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.

RFC 1858 couvre des considérations liées à la sécurité pour le fragment IP filtrant et met en valeur deux attaques sur les hôtes qui impliquent des fragments IP des paquets TCP, de l'attaque par fragments minuscule et de l'attaque par fragments superposante. Le blocage de ces attaques est desirable parce qu'elles peuvent compromettre un hôte, ou attachent toutes ses ressources internes.

RFC 1858 décrit également deux méthodes de défense contre ces attaques, le direct et l'indirect. Dans la méthode directe, des fragments initiaux qui sont plus petits qu'une longueur minimale sont jetés. La méthode indirecte implique de jeter le deuxième fragment d'un positionnement de fragment, si elle engage 8 octets dans le datagramme IP d'origine. Veuillez voir le RFC 1858 pour plus de détails.

Traditionnellement, des filtres de paquet comme ACLs sont appliqués aux non-fragments et au fragment initial d'un paquet IP parce qu'ils contiennent les deux couche 3 et les informations 4 que l'ACLs peut s'assortir contre pour une autorisation ou refuser à décision. On permet traditionnellement des fragments non initiaux par l'ACL parce qu'ils peuvent être bloqués ont basé sur les informations de la couche 3 dans les paquets ; cependant, parce que ces paquets ne contiennent pas les informations de la couche 4, ils n'apparient pas les informations de la couche 4 dans le rubrique de liste ACL, s'il existe. Permettre les fragments non initiaux d'un datagramme IP est acceptable parce que l'hôte recevant les fragments ne peut pas rassembler le datagramme IP d'origine sans fragment initial.

Des Pare-feu peuvent également être utilisés pour bloquer des paquets en mettant à jour une table des fragments de paquet répertoriés par source et adresse IP de destination, protocole, et ID

IP. Le Pare-feu de Cisco PIX et le Pare-feu de Cisco IOS® peuvent filtrer tous les fragments d'un flux particulier en mettant à jour cette table des informations, mais il est trop cher de faire ceci sur un routeur pour la fonctionnalité d'ACL de base. Le rôle principal d'un Pare-feu est de bloquer des paquets, et son rôle secondaire est de conduire des paquets ; le rôle principal d'un routeur est de conduire des paquets, et son rôle secondaire est de les bloquer.

Deux changements ont été faits des versions du logiciel Cisco IOS 12.1(2) et 12.0(11) pour aborder quelques problèmes de sécurité entourant le TCP fragmente. La méthode indirecte, comme décrit dans RFC 1858 , a été appliquée en tant qu'élément de vérifier standard de validité de paquet en entrée TCP/IP. Des modifications ont été également apportées à la fonctionnalité d'ACL en ce qui concerne des fragments non initiaux.

Types de rubriques de liste ACL

Il y a six types différents de lignes d'ACL, et chacun a une conséquence si un paquet fait ou ne s'assortit pas. Dans la liste suivante, la FO = 0 indique un non-fragment ou un fragment initial dans un écoulement de TCP, la FO > 0 indique que le paquet est un fragment non initial, L3 signifie la couche 3, et L4 signifie la couche 4.

Remarque: Quand il y a à la fois les informations des couches 3 et 4 dans la ligne d'ACL et le mot clé de **fragments** est présent, l'action d'ACL est conservatrice pour l'autorisation et refuse des actions. Les actions sont conservatrices parce que vous ne voulez pas refuser accidentellement une partie fragmentée d'un écoulement parce que les fragments ne contiennent pas les informations suffisantes pour apparier tous les attributs de filtre. Dans le cas de refuser, au lieu de refuser un fragment non initial, le prochain rubrique de liste ACL est traité. Dans le cas d'autorisation, on le suppose que les informations de la couche 4 dans le paquet, si disponibles, apparient les informations de la couche 4 dans la ligne d'ACL.

Ligne d'ACL d'autorisation avec les informations L3 seulement

1. Si les informations L3 d'un paquet apparient les informations L3 dans la ligne d'ACL, on leur permet.
2. Si les informations L3 d'un paquet n'apparient pas les informations L3 dans la ligne d'ACL, le prochain rubrique de liste ACL est traité.

Refusez la ligne d'ACL avec les informations L3 seulement

1. Si les informations L3 d'un paquet apparient les informations L3 dans la ligne d'ACL, on lui refuse.
2. Si les informations L3 d'un paquet n'apparient pas les informations L3 dans la ligne d'ACL, le prochain rubrique de liste ACL est traité.

Permettez la ligne d'ACL avec les informations L3 seulement, et le mot clé de fragments est présent

Si les informations L3 d'un paquet apparient les informations L3 dans la ligne d'ACL, le décalage de fragment du paquet est vérifié.

1. Si on permet un paquet FO > 0, le paquet.

2. Si un paquet FO = 0, le prochain rubrique de liste ACL est traité.

Refusez la ligne d'ACL avec les informations L3 seulement, et le mot clé de fragments est présent

Si les informations L3 d'un paquet apparient les informations L3 dans la ligne d'ACL, le décalage de fragment du paquet est vérifié.

1. Si un paquet FO > 0, le paquet est refusé.
2. Si un paquet FO = 0, la prochaine ligne d'ACL est traité.

Ligne d'ACL d'autorisation avec les informations L3 et L4

1. Si d'un paquet les informations le L3 et le L4 apparient la ligne d'ACL et la FO = 0, on permet le paquet.
2. Si les informations L3 d'un paquet apparient la ligne d'ACL et la FO > 0, on permet le paquet.

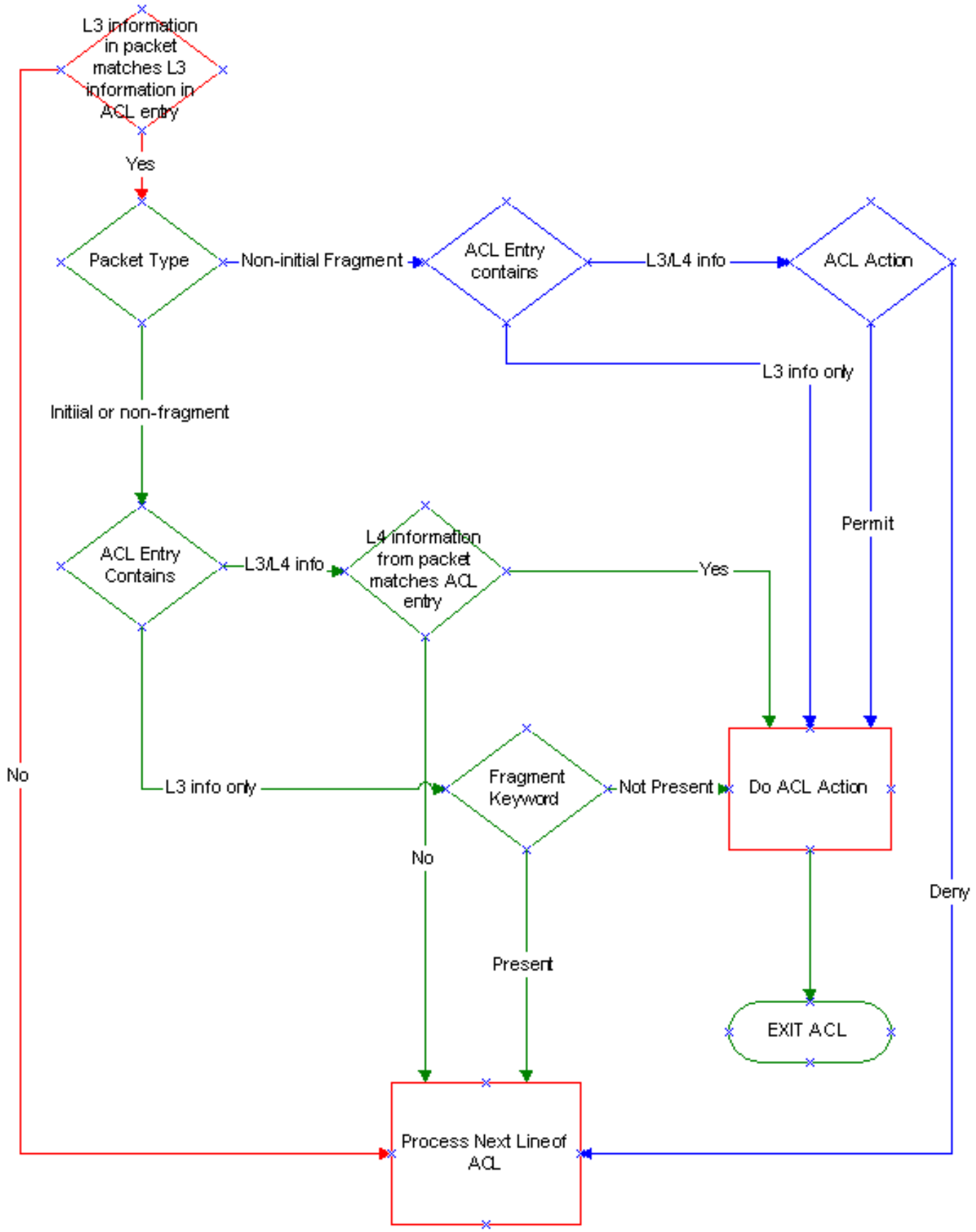
Refusez la ligne d'ACL avec les informations L3 et L4

1. Si d'un paquet les informations le L3 et le L4 apparient le rubrique de liste ACL et la FO = 0, le paquet est refusé.
2. Si les informations L3 d'un paquet apparient la ligne d'ACL et la FO > 0, le prochain rubrique de liste ACL est traité.

Organigramme de règles d'ACL

L'organigramme suivant montre les règles d'ACL quand des non-fragments, les fragments initiaux, et les fragments non initiaux sont vérifiés contre l'ACL.

Remarque: Les fragments non initiaux eux-mêmes contiennent seulement la couche 3, ne posent jamais les informations 4, bien que l'ACL puisse contenir le à la fois les informations des couches 3 et 4.



Comment les paquets peuvent apparier un ACL

Exemple 1

Les cinq scénarios possibles suivants impliquent différents types de paquets rencontrant l'ACL

100. Veuillez se référer à la table et à l'organigramme comme vous suivez ce qui se produit dans chaque situation. L'adresse IP du web server 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 pour le serveur sur le port 80 :

La première ligne de l'ACL contient le à la fois les informations des couches 3 et 4, qui apparie l'informations des couches 3 et 4 dans le paquet, ainsi on permet le paquet.

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

1. La première ligne de l'ACL contient le à la fois les informations des couches 3 et 4, mais les informations de la couche 4 dans l'ACL n'apparient pas le paquet, ainsi la prochaine ligne d'ACL est traitée.
2. La deuxième ligne de l'ACL refuse tous les paquets, ainsi le paquet est refusé.

Le paquet est un fragment non initial au serveur dans un écoulement du port 80 :

La première ligne de l'ACL contient l'informations des couches 3 et 4, les informations de la couche 3 dans l'ACL apparient le paquet, et l'action d'ACL est de laisser, ainsi le paquet est permis.

Le paquet est un fragment non initial au serveur dans un écoulement du port 21 :

La première ligne de l'ACL contient le à la fois les informations des couches 3 et 4. Les informations de la couche 3 dans l'ACL apparient le paquet, il n'y a aucune informations de la couche 4 dans le paquet, et l'action d'ACL est de laisser, ainsi le paquet est permis.

Le paquet est un fragment initial, un non-fragment ou un fragment non initial à un autre hôte sur le sous-réseau du serveur :

1. La première ligne de l'ACL contient les informations de la couche 3 qui n'apparient pas les informations de la couche 3 dans le paquet (l'adresse de destination), ainsi la prochaine ligne d'ACL est traitée.
2. La deuxième ligne de l'ACL refuse tous les paquets, ainsi le paquet est refusé.

Exemple 2

Ce qui suit les mêmes cinq scénarios possibles implique différents types de paquets rencontrant l'ACL 101. Référez-vous de nouveau, s'il vous plaît à la table et à l'organigramme comme vous suivez ce qui se produit dans chaque situation. L'adresse IP du web server 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 pour le serveur sur le port 80 :

1. La première ligne de l'ACL contient les informations de la couche 3 qui apparient les

informations de la couche 3 dans le paquet. L'action d'ACL est de refuser, mais parce que le mot clé de **fragments** est présent, le prochain rubrique de liste ACL est traité.
2. La deuxième ligne de l'ACL contient l'informations des couches 3 et 4, qui apparie le paquet, ainsi on permet le paquet.

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

1. La première ligne de l'ACL contient les informations de la couche 3, qui apparient le paquet, mais le rubrique de liste ACL a également le mot clé de **fragments**, qui n'apparie pas le paquet parce que FO = 0, ainsi le prochain rubrique de liste ACL est traité.
2. La deuxième ligne de l'ACL contient l'informations des couches 3 et 4. Dans ce cas, les informations de la couche 4 ne s'assortissent pas, ainsi le prochain rubrique de liste ACL est traité.
3. La troisième ligne de l'ACL refuse tous les paquets, ainsi le paquet est refusé

Le paquet est un fragment non initial au serveur dans un écoulement du port 80 :

La première ligne de l'ACL contient les informations de la couche 3 qui apparient les informations de la couche 3 dans le paquet. Souvenez-vous que quoique ce fasse partie d'un écoulement du port 80, il n'y a aucune informations de la couche 4 dans le fragment non initial. Le paquet est refusé parce que la couche 3 correspondances de l'information.

Le paquet est un fragment non initial au serveur dans un écoulement du port 21 :

La première ligne de l'ACL contient les informations de la couche 3 seulement, et elle apparie le paquet, ainsi le paquet est refusé.

Le paquet est un fragment initial, un non-fragment ou un fragment non initial à un autre hôte sur le sous-réseau du serveur :

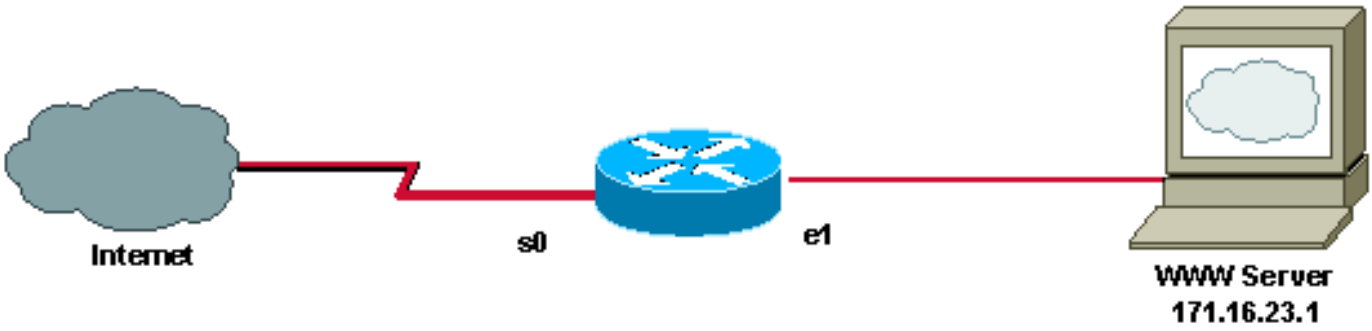
1. La première ligne de l'ACL contient les informations de la couche 3 seulement, et elle n'apparie pas le paquet, ainsi la prochaine ligne d'ACL est traitée.
2. La deuxième ligne de l'ACL contient l'informations des couches 3 et 4. Les informations de la couche 4 et de la couche 3 dans le paquet n'apparient pas cela de l'ACL, ainsi la prochaine ligne d'ACL est traitée.
3. La troisième ligne de l'ACL refuse ce paquet

scénarios de mot clé de fragments

Scénario 1

Le routeur B se connecte à un web server, et l'administrateur réseau ne veut pas ne permettre à aucun fragment pour atteindre le serveur. Ce scénario affiche ce qui se produit si l'administrateur réseau implémente l'ACL 100 contre l'ACL 101. L'ACL est d'arrivée appliqué sur l'interface des Routeurs Serial0 (s0) et devrait permettre seulement aux paquets non-fragmentés pour atteindre le web server. Voyez l'organigramme de règles d'ACL et le comment les paquets peuvent apparier des sections d'ACL pendant que vous suivez le scénario.

Conséquences d'utiliser le mot clé de fragments



Ce qui suit est l'ACL 100 :

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

La première ligne de l'ACL 100 permet seulement le HTTP au serveur, mais elle permet également des fragments non initiaux à n'importe quel port TCP sur le serveur. Il permet ces paquets parce que les fragments non initiaux ne contiennent pas les informations de la couche 4, et la logique d'ACL suppose que si les correspondances de l'information de la couche 3, puis les informations de la couche 4 s'assortiraient également, si elles étaient disponibles. La deuxième ligne est implicite et refuse tout autre trafic.

Il est important de noter que, en date des versions du logiciel Cisco IOS 12.1(2) et 12.0(11), le nouveau code d'ACL relâche les fragments qui ne font pas match any l'autre ligne dans l'ACL. Les versions antérieures permettent des fragments non initiaux si elles ne font pas match any l'autre ligne de l'ACL.

Ce qui suit est l'ACL 101 :

```
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
```

L'ACL 101 ne permet pas des fragments non initiaux au serveur en raison de la première ligne. Un fragment non initial au serveur est refusé quand il rencontre la première ligne d'ACL parce que les informations de la couche 3 dans le paquet apparient les informations de la couche 3 dans la ligne d'ACL.

L'initiale ou les non-fragments au port 80 sur le serveur apparient également la première ligne de l'ACL pour les informations de la couche 3, mais parce que le mot clé de fragments est présent, le prochain rubrique de liste ACL (la deuxième ligne) est traité. La deuxième ligne de l'ACL permet l'initiale ou les non-fragments parce qu'ils apparient la ligne d'ACL pour l'informations des couches 3 et 4.

Des fragments non initiaux destinés aux ports TCP d'autres hôtes sur le réseau de 171.16.23.0 sont bloqués par cet ACL. Les informations de la couche 3 en ces paquets n'apparient pas les informations de la couche 3 dans la première ligne d'ACL, ainsi la prochaine ligne d'ACL est traitée. Les informations de la couche 3 en ces paquets n'apparient pas les informations de la couche 3 dans la deuxième ligne d'ACL l'un ou l'autre, ainsi la troisième ligne d'ACL est traitée. La troisième ligne est implicite et refuse tout le trafic.

L'administrateur réseau dans ce scénario décide d'implémenter l'ACL 101 parce qu'il permet seulement des écoulements non-fragmentés de HTTP au serveur.

Scénario 2

Un client a la connexion Internet à deux sites différents, et il y a également une connexion secrète entre les deux sites. La stratégie de l'administrateur réseau est de laisser le groupe A dans le site 1 pour accéder au serveur HTTP au site 2. Les Routeurs aux deux sites emploient les adresses privées (RFC 1918) et le Traduction d'adresses de réseau (NAT) pour traduire les paquets qui sont conduits par l'Internet.

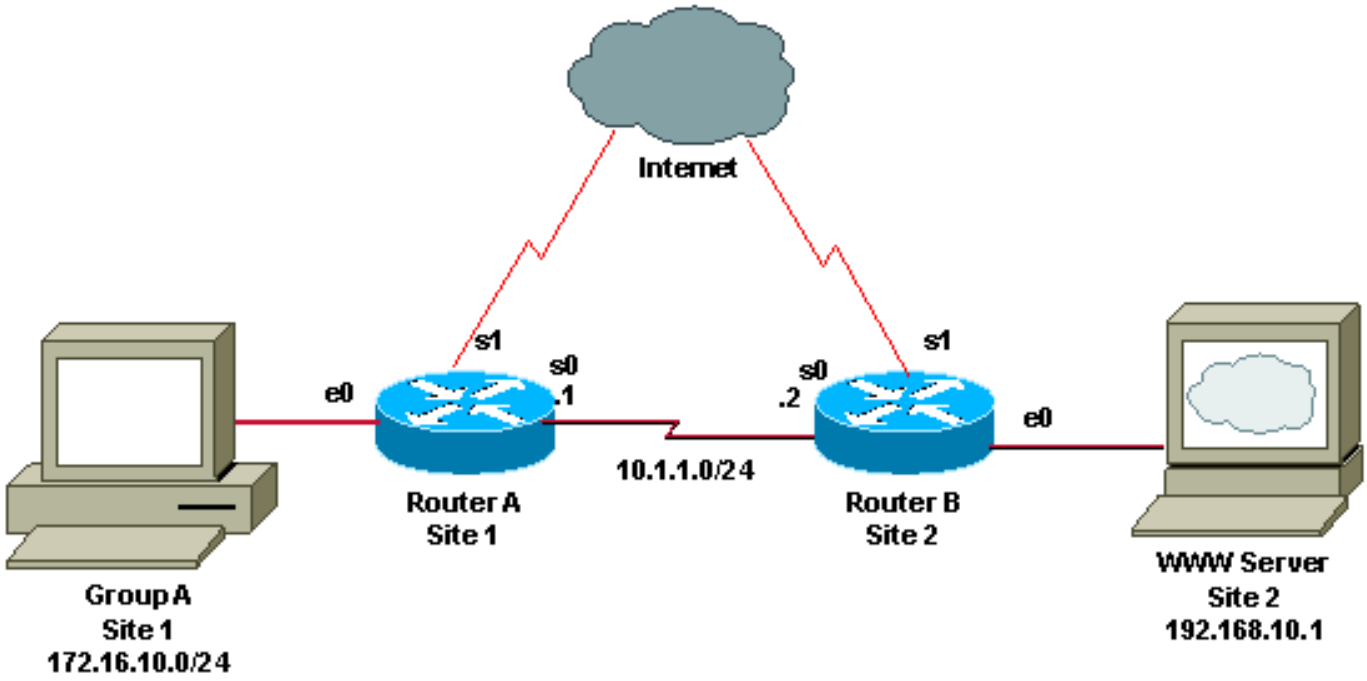
L'administrateur réseau au site 1 est stratégie-routage les adresses privées assignées pour grouper A, de sorte qu'ils utilisent la porte dérobée par Serial0 du routeur A (s0) en accédant au serveur HTTP au site 2. Le routeur au site 2 a une artère statique à 172.16.10.0, de sorte que de retour trafiquiez pour grouper A soit également conduit par la porte dérobée. Tout autre trafic est traité par NAT et conduit par l'Internet. L'administrateur réseau dans ce scénario doit décider quelle application ou écoulement va fonctionner si les paquets sont fragmentés. Il n'est pas possible de faire le HTTP et le travail d'écoulements de Protocole FTP (File Transfer Protocol) en même temps parce qu'on ou l'autre se casse.

Voyez l'organigramme de règles d'ACL et le comment les paquets peuvent apparier des sections d'ACL pendant que vous suivez le scénario.

Explication des options de l'administrateur réseau

Dans l'exemple suivant, le mappage de route appelé le FOO sur le routeur A envoie les paquets qui apparient l'ACL 100 à travers au routeur B à s0. Tous les paquets qui ne s'assortissent pas sont traités par NAT et prendre le default route par l'Internet.

Remarque: Si un paquet tombe le bas de l'ACL, ou est refusé par lui, alors il stratégie-n'est pas conduit.



Ce qui suit est une configuration de routeur partielle A, prouvant qu'un route-map de stratégie appelé le FOO est appliqué pour relier e0, où le trafic du groupe A présente 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
```

L'ACL 100 permet à routage de stratégie sur des les deux l'initiale, des non-fragments et les fragments non initiaux du HTTP circule au serveur. On permet l'initiale et les non-fragments des écoulements de HTTP au serveur par l'ACL et la stratégie conduit parce qu'elles apparient l'informations des couches 3 et 4 dans la première ligne d'ACL. On permet des fragments non initiaux par l'ACL et la stratégie conduits parce que les informations de la couche 3 dans le paquet apparient également la première ligne d'ACL ; la logique d'ACL suppose que les informations de la couche 4 dans le paquet s'assortiraient également si elles étaient disponibles.

Remarque: L'ACL 100 casse d'autres types d'écoulements fragmentés de TCP entre le groupe A et le serveur parce que l'initiale et les fragments non initiaux arrivent au serveur par des différents chemins ; les fragments initiaux sont traités par NAT et conduits par l'Internet, mais les fragments non initiaux du même écoulement sont stratégie conduits.

Les aides fragmentées d'un flux FTP illustrent le problème dans ce scénario. Les fragments initiaux d'une correspondance de flux FTP les informations de la couche 3, mais pas les informations de la couche 4, de la première ligne d'ACL, et eux sont ultérieurement refusés par la deuxième ligne. Ces paquets sont traités par NAT et conduits par l'Internet.

Les fragments non initiaux d'une correspondance de flux FTP les informations de la couche 3 dans la première ligne d'ACL, et la logique d'ACL assume une correspondance positive sur les informations de la couche 4. Ces paquets sont stratégie conduits, et l'hôte rassemblant ces paquets n'identifie pas les fragments initiaux en tant qu'élément du même écoulement que les fragments non initiaux stratégie-conduits parce que NAT a changé l'adresse source des fragments initiaux.

L'ACL 100 dans la configuration ci-dessous répare le problème de FTP. La première ligne de l'ACL 100 refuse les deux l'initiale et le FTP de non-initiale fragmente 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 s'assortissent sur les informations de la couche 3 dans la première ligne d'ACL, mais la présence du mot clé de **fragments** cause la prochaine ligne d'ACL d'être traitée. Le fragment initial n'apparie pas la deuxième ligne d'ACL pour les informations de la couche 4, et ainsi la prochaine ligne implicite de l'ACL est traitée, qui refuse le paquet. Les fragments non initiaux apparient les informations de la couche 3 dans la première ligne de l'ACL, ainsi ils sont refusés. Chacun des deux parafent et des fragments non initiaux sont traités par NAT et conduits par l'Internet, ainsi le serveur n'a aucun problème avec le réassemblage.

Réparer le HTTP fragmenté par ruptures de flux FTP circule parce que les fragments HTTP initiaux sont maintenant stratégie conduits, mais les fragments non initiaux sont traités par NAT et conduits par l'Internet.

Quand un fragment initial d'un écoulement de HTTP du groupe A au serveur rencontre la première ligne de l'ACL, il s'assortit sur les informations de la couche 3 dans l'ACL, mais en raison du mot clé de **fragments**, la prochaine ligne de l'ACL est traitée. La deuxième ligne des autorisations et de la stratégie d'ACL conduit le paquet au serveur.

Quand les fragments HTTP de non-initiale ont destiné du groupe A au serveur rencontre la

première ligne de l'ACL, les informations de la couche 3 dans le paquet apparient la ligne d'ACL et le paquet est refusé. Ces paquets sont traités par NAT et traversent l'Internet pour arriver au serveur.

Le premier ACL dans ce scénario permet des écoulements fragmentés de HTTP et casse les flux FTP fragmentés. Le deuxième ACL permet les flux FTP fragmentés et casse des écoulements fragmentés de HTTP. Les écoulements de TCP enfoncent chaque cas parce que l'initiale et les fragments non initiaux prennent des différents chemins au serveur. Le réassemblage n'est pas possible parce que NAT a changé l'adresse source des fragments non initiaux.

Il n'est pas possible de construire un ACL qui permet les deux genres d'écoulements fragmentés au serveur, ainsi l'administrateur réseau doit choisir qui le circulent veulent fonctionner.

Informations connexes

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