ASA 8.2 : Le paquet traversent un Pare-feu ASA

Contenu

Introduction

Ce document décrit le paquet traversent un Pare-feu de l'appliance de sécurité adaptable Cisco (ASA). Il affiche que la procédure de Cisco ASA traitait les paquets internes. Il discute également des différentes possibilités où le paquet pourrait décrocher et différentes situations où le paquet progresse en avant.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de la gamme Cisco 5500 ASA.

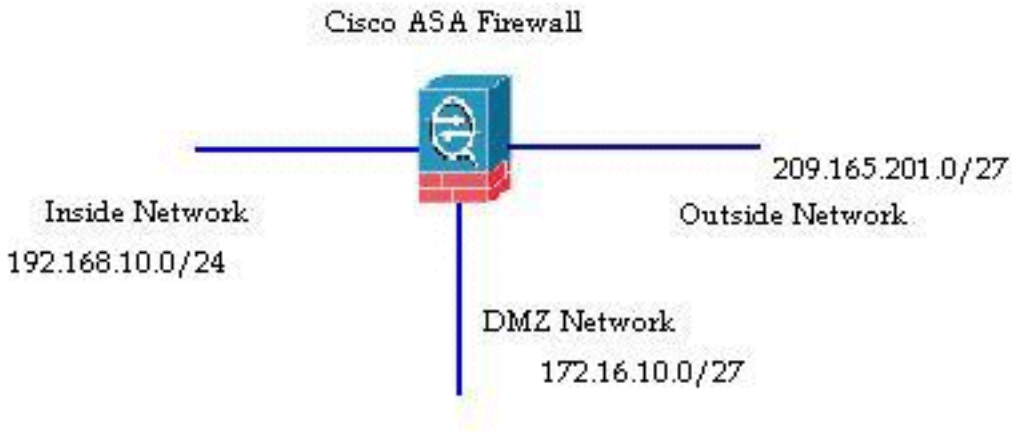
[Composants utilisés](#)

Les informations dans ce document sont basées sur la gamme ASA de Cisco ASA 5500 qui exécutent la version de logiciel 8.2.

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.

Informations générales

L'interface qui reçoit le paquet s'appelle l'**interface d'entrée** et l'interface par lesquelles les sorties de paquet s'appelle l'**interface de sortie**. Quand vous vous référez au paquet traversez n'importe quel périphérique, la tâche est facilement simplifié si vous la regardez en termes de ces deux interfaces. Voici un exemple de scénario :



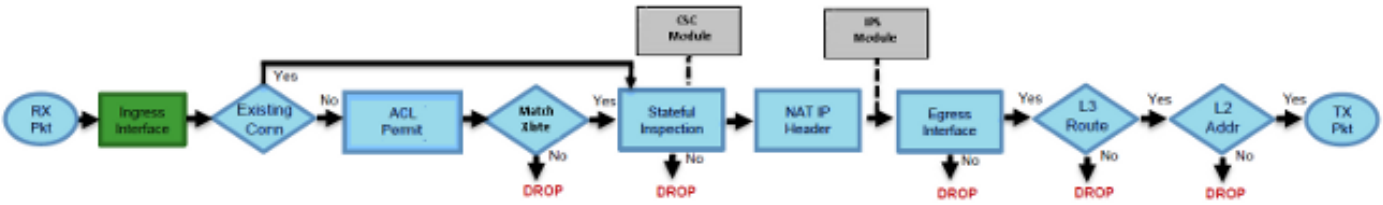
Quand les tentatives intérieures d'un utilisateur (192.168.10.5) d'accéder à un web server dans le réseau de la zone démilitarisée (DMZ) (172.16.10.5), l'écoulement de paquet ressemble à ceci :

- Adresse source - 192.168.10.5
- Port de source - 22966
- Adresse de destination - 172.16.10.5
- Destination port - 8080
- Interface d'entrée - À l'intérieur
- Interface de sortie - DMZ
- Protocol l'a utilisé - TCP (Transmission Control Protocol)

Après que vous déterminiez les détails du paquet circulent comme décrit ici, il est facile de localiser la question dans cette entrée spécifique de connexion.

Algorithme de processus de paquet de Cisco ASA

Voici un diagramme de la façon dont Cisco ASA traite le paquet qu'il reçoit :



Voici les différentes étapes en détail :

1. Le paquet est atteint à l'interface d'entrée.
2. Une fois que le paquet atteint la mémoire tampon interne de l'interface, l'entrée contre- de

l'interface est incrémentée par on.

3. Cisco ASA regarde d'abord ses détails internes de table de connexion afin de vérifier si c'est une connexion en cours. Si l'écoulement de paquet apparie une connexion en cours, alors le contrôle de liste de contrôle d'accès (ACL) est sauté et le paquet est fait avancer.Si l'écoulement de paquet n'apparie pas une connexion en cours, alors l'état de TCP est vérifié. Si c'est un paquet de synchronisation ou paquet d'UDP (User Datagram Protocol), alors le compteur de connexion est incrémenté par on et le paquet est envoyé pour un contrôle d'ACL. Si ce n'est pas un paquet de synchronisation, le paquet est lâché et l'événement est enregistré.
4. Le paquet est traité selon l'interface ACLs. Il est vérifié dans la commande séquentielle des rubriques de liste ACL et s'il apparie les rubriques de liste ACL l'uns des, il avance. Autrement, le paquet est lâché et les informations sont enregistré. Le nombre de hits d'ACL est incrémenté par on quand le paquet apparie le rubrique de liste ACL.
5. Le paquet est vérifié pour assurer les Règles de traduction. Si un paquet traverse ce contrôle, alors une entrée de connexion est créée pour cet écoulement et le paquet avance. Autrement, le paquet est lâché et les informations sont enregistré.
6. Le paquet est soumis à un contrôle d'inspection. Cette inspection vérifie si cet écoulement spécifique de paquet est conformément au protocole. Cisco ASA a une engine intégrée d'inspection qui examine chaque connexion selon son ensemble prédéfini de fonctionnalité de niveau application. S'il passait l'inspection, il est fait avancer. Autrement, le paquet est lâché et les informations sont enregistré.Des contrôles de Sécurité supplémentaires seront mis en application si un module de la sécurité du contenu (CSC) est impliqué.
7. Les informations d'en-tête IP sont traduites selon la règle de la translation d'adresses d'adresse du port de translation d'adresses d'adresse réseau (NAT/PAT) et des sommes de contrôle sont mises à jour en conséquence. Le paquet est expédié à l'Advanced Inspection and Prevention Security Services Module (AIP SSM) pour les contrôles de Sécurité associés par IPS quand le module AIP est impliqué.
8. Le paquet est expédié à l'interface de sortie basée sur les Règles de traduction. Si aucune interface de sortie n'est spécifiée dans la règle de conversion, alors l'interface de destination est décidée a basé sur la recherche de route globale.
9. Sur l'interface de sortie, la recherche de route d'interface est effectuée. Souvenez-vous, l'interface de sortie est déterminé par la règle de conversion qui prend la priorité.
10. Une fois une artère de la couche 3 a été trouvée et le prochain saut identifié, posent 2 que la résolution est exécutée. La réécriture de la couche 2 de l'en-tête MAC se produit à ce stade.
11. Le paquet est transmis sur le fil, et les compteurs d'interface incrémentent sur l'interface de sortie.

Explication de NAT

Référez-vous à ces documents pour plus de détails sur l'ordre de l'exécution NAT :

- Version de logiciel 8.2 de Cisco ASA et plus tôt
- Version de logiciel 8.3 de Cisco ASA et plus tard

Commandes show

Voici quelques commandes utiles qui aident à dépister les détails d'écoulement de paquet à

différentes étapes dans le processus :

```
show interface
show conn
show access-list
show xlate
show service-policy inspect
show run static
show run nat
show run global
show nat
show route
show arp
```

Messages de Syslog

Les messages de Syslog fournissent les informations utiles au sujet du traitement de paquets. Voici quelques messages de Syslog d'exemple pour votre référence :

- Message de Syslog quand il n'y a aucune entrée de connexion :`%ASA-6-106015: Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name`
- Message de Syslog quand le paquet est refusé par un ACL :`%ASA-4-106023: Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port by access_group acl_ID`
- Message de Syslog quand il y a aucune règle de conversion trouvée :`%ASA-3-305005: No translation group found for protocol src interface_name: source_address/source_port dst interface_name:dest_address/dest_port`
- Message de Syslog quand un paquet est refusé par inspection de Sécurité :`%ASA-4-405104: H225 message received from outside_address/outside_port to inside_address/inside_port before SETUP`
- Message de Syslog quand il n'y a aucune informations d'artère :`%ASA-6-110003: Routing failed to locate next-hop for protocol from src interface:src IP/src port to dest interface:dest IP/dest port`

Pour une liste complète de tous les messages de Syslog générés par Cisco ASA avec une brève explication, référez-vous aux messages de Syslog de gamme de Cisco ASA.

Informations connexes

- Page de support de Cisco ASA
- Référence de commandes de gamme de Cisco ASA 5500, 8.2
- Guide de configuration de gamme de Cisco ASA 5500, 8.3
- Support et documentation techniques - Cisco Systems