ASA 8.2 : Flux de paquets dans un pare-feu ASA

Table des matières

[Introduction](#)
[Conditions préalables](#)
[Exigences](#)
[Composants utilisés](#)
[Informations générales](#)
[Algorithme de traitement des paquets Cisco ASA](#)
[Explication de la NAT](#)
[Commandes show](#)
[périodiques](#)
[Informations connexes](#)

Introduction

Ce document décrit le flux de paquets à travers un pare-feu Cisco Adaptive Security Appliance (ASA). Elle illustre la procédure Cisco ASA de traitement des paquets internes. Il discute également des différentes possibilités où le paquet pourrait décrocher et différentes situations où le paquet progresse en avant.

Conditions préalables

Exigences

Cisco vous recommande de connaître les ASA de la gamme Cisco 5500.

Composants utilisés

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

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. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

L'interface qui reçoit le paquet est appelée l'interface d'entrée et l'interface par laquelle le paquet sort est appelée l'interface de sortie. Lorsque vous vous référez au flux de paquets à travers n'importe quel périphérique, la tâche est facilement simplifiée si vous l'examinez en termes de ces deux interfaces. Voici un exemple de scénario :

Lorsqu'un utilisateur interne (192.168.10.5) tente d'accéder à un serveur Web dans le réseau de zone démilitarisée (DMZ) (172.16.10.5), le flux de paquets se présente comme suit :

- Adresse source : 192.168.10.5
- Port source - 22966
- Adresse de destination : 172.16.10.5
- Port de destination - 8080
- Interface d'entrée - Interne
- Interface de sortie - DMZ
- Protocole utilisé - TCP (Transmission Control Protocol)

Une fois que vous avez déterminé les détails du flux de paquets comme décrit ici, il est facile d'isoler le problème à cette entrée de connexion spécifique.

Algorithme de traitement des paquets 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 au niveau de l’interface d’entrée.
2. Une fois que le paquet atteint la mémoire tampon interne de l'interface, le compteur d'entrée de l'interface est incrémenté de un.
3. Cisco ASA examine d'abord les détails de sa table de connexion interne afin de vérifier s'il s'agit d'une connexion actuelle. Si le flux de paquets correspond à une connexion en cours, la vérification de la liste de contrôle d'accès (ACL) est ignorée et le paquet est déplacé vers l'avant.

   Si le flux de paquets ne correspond pas à une connexion en cours, l'état TCP est vérifié. S’il s’agit d’un paquet SYN ou UDP (User Datagram Protocol), le compteur de connexion est incrémenté de 1 et le paquet est envoyé pour vérification de la liste de contrôle d’accès. S'il ne s'agit pas d'un paquet SYN, le paquet est abandonné et l'événement est consigné.
4. Le paquet est traité conformément aux listes de contrôle d’accès d’interface. Elle est vérifiée dans l’ordre séquentiel des entrées de la liste de contrôle d’accès et si elle correspond à l’une des entrées de la liste, elle avance. Sinon, le paquet est abandonné et les informations sont consignées. Le nombre de succès de la liste de contrôle d’accès est incrémenté de un lorsque le paquet correspond à l’entrée de la liste.
5. Le paquet est vérifié pour les règles de traduction. Si un paquet passe par cette vérification, une entrée de connexion est créée pour ce flux et le paquet avance. Sinon, le paquet est abandonné et les informations sont consignées.

6. Le paquet est soumis à une vérification d'inspection. Cette inspection vérifie si ce flux de paquets spécifique est ou non conforme au protocole. Cisco ASA dispose d'un moteur d'inspection intégré qui inspecte chaque connexion conformément à son ensemble prédéfini de fonctionnalités au niveau de l'application. S'il a réussi l'inspection, il est avancé. Sinon, le paquet est abandonné et les informations sont consignées.

   Des contrôles de sécurité supplémentaires seront mis en oeuvre si un module CSC (Content Security) est impliqué.

7. Les informations d'en-tête IP sont traduites conformément à la règle NAT/PAT (Network Address Translation/Port Address Translation) et les sommes de contrôle sont mises à jour en conséquence. Le paquet est transmis au module AIP-SSM (Advanced Inspection and Prevention Security Services Module) pour des vérifications de sécurité liées à IPS lorsque le module AIP est impliqué.

8. Le paquet est transmis à l'interface de sortie en fonction des règles de traduction. Si aucune interface de sortie n'est spécifiée dans la règle de traduction, l'interface de destination est décidée en fonction de la recherche de route globale.

9. Sur l'interface de sortie, la recherche de route d'interface est effectuée. N'oubliez pas que l'interface de sortie est déterminée par la règle de traduction qui prend la priorité.

10. Une fois qu'une route de couche 3 a été trouvée et que le saut suivant a été identifié, la résolution de couche 2 est effectuée. La réécriture de couche 2 de l'en-tête MAC se produit à ce stade.

11. Le paquet est transmis sur le câble et les compteurs d'interface s'incrémentent sur l'interface de sortie.

Explication de la NAT

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

- Logiciel Cisco ASA versions 8.2 et antérieures
- Logiciel Cisco ASA versions 8.3 et ultérieures

Commandes show

Voici quelques commandes utiles qui aident à suivre les détails du flux de paquets à différentes étapes du 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
```

périodiques

Les messages Syslog fournissent des informations utiles sur le traitement des paquets. Voici quelques exemples de messages syslog à titre de référence :

- Message Syslog en l'absence d'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 Syslog lorsque le paquet est refusé par une liste de contrôle d’accès :

```
%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 Syslog lorsqu'aucune règle de traduction n'a été 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 Syslog lorsqu'un paquet est refusé par l'inspection de sécurité :

```
%ASA-4-405104: H225 message received from outside_address/outside_port to
 inside_address/inside_port before SETUP
```

- Message Syslog en l'absence d'informations de route :

```
%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 Syslog générés par Cisco ASA avec une brève explication, référez-vous à Messages Syslog de la gamme Cisco ASA.

Informations connexes

- Page d'assistance Cisco ASA
- Référence des commandes de la gamme Cisco ASA 5500, 8.2
- Guide de configuration de la gamme Cisco ASA 5500, 8.3
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.