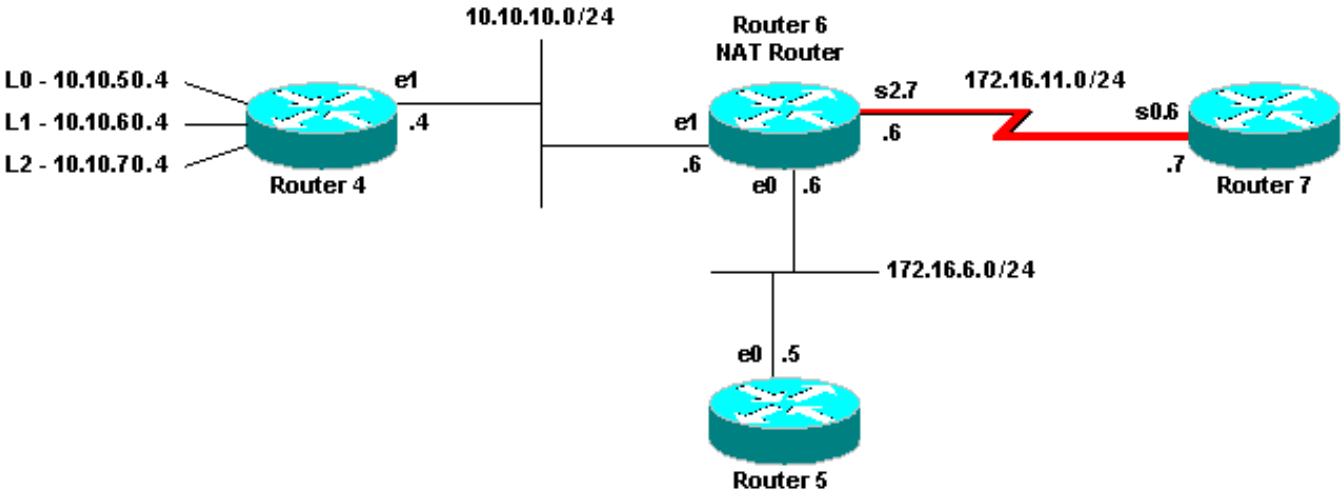
internes

Pour déterminer si le problème se trouve dans les opérations NAT :

1. En fonction de la configuration, définissez clairement ce que la NAT est censée atteindre.Vous pouvez déterminer qu'il y a un problème avec la configuration. Pour plus d'informations sur la configuration NAT, reportez-vous à Configuration de la traduction d'adresses réseau : Mise en route.
2. Vérifiez que des traductions correctes existent dans la table de traduction.
3. Utilisez les commandes **show** et **debug** pour vérifier que la traduction a lieu.
4. Examinez en détail ce qui arrive au paquet et vérifiez que les routeurs disposent des informations de routage correctes pour le déplacer.

- **Peut envoyer une requête ping à un routeur, mais pas à un autre routeur**

Dans ce schéma de réseau, le routeur 4 peut envoyer une requête ping au routeur 5 (172.16.6.5), mais pas au routeur 7 (172.16.11.7) :



Le routeur 4 ne peut pas envoyer de requête ping au routeur 7

Les protocoles de routage n'exécutent pas les routeurs. La passerelle par défaut du routeur 4 est le routeur 6. Le routeur 6 est configuré avec NAT :

```
interface Ethernet0 ip address 172.16.6.6 255.255.255.0 ip directed-broadcast ip nat outside !
interface Ethernet1 ip address 10.10.10.6 255.255.255.0 ip nat inside ! interface Serial2.7
point-to-point ip address 172.16.11.6 255.255.255.0 ip nat outside frame-relay interface-dlci
101 ! ip nat pool test 172.16.11.70 172.16.11.71 prefix-length 24 ip nat inside source list 7
pool test ip nat inside source static 10.10.10.4 172.16.6.14 ! access-list 7 permit 10.10.50.4
access-list 7 permit 10.10.60.4 access-list 7 permit 10.10.70.4
```

Pour dépanner :

1. Vous devez déterminer si NAT fonctionne correctement. Vous savez, d'après la configuration, que l'adresse IP du routeur 4 (10.10.10.4) est traduite de manière statique en 172.16.6.14. Vous pouvez utiliser la commande show ip nat translation sur le routeur 6 pour vérifier que la traduction existe dans la table de traduction :

```
router-6#show ip nat translation Pro Inside global Inside local Outside local Outside global ---
172.16.6.14 10.10.10.4 --- ---
```

2. Assurez-vous que cette traduction se produit lorsque le routeur 4 source le trafic IP. Vous

pouvez effectuer cette opération de deux manières à partir du routeur 6, exécuter le **débogage** NAT ou surveiller les statistiques NAT à l'aide de la commande **show ip nat statistics**. Comme les commandes **debug** sont le dernier recours, commencez par la commande **show**.

3. Surveillez le compteur pour vous assurer qu'il augmente au fur et à mesure qu'il reçoit le trafic du routeur 4. Le compteur s'incrémente chaque fois que la table de traduction est utilisée pour traduire une adresse.

4. Effacez les statistiques, affichez les statistiques, puis essayez d'envoyer une requête ping au routeur 7 à partir du routeur 4, puis affichez à nouveau les statistiques.

```
router-6#clear ip nat statistics router-6# router-6# show ip nat statistics Total active
translations: 1 (1 static, 0 dynamic; 0 extended) Outside interfaces: Ethernet0, Serial2.7
Inside interfaces: Ethernet1 Hits: 0 Misses: 0 Expired translations: 0 Dynamic mappings: --
Inside Source access-list 7 pool test refcount 0 pool test: netmask 255.255.255.0 start
172.16.11.70 end 172.16.11.71 type generic, total addresses 2, allocated 0 (0%), misses 0
router-6#
```

Après avoir utilisé la commande **ping 172.16.11.7** sur le routeur 4, les statistiques NAT sur le routeur 6 sont les suivantes :

```
router-6#show ip nat statistics Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces: Ethernet0, Serial2.7 Inside interfaces: Ethernet1 Hits: 5 Misses: 0 Expired
translations: 0 Dynamic mappings: -- Inside Source access-list 7 pool test refcount 0 pool test:
netmask 255.255.255.0 start 172.16.11.70 end 172.16.11.71 type generic, total addresses 2,
allocated 0 (0%), misses 0
```

Vous pouvez voir d'après les commandes show que le nombre de résultats est incrémenté par cinq. Dans une **requête ping** réussie à partir d'un routeur Cisco, le nombre de résultats augmente de dix. Les cinq échos ICMP (Internet Control Message Protocol) envoyés par le routeur source (Router 4) sont traduits et les cinq réponses d'écho aux paquets du routeur de destination (Router 7) doivent être traduites, pour un total de dix résultats. La perte de cinq résultats est due au fait que les réponses d'écho ne sont pas traduites ou ne sont pas envoyées depuis le routeur 7.

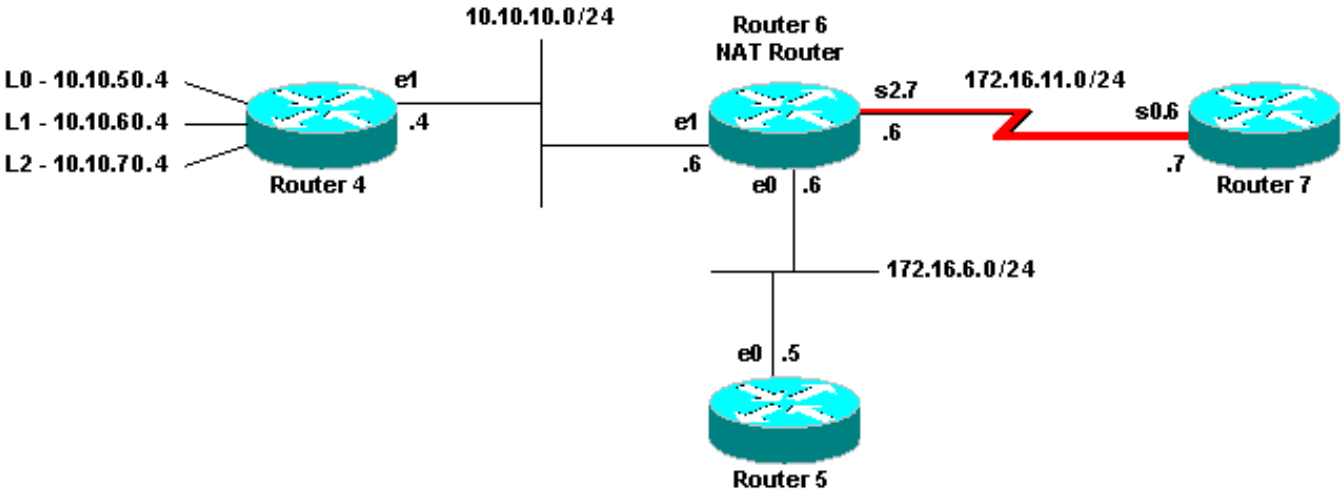
Recherchez une raison pour laquelle le routeur 7 n'envoie pas de paquets de réponse d'écho au routeur 4. Vous examinez ce que la NAT fait au paquet. Le routeur 4 envoie des paquets d'écho ICMP avec l'adresse source 10.10.10.4 et l'adresse de destination 172.16.11.7. Après la NAT, le paquet reçu par le routeur 7 a une adresse source 172.16.6.14 et une adresse de destination 172.16.11.7. Le routeur 7 doit répondre à 172.16.6.14, et, puisque l'adresse 172.16.6.14 n'est pas directement connectée au routeur 7, il a besoin d'une route pour ce réseau pour pouvoir répondre. Contrôlez la table de routage du routeur 7 pour vérifier que la route existe.

```
router-7#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i -
IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set 172.16.0.0/24 is subnetted, 4 subnets C 172.16.12.0 is directly connected, Serial0.8 C
172.16.9.0 is directly connected, Serial0.5 C 172.16.11.0 is directly connected, Serial0.6 C
172.16.5.0 is directly connected, Ethernet0
```

Vous pouvez constater que la table de routage du routeur 7 ne contient pas de route pour 172.16.6.14. Une fois cette route ajoutée, la requête ping fonctionne. Il est utile de surveiller les statistiques NAT à l'aide de la commande **show ip nat statistics**. Dans un environnement NAT plus complexe avec plusieurs traductions, cette commande **show** n'est plus utile. Vous pouvez ensuite exécuter **des débogages** sur le routeur.

- **Les périphériques externes au réseau ne peuvent pas communiquer avec les routeurs internes**

Dans ce problème, le routeur 4 peut **envoyer une requête ping** aux routeurs 5 et 7, mais les périphériques du réseau 10.10.50.0 ne peuvent pas communiquer avec le routeur 5 ou 7. Le schéma de réseau est le suivant :



Le réseau ne peut pas communiquer avec le routeur

```
interface Ethernet0 ip address 172.16.6.6 255.255.255.0 ip directed-broadcast ip nat outside
media-type 10BaseT ! interface Ethernet1 ip address 10.10.10.6 255.255.255.0 ip nat inside
media-type 10BaseT ! interface Serial2.7 point-to-point ip address 172.16.11.6 255.255.255.0 ip
nat outside frame-relay interface-dlci 101 ! ip nat pool test 172.16.11.70 172.16.11.71 prefix-
length 24 ip nat inside source list 7 pool test ip nat inside source static 10.10.10.4
172.16.6.14 ! access-list 7 permit 10.10.50.4 access-list 7 permit 10.10.60.4 access-list 7
permit 10.10.70.4
```

Indiquez le comportement attendu de la fonction NAT. À partir de la configuration du routeur 6, vous savez que NAT est censé traduire dynamiquement 10.10.50.4 en la première adresse disponible dans le pool NAT « test ». Le pool se compose des adresses 172.16.11.70 et 172.16.11.71. À partir de ce problème, vous pouvez comprendre que les paquets que les routeurs 5 et 7 reçoivent ont soit une adresse source de 172.16.11.70 ou 172.16.11.71. Ces adresses se trouvent sur le même sous-réseau que le routeur 7. Par conséquent, le routeur 7 doit disposer d'une route connectée directement. Toutefois, s'il n'en possède pas déjà, le routeur 5 doit disposer d'une route vers le sous-réseau .

Vous pouvez utiliser la commande show ip route pour voir que la table de routage du routeur 5 contient l'adresse 172.16.11.0 :

```
router-5#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i -
IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set 172.16.0.0/24 is subnetted, 4 subnets C 172.16.9.0 is directly connected, Serial1 S
172.16.11.0 [1/0] via 172.16.6.6 C 172.16.6.0 is directly connected, Ethernet0 C 172.16.2.0 is
directly connected, Serial0
```

Vous pouvez utiliser la commande **show ip route pour voir que la table de routage du routeur contient l'adresse 7172.16.11.0 comme sous-réseau directement connecté :**

```
router-6#show ip nat translation Pro Inside global Inside local Outside local Outside global --- 172.16.6.14 10.10.10.4 --- --- --- 172.16.11.70 10.10.50.4 --- ---
```

Vérifiez la table de traduction NAT et vérifiez que la traduction attendue existe. Puisque la traduction souhaitée est créée dynamiquement, vous devez d'abord envoyer le trafic IP provenant de l'adresse appropriée. Après une **requête ping** envoyée, provenant de 10.10.50.4 et destinée à 172.16.11.7, la table de traduction du routeur 6 indique :

```
router-6#show ip nat translation Pro Inside global Inside local Outside local Outside global --- 172.16.6.14 10.10.10.4 --- --- --- 172.16.11.70 10.10.50.4 --- ---
```

Puisque la traduction attendue se trouve dans la table de traduction, vous savez que les paquets d'écho ICMP sont correctement traduits. Une option est que vous pouvez surveiller les statistiques NAT, mais ce n'est pas utile dans un environnement complexe. Une autre option consiste à exécuter le débogage NAT sur le routeur NAT (routeur 6). Vous pouvez exécuter **debug ip nat** sur le routeur 6 pendant que vous envoyez une **requête ping** provenant de 10.10.50.4 et destinée à 172.16.11.7. Les résultats **de débogage** figurent dans l'exemple de code suivant.

> **Note**: Quand vous utilisez n'importe quelle commande debug sur un routeur, vous pouvez surcharger le routeur et le rendre inopérable. Faites toujours preuve d'une extrême prudence et, si possible, n'exécutez jamais un **débogage** sur un routeur de production critique sans la supervision d'un ingénieur du support technique Cisco.

::

```
router-6# show log Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns) Console logging: level debugging, 39 messages logged Monitor logging: level debugging, 0 messages logged Buffer logging: level debugging, 39 messages logged Trap logging: level informational, 33 message lines logged Log Buffer (4096 bytes): 05:32:23: NAT: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [70] 05:32:23: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [70] 05:32:25: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [71] 05:32:25: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [71] 05:32:27: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [72] 05:32:27: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [72] 05:32:29: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [73] 05:32:29: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [73] 05:32:31: NAT*: s=10.10.50.4->172.16.11.70, d=172.16.11.7 [74] 05:32:31: NAT*: s=172.16.11.7, d=172.16.11.70->10.10.50.4 [74]
```

Comme vous pouvez le voir à partir de la sortie de **débogage** précédente, la première ligne affiche l'adresse source 10.10.50.4 traduite en 172.16.11.70. La deuxième ligne indique que l'adresse de destination 172.16.11.70 est traduite en 10.10.50.4. Ce schéma se répète dans le reste du débogage. Cela signifie que le routeur 6 traduit les paquets dans les deux directions.

Révision :

1. Le routeur 4 envoie un paquet de 10.10.50.4 vers 172.16.11.7.

2. Le routeur 6 effectue la NAT sur le paquet et transfère un paquet avec une source 172.16.11.70 et une destination 172.16.11.7.

3. Le routeur 7 envoie une réponse de 172.16.11.7 vers 172.16.11.70.

4. Le routeur 6 effectue la NAT sur le paquet. Ainsi, le paquet a l'adresse source 172.16.11.7 et l'adresse de destination 10.10.50.4.

5. Le routeur 6 achemine le paquet vers 10.10.50.4 en fonction des informations de la table de

routage du routeur 6. Vous devez utiliser la commande show ip route pour confirmer que le routeur 6 dispose de la route nécessaire dans sa table de routage.

```
router-6#show ip route Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP i -
IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area * - candidate default, U -
per-user static route, o - ODR P - periodic downloaded static route Gateway of last resort is
not set 172.16.0.0/24 is subnetted, 5 subnets C 172.16.8.0 is directly connected, Serial1 C
172.16.10.0 is directly connected, Serial2.8 C 172.16.11.0 is directly connected, Serial2.7 C
172.16.6.0 is directly connected, Ethernet0 C 172.16.7.0 is directly connected, Serial0
10.0.0.0/24 is subnetted, 1 subnets C 10.10.10.0 is directly connected, Ethernet1
```

Liste de contrôle des problèmes courants

Utilisez cette liste de contrôle pour résoudre les problèmes courants :

- **Traduction non installée dans la table de traduction**

Si vous constatez que la traduction appropriée n'est pas installée dans la table de traduction, vérifiez :

1. La configuration est correcte. Il est difficile d'obtenir NAT pour obtenir ce que vous voulez parfois. Pour obtenir de l'aide pour la configuration, consultez la rubrique Configuration de la traduction d'adresses réseau : Mise en route.
2. Aucune liste d'accès entrante ne refuse l'entrée de paquets à partir du routeur NAT.
3. Le routeur NAT dispose de la route appropriée dans la table de routage si le paquet va de l'intérieur vers l'extérieur. Référez-vous à Ordre des opérations NAT pour plus d'informations.
4. La liste d'accès référencée par la commande NAT autorise tous les réseaux nécessaires.
5. Il y a assez d'adresses dans le pool NAT. Cela ne pose problème que si NAT n'est pas configuré pour la congestion.
6. Les interfaces du routeur sont convenablement définies en tant que NAT extérieure ou intérieure.
7. Pour la traduction de la charge utile des paquets DNS (Domain Name System), assurez-vous que la traduction a lieu sur l'adresse dans l'en-tête IP du paquet. Si ceci ne se produit pas, alors la NAT ne regarde pas dans les données utiles du paquet.

- **L'entrée de traduction correcte n'est pas utilisée**

Si l'entrée de traduction correcte est installée dans la table de traduction, mais n'est pas utilisée, vérifiez :

1. Vérifiez qu'il n'existe aucune liste d'accès entrante qui refuse l'entrée des paquets à partir du routeur NAT.
2. Pour les paquets qui vont de l'intérieur vers l'extérieur, vérifiez qu'il existe une route vers la destination, car elle est vérifiée avant la traduction. Référez-vous à Ordre des opérations NAT pour plus d'informations.

- **La NAT fonctionne correctement, mais il reste des problèmes de connectivité**

Dépannez le problème de connectivité :

1. Vérifiez la connectivité de la couche 2.
2. Vérifiez les informations de routage de la couche 3.
3. Recherchez les filtres de paquets qui causent le problème.

- **La traduction NAT pour le port 80 ne fonctionne pas**

Cela signifie que la traduction NAT pour le port 80 ne fonctionne pas, mais la traduction pour les autres ports fonctionne normalement.

Pour résoudre ce problème :

1. Exécutez les commandes **debug ip nat translations** et **debug ip packet** afin de vérifier si les traductions sont correctes et si l'entrée de traduction correcte est installée dans la table de traduction.
2. Vérifiez que le serveur répond.
3. Désactivez le serveur HTTP.
4. Effacez les tables de NAT et ARP.

- **%NAT : System busy. Try later**

Le message d'erreur try later apparaît lorsqu'une commande **show** liée à NAT ou une **commande show running-config** ou **write memory** est exécutée. Ceci est dû à l'augmentation de la taille de la table NAT. Quand la taille de la table NAT augmente, le routeur manque de mémoire.

1. Rechargez le routeur afin de résoudre ce problème.
2. Si le message d'erreur apparaît quand le HSRP SNAT est configuré, configurez ces commandes afin de résoudre le problème : Router(config)#standby delay minimum 20 reload 20Router(config)#standby 2 preempt delay minimum 20 reload 20 sync 10

- **La grande table de traduction augmente la CPU**

Un hôte peut envoyer des centaines de traductions, ce qui entraîne une utilisation élevée du CPU. En d'autres termes, la table peut devenir si volumineuse que la CPU fonctionne à 100 pour cent. La commande **ip nat translation max-entry 300** crée la limite de 300 par hôte ou une limite globale de la quantité de traductions sur le routeur. La solution consiste à utiliser la commande ip nat translation max-entries all-hosts 300.

- **% d'adresses IP publiques déjà mappées (adresse IP interne - > adresse IP publique)**

Ce message apparaît lorsque vous essayez de configurer deux adresses IP internes sur une adresse IP publique qui écoute sur les mêmes ports.

```
% X.X.X.X already mapped (172.30.62.101 -> X.X.X.X)
```

Afin de corriger ceci, configurez l'adresse IP publique pour qu'elle ait deux adresses IP internes et utilisez deux adresses IP publiques dans le DNS.

- **Aucune entrée dans la table ARP**

Cela résulte du no-alias sur les entrées NAT. Les no-alias signifie que le routeur ne répond pas pour les adresses et n'installe pas d'entrée ARP. Si un autre routeur utilise un pool NAT en tant que regroupement global intérieur composé des adresses sur un sous-réseau lié, un alias est généré pour cette adresse de sorte que le routeur puisse répondre aux demandes de protocole de résolution d'adresse (ARP) de ces adresses. Ainsi le routeur dispose d'entrées ARP pour les fausses adresses.

- **Jeton 0 incorrect, TOK_NUMBER|TOK_PUNCT souhaité**

Ce message d'erreur est juste un message d'information et n'a pas d'incidence sur le comportement normal du périphérique.

`Bad token 0, wanted TOK_NUMBER|TOK_PUNCT`

L'erreur signifie que la NAT tente d'effectuer une correction de couche 4 sur l'adresse dans un FTP ouvert et ne trouve pas les adresses IP qu'elle doit traduire dans le paquet. La raison pour laquelle le message inclut des jetons est que les adresses IP du paquet sont trouvées par la recherche d'un jeton, ou d'un ensemble de symboles, dans le paquet IP, afin de trouver les détails nécessaires à la traduction.

Quand une session FTP est initiée, elle négocie deux canaux, un canal de commande et un canal de transmission de données. Ce sont deux adresses IP avec différents numéros de port. Le client et le serveur FTP négocient un deuxième canal de données vers lequel transférer des fichiers. Le paquet échangé via le canal de contrôle a le format « PORT, i, i, i, i, i, p, p », où i, i, i, i sont les quatre octets d'une adresse IP et p, p spécifie le port. NAT tente de correspondre à ce modèle et de traduire adresse/port, si nécessaire. NAT doit traduire les deux schémas de canaux. La NAT recherche des numéros dans le flux de commande jusqu'à ce qu'elle pense avoir trouvé un commande de port qui requiert une traduction. Il analyse ensuite la traduction, qu'il calcule avec le même format.

Si le paquet est endommagé ou si le serveur FTP ou le client a des commandes mal formées, NAT ne peut pas calculer correctement la traduction et génère cette erreur. Vous pouvez définir le client FTP sur « passive » afin qu'il initie les deux canaux.

Informations connexes

- Page de support NAT
- Support technique - Cisco Systems