Listes de contrôle d'accès et fragments IP

Contenu

Introduction

Ce livre blanc explique les différents genres d'entrées de liste de contrôle d'accès (ACL) et ce qui se produit quand les différents genres de paquets rencontrent ces diverses entrées. Les ACL sont utilisées pour bloquer des paquets IP d'être retransmis par un routeur.

Le document RFC 1858 couvre les considérations de sécurité pour le filtrage des fragments IP et met en évidence deux attaques sur des hôtes qui impliquent des fragments IP de paquets TCP, l'attaque par fragments minuscules et l'attaque par fragments superposés. Le blocage de ces attaques est souhaitable car elles peuvent compromettre un hôte ou bloquer toutes ses ressources internes.

Le document RFC 1858 décrit également deux méthodes de défense contre ces attaques, directe et indirecte. Dans la méthode directe, les fragments initiaux qui sont plus petits qu'une longueur minimale sont éliminés. La méthode indirecte consiste à supprimer le deuxième fragment d'un jeu de fragments, s'il commence 8 octets dans le datagramme IP d'origine. Pour plus de détails, consultez RFC 1858 .

Traditionnellement, les filtres de paquets tels que les ACL sont appliqués aux non-fragments et au fragment initial d'un paquet IP parce qu'ils contiennent à la fois des informations de couche 3 et 4 auxquelles les ACL peuvent correspondre pour une décision d'autorisation ou de refus. Les fragments non initiaux sont traditionnellement autorisés via la liste de contrôle d’accès car ils peuvent être bloqués en fonction des informations de couche 3 dans les paquets ; cependant, comme ces paquets ne contiennent pas d’informations de couche 4, ils ne correspondent pas aux informations de couche 4 de l’entrée de liste de contrôle d’accès, s’il existe. Autoriser les fragments non initiaux d’un datagramme IP à traverser est acceptable car l’hôte qui reçoit les fragments ne peut pas réassembler le datagramme IP d’origine sans le fragment initial.

Les pare-feu peuvent également être utilisés pour bloquer les paquets en conservant une table de fragments de paquets indexés par adresse IP source et de destination, protocole et ID IP. Le

pare-feu Cisco PIX Firewall et le pare-feu Cisco IOS® peuvent filtrer tous les fragments d'un flux particulier en conservant cette table d'informations, mais il est trop coûteux de le faire sur un routeur pour des fonctionnalités ACL de base. Le rôle principal d'un pare-feu est de bloquer les paquets, et son rôle secondaire est d'acheminer les paquets ; le rôle principal d'un routeur est de router les paquets, et son rôle secondaire est de les bloquer.

Deux modifications ont été apportées aux versions 12.1(2) et 12.0(11) du logiciel Cisco IOS pour résoudre certains problèmes de sécurité liés aux fragments TCP. La méthode indirecte, décrite dans la RFC 1858 , a été mise en oeuvre dans le cadre du contrôle standard de l'intégrité des paquets d'entrée TCP/IP. Des modifications ont également été apportées à la fonctionnalité des listes de contrôle d'accès en ce qui concerne les fragments non initiaux.

Types d'entrées ACL

Il existe six types différents de lignes ACL et chacune a une conséquence si un paquet ne correspond pas ou ne correspond pas. Dans la liste suivante, FO = 0 indique un non-fragment ou un fragment initial dans un flux TCP, FO > 0 indique que le paquet est un fragment non initial, L3 signifie couche 3 et L4, couche 4.

Remarque : Lorsque la ligne de liste de contrôle d'accès contient des informations de couche 3 et de couche 4 et que le mot clé **fragments** est présent, l'action de la liste de contrôle d'accès est conservatrice pour les actions d'autorisation et de refus. Les actions sont conservatrices car vous ne voulez pas refuser accidentellement une partie fragmentée d'un flux, car les fragments ne contiennent pas suffisamment d'informations pour correspondre à tous les attributs de filtre. Dans le cas de refus, au lieu de refuser un fragment non initial, l'entrée de liste de contrôle d'accès suivante est traitée. Dans le cas de l'autorisation, on suppose que les informations de couche 4 du paquet, si elles sont disponibles, correspondent aux informations de couche 4 de la ligne de liste de contrôle d'accès.

Autoriser la ligne ACL avec les informations de couche 3 uniquement

1. Si les informations de couche 3 d'un paquet correspondent aux informations de couche 3 de la ligne de liste de contrôle d'accès, elles sont autorisées.
2. Si les informations de couche 3 d'un paquet ne correspondent pas aux informations de couche 3 de la ligne de liste de contrôle d'accès, l'entrée de liste de contrôle d'accès suivante est traitée.

Refuser la ligne ACL avec les informations de couche 3 uniquement

1. Si les informations de couche 3 d'un paquet correspondent aux informations de couche 3 de la ligne de liste de contrôle d'accès, elles sont refusées.
2. Si les informations de couche 3 d'un paquet ne correspondent pas aux informations de couche 3 de la ligne de liste de contrôle d'accès, l'entrée de liste de contrôle d'accès suivante est traitée.

Autoriser la ligne ACL avec les informations de couche 3 uniquement, et le mot clé fragments est présent

Si les informations de couche 3 d'un paquet correspondent aux informations de couche 3 de la

ligne de liste de contrôle d'accès, le décalage de fragment du paquet est vérifié.

1. Si FO > 0 d'un paquet, le paquet est autorisé.
2. Si FO = 0 d'un paquet, l'entrée de liste de contrôle d'accès suivante est traitée.

Refuser la ligne ACL avec les informations de couche 3 uniquement, et le mot clé fragments est présent

Si les informations de couche 3 d'un paquet correspondent aux informations de couche 3 de la ligne de liste de contrôle d'accès, le décalage de fragment du paquet est vérifié.

1. Si le FO > 0 d'un paquet est refusé.
2. Si FO = 0 d'un paquet, la ligne de liste de contrôle d'accès suivante est traitée.

Autoriser la ligne ACL avec les informations L3 et L4

1. Si les informations de couche 3 et de couche 4 d'un paquet correspondent à la ligne ACL et à FO = 0, le paquet est autorisé.
2. Si les informations de couche 3 d'un paquet correspondent à la ligne de la liste de contrôle d'accès et à FO > 0, le paquet est autorisé.

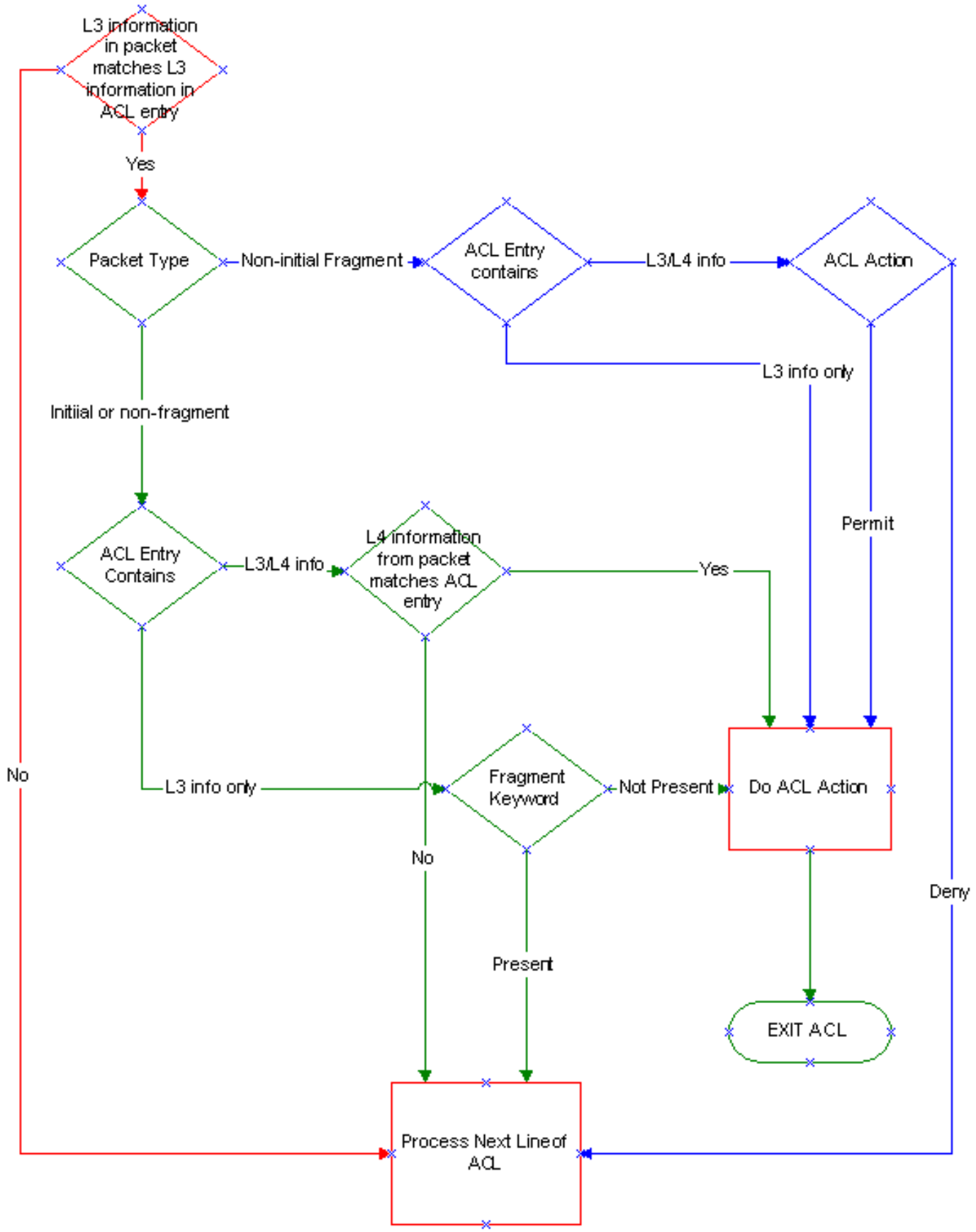
Refuser la ligne ACL avec les informations L3 et L4

1. Si les informations de couche 3 et de couche 4 d'un paquet correspondent à l'entrée de la liste de contrôle d'accès et à FO = 0, le paquet est refusé.
2. Si les informations de couche 3 d'un paquet correspondent à la ligne de liste de contrôle d'accès et à FO > 0, l'entrée de liste de contrôle d'accès suivante est traitée.

Organigramme des règles ACL

L'organigramme suivant illustre les règles de liste de contrôle d'accès lorsque des fragments non-fragments, des fragments initiaux et des fragments non initiaux sont vérifiés par rapport à la liste de contrôle d'accès.

Remarque : Les fragments non initiaux eux-mêmes contiennent uniquement des informations de couche 3, jamais de couche 4, bien que la liste de contrôle d'accès puisse contenir des informations de couche 3 et de couche 4.



Comment les paquets peuvent correspondre à une liste de contrôle d'accès

Exemple 1

Les cinq scénarios suivants impliquent différents types de paquets rencontrant la liste de contrôle d'accès 100. Reportez-vous au tableau et à l'organigramme lorsque vous suivez ce qui se passe dans chaque situation. L'adresse IP du serveur Web est 171.16.23.1.

```
access-list 100 permit tcp any host 171.16.23.1 eq 80

access-list 100 deny ip any any
```

Le paquet est un fragment initial ou un non-fragment destiné au serveur sur le port 80 :

La première ligne de la liste de contrôle d'accès contient des informations de couche 3 et de couche 4, qui correspondent aux informations de couche 3 et de couche 4 du paquet, de sorte que le paquet est autorisé.

Le paquet est un fragment initial ou un non-fragment destiné au serveur sur le port 21 :

1. La première ligne de la liste de contrôle d'accès contient à la fois des informations de couche 3 et de couche 4, mais les informations de couche 4 de la liste de contrôle d'accès ne correspondent pas au paquet, de sorte que la ligne de liste de contrôle d'accès suivante est traitée.
2. La deuxième ligne de la liste de contrôle d'accès refuse tous les paquets, donc le paquet est refusé.

Le paquet est un fragment non initial vers le serveur dans un flux du port 80 :

La première ligne de la liste de contrôle d'accès contient des informations de couche 3 et de couche 4, les informations de couche 3 de la liste de contrôle d'accès correspondent au paquet et l'action de la liste de contrôle d'accès est d'autoriser, de sorte que le paquet est autorisé.

Le paquet est un fragment non initial vers le serveur dans un flux du port 21 :

La première ligne de la liste de contrôle d'accès contient des informations de couche 3 et de couche 4. Les informations de couche 3 de la liste de contrôle d'accès correspondent au paquet, il n'y a aucune information de couche 4 dans le paquet et l'action de la liste de contrôle d'accès est d'autoriser, de sorte que le paquet est autorisé.

Le paquet est un fragment initial, non fragmenté ou non initial vers un autre hôte du sous-réseau du serveur :

1. La première ligne de la liste de contrôle d'accès contient des informations de couche 3 qui ne correspondent pas aux informations de couche 3 du paquet (l'adresse de destination), de sorte que la ligne de liste de contrôle d'accès suivante est traitée.
2. La deuxième ligne de la liste de contrôle d'accès refuse tous les paquets, donc le paquet est refusé.

Exemple 2

Les cinq mêmes scénarios possibles suivants impliquent différents types de paquets rencontrant la liste de contrôle d'accès 101. Encore une fois, veuillez consulter le tableau et le diagramme de flux au fur et à mesure que vous suivez ce qui se passe dans chaque situation. L'adresse IP du serveur Web est 171.16.23.1.

```
access-list 101 deny ip any host 171.16.23.1 fragments

access-list 101 permit tcp any host 171.16.23.1 eq 80

access-list 101 deny ip any any
```

Le paquet est un fragment initial ou un non-fragment destiné au serveur sur le port 80 :

1. La première ligne de la liste de contrôle d'accès contient des informations de couche 3 qui correspondent aux informations de couche 3 du paquet. L'action de la liste de contrôle d'accès consiste à refuser, mais comme le mot clé **fragments** est présent, l'entrée de liste de contrôle d'accès suivante est traitée.
2. La deuxième ligne de la liste de contrôle d'accès contient les informations des couches 3 et 4, qui correspondent au paquet, de sorte que le paquet est autorisé.

Le paquet est un fragment initial ou un non-fragment destiné au serveur sur le port 21 :

1. La première ligne de la liste de contrôle d'accès contient des informations de couche 3, qui correspondent au paquet, mais l'entrée de la liste de contrôle d'accès contient également le mot clé **fragments**, qui ne correspond pas au paquet car FO = 0, de sorte que l'entrée de la liste de contrôle d'accès suivante est traitée.
2. La deuxième ligne de la liste de contrôle d'accès contient des informations sur les couches 3 et 4. Dans ce cas, les informations de couche 4 ne correspondent pas, de sorte que l'entrée de liste de contrôle d'accès suivante est traitée.
3. La troisième ligne de la liste de contrôle d'accès refuse tous les paquets, de sorte que le paquet est refusé

Le paquet est un fragment non initial vers le serveur dans un flux du port 80 :

La première ligne de la liste de contrôle d'accès contient des informations de couche 3 qui correspondent aux informations de couche 3 du paquet. Rappelez-vous que même si cela fait partie d'un flux de port 80, il n'y a aucune information de couche 4 dans le fragment non initial. Le paquet est refusé car les informations de couche 3 correspondent.

Le paquet est un fragment non initial vers le serveur dans un flux du port 21 :

La première ligne de la liste de contrôle d'accès contient uniquement des informations de couche 3 et correspond au paquet, de sorte que le paquet est refusé.

Le paquet est un fragment initial, non fragmenté ou non initial vers un autre hôte du sous-réseau du serveur :

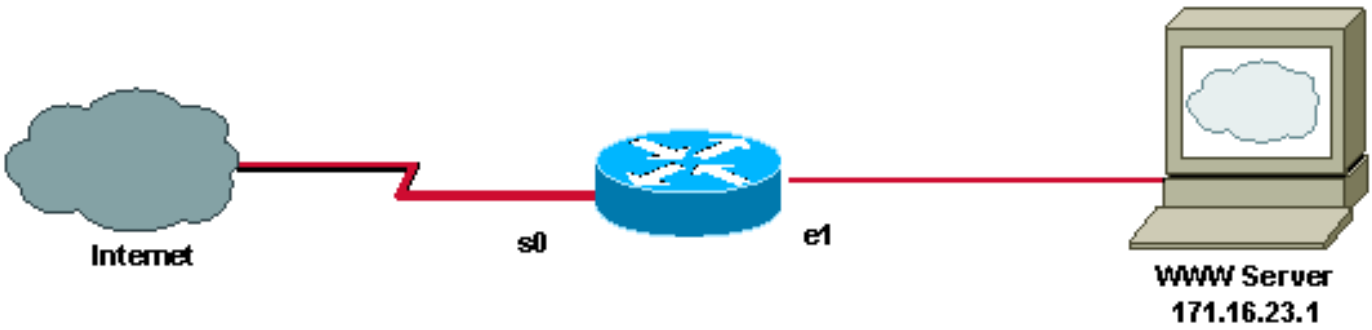
1. La première ligne de la liste de contrôle d’accès contient uniquement des informations de couche 3 et ne correspond pas au paquet. La ligne de liste de contrôle d’accès suivante est donc traitée.
2. La deuxième ligne de la liste de contrôle d’accès contient des informations sur les couches 3 et 4. Les informations de couche 4 et de couche 3 du paquet ne correspondent pas à celles de la liste de contrôle d’accès. La ligne de liste de contrôle d’accès suivante est donc traitée.
3. La troisième ligne de la liste de contrôle d’accès refuse ce paquet

Scénarios de mots clés de fragments

Scénario 1

Le routeur B se connecte à un serveur Web et l’administrateur réseau ne souhaite pas autoriser l’accès de fragments au serveur. Ce scénario montre ce qui se passe si l’administrateur réseau implémente la liste de contrôle d’accès 100 par rapport à la liste de contrôle d’accès 101. La liste de contrôle d’accès est appliquée en entrée sur l’interface Serial0 (s0) du routeur et doit autoriser uniquement les paquets non fragmentés à atteindre le serveur Web. Reportez-vous à l'organigramme des règles de liste de contrôle d'accès et aux sections Comment les paquets peuvent correspondre à une liste de contrôle d'accès lorsque vous suivez le scénario.

Conséquences de l'utilisation du mot clé de fragments



La liste de contrôle d’accès ACL 100 est la suivante :

```
access-list 100 permit tcp any host 171.16.23.1 eq 80

access-list 100 deny ip any any
```

La première ligne de la liste de contrôle d’accès 100 autorise uniquement le protocole HTTP au serveur, mais autorise également les fragments non initiaux à tout port TCP sur le serveur. Il autorise ces paquets parce que les fragments non initiaux ne contiennent pas d'informations de couche 4 et la logique de la liste de contrôle d'accès suppose que si les informations de couche 3 correspondent, les informations de couche 4 correspondent également, si elles étaient disponibles. La deuxième ligne est implicite et refuse tout autre trafic.

Il est important de noter que, depuis les versions 12.1(2) et 12.0(11) du logiciel Cisco IOS, le nouveau code de liste de contrôle d’accès supprime les fragments qui ne correspondent à aucune autre ligne de la liste de contrôle d’accès. Les versions antérieures autorisent les fragments non initiaux à travers s'ils ne correspondent à aucune autre ligne de la liste de contrôle d'accès.

La liste de contrôle d’accès ACL 101 est la suivante :

```
access-list 101 deny ip any host 171.16.23.1 fragments

access-list 101 permit tcp any host 171.16.23.1 eq 80

access-list 101 deny ip any any
```

La liste de contrôle d’accès 101 n’autorise pas les fragments non initiaux à traverser le serveur en raison de la première ligne. Un fragment non initial vers le serveur est refusé lorsqu’il rencontre la première ligne de liste de contrôle d’accès, car les informations de couche 3 du paquet correspondent aux informations de couche 3 de la ligne de liste de contrôle d’accès.

Les fragments initiaux ou non au port 80 sur le serveur correspondent également à la première ligne de la liste de contrôle d’accès pour les informations de couche 3, mais comme le mot clé fragments est présent, l’entrée de la liste de contrôle d’accès suivante (la deuxième ligne) est traitée. La deuxième ligne de la liste de contrôle d’accès autorise les fragments initiaux ou non, car ils correspondent à la ligne de la liste de contrôle d’accès pour les informations de couche 3 et de couche 4.

Les fragments non initiaux destinés aux ports TCP des autres hôtes du réseau 171.16.23.0 sont bloqués par cette liste de contrôle d’accès. Les informations de couche 3 de ces paquets ne correspondent pas aux informations de couche 3 de la première ligne de liste de contrôle d’accès, de sorte que la ligne de liste de contrôle d’accès suivante est traitée. Les informations de couche 3 de ces paquets ne correspondent pas non plus aux informations de couche 3 de la deuxième ligne de liste de contrôle d’accès, de sorte que la troisième ligne de liste de contrôle d’accès est traitée. La troisième ligne est implicite et refuse tout trafic.

Dans ce scénario, l’administrateur réseau décide d’implémenter la liste de contrôle d’accès 101, car elle autorise uniquement les flux HTTP non fragmentés vers le serveur.

Scénario 2

Un client dispose d'une connectivité Internet sur deux sites différents, et il existe également une connexion de porte dérobée entre les deux sites. La politique de l'administrateur réseau consiste à autoriser le groupe A du site 1 à accéder au serveur HTTP du site 2. Les routeurs des deux sites utilisent des adresses privées (RFC 1918) et NAT (Network Address Translation) pour traduire les paquets routés via Internet.

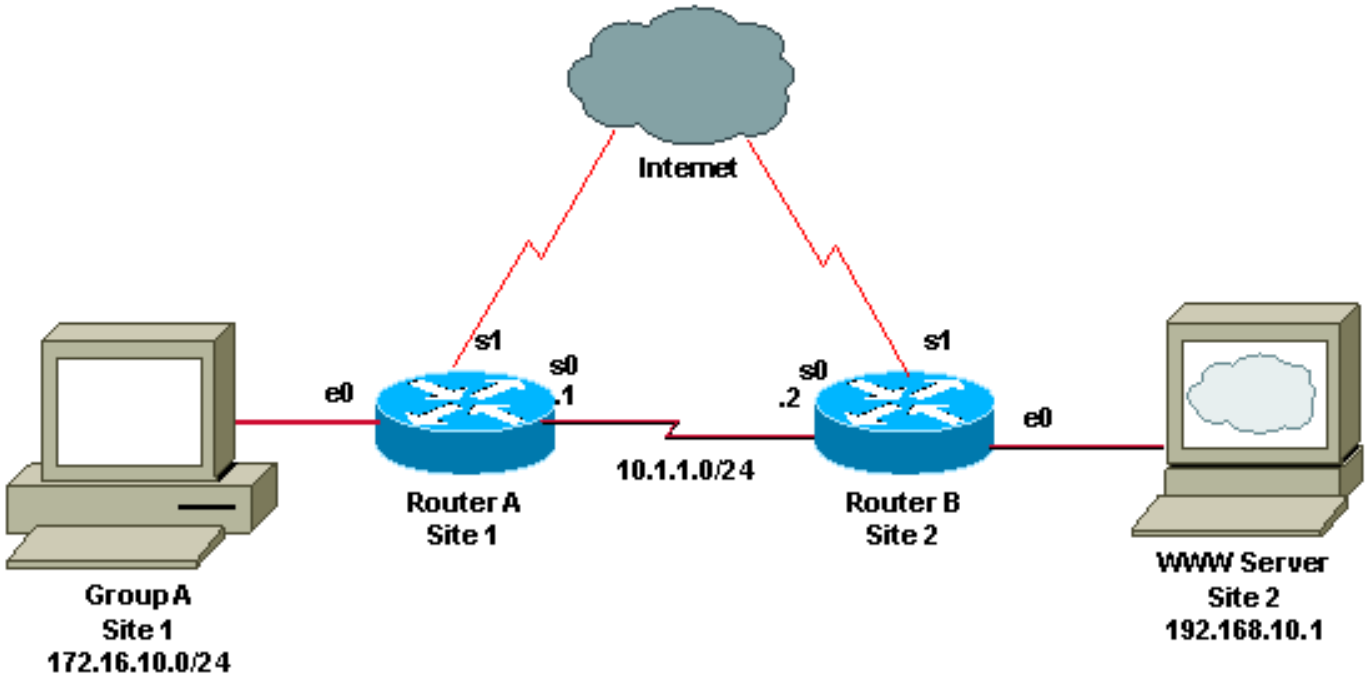
L’administrateur réseau du site 1 achemine les adresses privées affectées au groupe A, de sorte qu’elles utilisent la porte dérobée via l’interface Serial0 (s0) du routeur A lors de l’accès au serveur HTTP du site 2. Le routeur du site 2 dispose d’une route statique vers 172.16.10.0, de sorte que le trafic de retour vers le groupe A est également acheminé par la porte dérobée. Tout autre trafic est traité par NAT et routé via Internet. Dans ce scénario, l’administrateur réseau doit décider quelle application ou quel flux va fonctionner si les paquets sont fragmentés. Il n'est pas possible de faire fonctionner simultanément les flux HTTP et FTP (File Transfer Protocol), car l'un ou l'autre se brise.

Reportez-vous à l'organigramme des règles de liste de contrôle d'accès et aux sections Comment les paquets peuvent correspondre à une liste de contrôle d'accès lorsque vous suivez le scénario.

Explication des options de l'administrateur réseau

Dans l'exemple suivant, la carte de route appelée FOO sur le routeur A envoie des paquets correspondant à la liste de contrôle d'accès 100 au routeur B via s0. Tous les paquets qui ne correspondent pas sont traités par NAT et empruntent la route par défaut via Internet.

Remarque : si un paquet tombe en bas de la liste de contrôle d'accès ou est refusé par celle-ci, il n'est pas routé par une stratégie.



Voici une configuration partielle du routeur A, montrant qu'une route-map de stratégie appelée FOO est appliquée à l'interface e0, où le trafic du groupe A entre dans le routeur :

```
hostname Router_A
int e0
ip policy route-map FOO
route-map FOO permit 10
match ip address 100
set ip next-hop 10.1.1.2

access-list 100 permit tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 eq 80
access-list 100 deny ip any any
```

La liste de contrôle d'accès 100 autorise le routage de stratégie sur les fragments initiaux, non-fragments et non initiaux de flux HTTP vers le serveur. Les flux HTTP initiaux et non fragmentés vers le serveur sont autorisés par la liste de contrôle d'accès et la stratégie routées car ils correspondent aux informations des couches 3 et 4 de la première ligne de liste de contrôle d'accès. Les fragments non initiaux sont autorisés par la liste de contrôle d'accès et la politique routée, car les informations de couche 3 du paquet correspondent également à la première ligne de la liste de contrôle d'accès ; la logique de la liste de contrôle d'accès suppose que les informations de couche 4 du paquet correspondent également si elles étaient disponibles.

Remarque : la liste de contrôle d'accès 100 casse d'autres types de flux TCP fragmentés entre le groupe A et le serveur, car les fragments initiaux et non initiaux parviennent au serveur via

différents chemins ; les fragments initiaux sont traités par NAT et routés via Internet, mais les fragments non initiaux du même flux sont routés par la stratégie.

Un flux FTP fragmenté illustre le problème dans ce scénario. Les fragments initiaux d'un flux FTP correspondent aux informations de couche 3, mais pas aux informations de couche 4, de la première ligne de liste de contrôle d'accès, et ils sont ensuite refusés par la deuxième ligne. Ces paquets sont traités par NAT et routés via Internet.

Les fragments non initiaux d'un flux FTP correspondent aux informations de couche 3 de la première ligne de liste de contrôle d'accès, et la logique de liste de contrôle d'accès suppose une correspondance positive sur les informations de couche 4. Ces paquets sont routés par des politiques, et l'hôte qui les réassemble ne reconnaît pas les fragments initiaux comme faisant partie du même flux que les fragments non initiaux routés par des politiques, car NAT a modifié l'adresse source des fragments initiaux.

La liste de contrôle d'accès 100 dans la configuration ci-dessous corrige le problème FTP. La première ligne de la liste de contrôle d'accès 100 refuse les fragments FTP initiaux et non initiaux du groupe A au serveur.

```
hostname Router_A

int e0
ip policy route-map FOO
route-map FOO permit 10
match ip address 100
set ip next-hop 10.1.1.2

access-list 100 deny tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 fragments
access-list 100 permit tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 eq 80
access-list 100 deny ip any any
```

Les fragments initiaux correspondent aux informations de couche 3 dans la première ligne de liste de contrôle d'accès, mais la présence du mot clé **fragments** entraîne le traitement de la ligne de liste de contrôle d'accès suivante. Le fragment initial ne correspond pas à la deuxième ligne de la liste de contrôle d'accès pour les informations de couche 4. La ligne implicite suivante de la liste de contrôle d'accès est donc traitée, ce qui refuse le paquet. Les fragments non initiaux correspondent aux informations de couche 3 de la première ligne de la liste de contrôle d'accès, de sorte qu'ils sont refusés. Les fragments initiaux et non initiaux sont traités par NAT et routés via Internet, de sorte que le serveur n'a aucun problème de réassemblage.

La correction des flux FTP casse les flux HTTP fragmentés car les fragments HTTP initiaux sont maintenant routés par la stratégie, mais les fragments non initiaux sont traités par NAT et routés via Internet.

Lorsqu'un fragment initial d'un flux HTTP du groupe A au serveur rencontre la première ligne de la liste de contrôle d'accès, il correspond aux informations de couche 3 de la liste de contrôle d'accès, mais en raison du mot clé **fragments**, la ligne suivante de la liste de contrôle d'accès est traitée. La deuxième ligne de la liste de contrôle d'accès autorise et achemine le paquet vers le serveur.

Lorsque des fragments HTTP non initiaux destinés du groupe A au serveur rencontrent la première ligne de la liste de contrôle d'accès, les informations de couche 3 du paquet correspondent à la ligne de la liste de contrôle d'accès et le paquet est refusé. Ces paquets sont

traités par NAT et traversent Internet pour accéder au serveur.

La première liste de contrôle d’accès de ce scénario autorise les flux HTTP fragmentés et rompt les flux FTP fragmentés. La deuxième liste de contrôle d’accès autorise les flux FTP fragmentés et rompt les flux HTTP fragmentés. Dans chaque cas, les flux TCP sont interrompus car les fragments initiaux et non initiaux empruntent des chemins différents vers le serveur. Le réassemblage n'est pas possible, car NAT a modifié l'adresse source des fragments non initiaux.

Il n’est pas possible de construire une liste de contrôle d’accès qui autorise les deux types de flux fragmentés vers le serveur. L’administrateur réseau doit donc choisir le flux qu’il souhaite utiliser.

Informations connexes

- Page de support pour le routage IP
- Support et documentation techniques - Cisco Systems