ASA 8.3 : Établir et dépanner les problèmes de connexion dans le dispositif de sécurité Cisco

Contenu

Introduction

Lorsqu'un appareil de sécurité adaptatif (ASA) Cisco est initialement configuré, il dispose d'une stratégie de sécurité par défaut dans laquelle tout le monde à l'intérieur peut sortir et personne à l'extérieur ne peut entrer. Si votre site nécessite une stratégie de sécurité différente, vous pouvez autoriser des utilisateurs externes à se connecter à votre serveur Web via l'ASA.

Une fois la connectivité de base établie via Cisco ASA, vous pouvez modifier la configuration du pare-feu. Assurez-vous que toutes les modifications de configuration apportées à l'ASA sont conformes à votre stratégie de sécurité de site.

Reportez-vous à la section PIX/ASA : Établir et dépanner la connectivité via l'appliance de sécurité Cisco pour une configuration identique sur Cisco ASA avec les versions 8.2 et antérieures.

Conditions préalables

Conditions requises

Ce document suppose que certaines configurations de base ont déjà été effectuées sur Cisco ASA. Référez-vous à ces documents pour des exemples de configuration initiale d'ASA :

- ASA 8.3(x) : Connexion d'un seul réseau interne à Internet
- Configuration du client PPPoE sur un dispositif de sécurité adaptatif Cisco (ASA)

Components Used

Les informations de ce document sont basées sur un appareil de sécurité adaptatif (ASA) Cisco qui exécute les versions 8.3 et ultérieures.

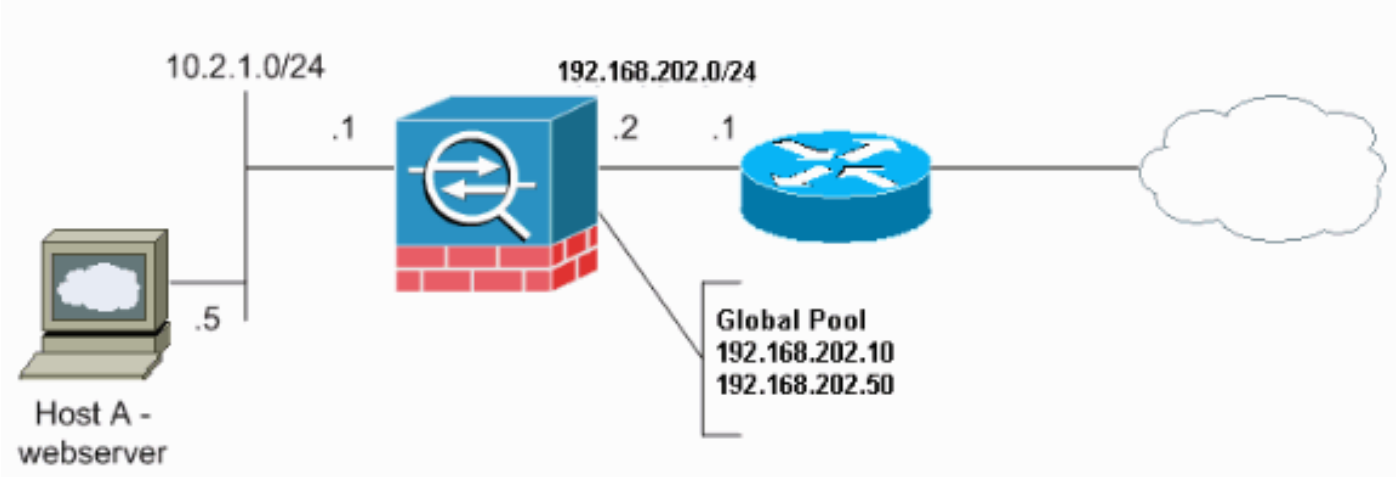
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Fonctionnement de la connectivité via l'ASA

Dans ce réseau, l'hôte A est le serveur Web dont l'adresse interne est 10.2.1.5. Une adresse externe (traduite) 192.168.202.5 est attribuée au serveur Web. Les utilisateurs Internet doivent pointer vers 192.168.202.5 pour accéder au serveur Web. L'entrée DNS de votre serveur Web doit être cette adresse. Aucune autre connexion n'est autorisée à partir d'Internet.



Remarque : les schémas d'adressage IP utilisés dans cette configuration ne sont pas routables légalement sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisés dans un environnement de laboratoire.

Configuration de la connectivité via Cisco ASA

Complétez ces étapes afin de configurer la connectivité via l'ASA :

1. Créez un objet réseau qui définit le sous-réseau interne et un autre objet réseau pour la plage du pool d'adresses IP. Configurez la NAT à l'aide des objets réseau suivants :

```
object network inside-net
subnet 0.0.0.0 0.0.0.0
object network outside-pat-pool
range 192.168.202.10 192.168.202.50
nat (inside,outside) source dynamic inside-net  outside-pat-pool
```

2. Attribuez une adresse traduite statique à l'hôte interne auquel les utilisateurs d'Internet ont accès.

```
object network obj-10.2.1.5
  host 10.2.1.5
  nat (inside,outside) static 192.168.202.5
```

3. Utilisez la commande **access-list** pour autoriser les utilisateurs externes via Cisco ASA. Toujours utiliser l'adresse traduite dans la commande **access-list**.

```
access-list 101 permit tcp any host 192.168.202.5 eq www
  access-group 101 in interface outside
```

Autoriser le trafic de diffusion ARP

L'appliance de sécurité connecte le même réseau sur ses interfaces internes et externes. Comme le pare-feu n'est pas un saut routé, vous pouvez facilement introduire un pare-feu transparent à un réseau existant. Le réadressage IP n'est pas nécessaire. Le trafic IPv4 est autorisé à travers le pare-feu transparent automatiquement d'une interface de sécurité supérieure à une interface de sécurité inférieure, sans liste d'accès. Les protocoles ARP (Address Resolution Protocol) sont autorisés à travers le pare-feu transparent dans les deux directions sans liste d'accès. Le trafic ARP peut être contrôlé par l'inspection ARP. Pour le trafic de couche 3 qui passe d'une interface de faible à haute sécurité, une liste d'accès étendue est requise.

Remarque : L'appliance de sécurité en mode transparent ne transmet pas de paquets CDP (Cisco Discovery Protocol), ni de paquets IPv6, ni de paquets qui n'ont pas d'EtherType valide supérieur ou égal à 0x600. Par exemple, vous ne pouvez pas transmettre des paquets IS-IS. Une exception est faite pour les unités de données de protocole de pont (BPDU), qui sont prises en charge.

Adresses MAC autorisées

Ces adresses MAC de destination ont la permission de passer à travers le pare-feu transparent. Les adresses MAC qui ne figurent pas sur cette liste sont supprimées :

- L'adresse MAC de destination de VÉRITABLE diffusion équivaut à FFFF.FFFF.FFFF
- Addresses MAC multicast Ipv4 de 0100.5E00.0000 à 0100.5EFE.FFFF
- Addresses MAC multicast Ipv6 de 3333.0000.0000 à 3333.FFFF.FFFF
- L'adresse multicast BPDU est égale à 0100.0CCC.CCCD
- Adresses MAC multicast AppleTalk de 0900.0700.0000 à 0900.07FF.FFFF

Trafic non autorisé à passer en mode routeur

En mode routeur, certains types de trafic ne peuvent pas traverser l'appliance de sécurité même si vous l'autorisez dans une liste d'accès. Cependant, le pare-feu transparent peut autoriser presque tout trafic via une liste d'accès étendue (pour le trafic IP) ou une liste d'accès EtherType (pour le trafic non IP).

Par exemple, vous pouvez établir des juxtapositions de protocole de routage à travers un pare-feu

transparent . Vous pouvez autoriser le trafic OSPF (Open Shortest Path First), RIP (Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol) ou BGP (Border Gateway Protocol) via une liste de contrôle d'accès étendue. De même, les protocoles tels que le protocole HSRP (Hot Standby Router Protocol) ou le protocole VRRP (Virtual Router Redundancy Protocol) peuvent passer par l'appliance de sécurité.

Le trafic non IP (par exemple, AppleTalk, IPX, BPDU et MPLS) peut être configuré pour passer par une liste d'accès EtherType.

Pour les caractéristiques qui ne sont pas directement prises en charge sur le pare-feu transparent, vous pouvez laisser le trafic passer de façon à ce que les routeurs en amont et en aval puissent prendre en charge la fonctionnalité. Par exemple, en utilisant une liste d'accès étendue, vous pouvez autoriser le trafic DHCP (Dynamic Host Configuration Protocol) (au lieu de la fonction de relais DHCP non prise en charge) ou le trafic de multidiffusion tel que celui créé par IP/TV.

Dépannage des problèmes de connectivité

Si les utilisateurs d'Internet ne peuvent pas accéder à votre site Web, procédez comme suit :

1. Assurez-vous que les adresses de configuration sont correctement entrées :Adresse externe valideAdresse interne correcteLe DNS externe a traduit l'adresse
2. Recherchez les erreurs sur l'interface externe.Le dispositif de sécurité Cisco est préconfiguré pour détecter automatiquement les paramètres de vitesse et de duplex sur une interface. Cependant, plusieurs situations peuvent entraîner l'échec du processus de négociation automatique. Cela entraîne des incohérences de vitesse ou de mode duplex (et des problèmes de performances). Pour une infrastructure réseau à fonction critique, Cisco va manuellement coder en dur la vitesse et le duplex sur chaque interface afin d'éviter tout risque d'erreur. Ces dispositifs ne se déplacent généralement pas. Par conséquent, si vous les configurez correctement, vous ne devriez pas avoir besoin de les modifier.**Exemple :**
   ```
   asa(config)#interface ethernet 0/0
   asa(config-if)#duplex full
   asa(config-if)#speed 100
   asa(config-if)#exit
   ```

   Dans certaines situations, le codage en dur des paramètres de vitesse et de duplex génère des erreurs. Par conséquent, vous devez configurer l'interface avec le paramètre par défaut du mode de détection automatique comme le montre cet exemple :**Exemple :**
   ```
   asa(config)#interface ethernet 0/0
   asa(config-if)#duplex auto
   asa(config-if)#speed auto
   asa(config-if)#exit
   ```

3. Si le trafic n'envoie pas ou ne reçoit pas via l'interface de l'ASA ou du routeur de tête de réseau, essayez d'effacer les statistiques ARP.
   ```
   asa#clear arp
   ```

4. Utilisez les commandes **show run object** et **show run static** afin de vous assurer que la traduction statique est activée.**Exemple :**

   ```
   object service www
   service tcp source eq www
   object network 192.168.202.2
   ```

```
host 192.168.202.2
object network 10.2.1.5
host 10.2.1.5
object service 1025
service tcp source eq 1025
nat (inside,outside) source static 10.2.1.5 192.168.202.2 service 1025 www
```

Dans ce scénario, l'adresse IP externe est utilisée comme adresse IP mappée pour le serveur Web.

```
nat (inside,outside) source dynamic 10.2.1.5 interface service 1025 www
```

5. Vérifiez que la route par défaut sur le serveur Web pointe vers l'interface interne de l'ASA.
6. Vérifiez la table de traduction à l'aide de la commande show xlate afin de voir si la traduction a été créée.
7. Utilisez la commande logging buffered afin de vérifier les fichiers journaux pour voir si des refus se produisent. (Recherchez l'adresse traduite et vérifiez si vous voyez des refus.)
8. Utilisez la commande capture :

```
access-list webtraffic permit tcp any host 192.168.202.5

capture capture1 access-list webtraffic interface outside
```

Remarque : cette commande génère une quantité significative de sortie. Il peut entraîner un blocage ou un rechargement d'un routeur sous de lourdes charges de trafic.

9. Si les paquets arrivent à l'ASA, assurez-vous que votre route vers le serveur Web à partir de l'ASA est correcte. (Vérifiez les commandes route de votre configuration ASA.)
10. Vérifiez si le proxy ARP est désactivé. Émettez la commande show running-config sysopt dans ASA 8.3.Ici, le proxy ARP est désactivé par la commande **sysopt noproxyarp outside** :

```
ciscoasa#show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt noproxyarp outside
sysopt connection permit-vpn
```

Afin de réactiver le proxy ARP, entrez cette commande en mode de configuration globale :

```
ciscoasa(config)#no sysopt noproxyarp outside
```

Lorsqu'un hôte envoie du trafic IP à un autre périphérique sur le même réseau Ethernet, l'hôte doit connaître l'adresse MAC du périphérique. Le protocole ARP est un protocole de couche 2 qui résout une adresse IP en adresse MAC. Un hôte envoie une requête ARP et demande « Qui est cette adresse IP ? ». Le périphérique propriétaire de l'adresse IP répond : « Je possède cette adresse IP ; voici mon adresse MAC. »Le proxy ARP permet au dispositif de sécurité de répondre à une requête ARP au nom des hôtes derrière. Pour ce faire, il répond aux requêtes ARP pour les adresses mappées statiques de ces hôtes. Le dispositif de sécurité répond à la demande avec sa propre adresse MAC, puis transfère les paquets IP à l'hôte interne approprié.Par exemple, dans le diagramme de ce document, lorsqu'une requête ARP est faite pour l'adresse IP globale du serveur Web, 192.168.202.5, le dispositif de sécurité répond avec sa propre adresse MAC. Si le proxy ARP n'est pas

activé dans cette situation, les hôtes du réseau externe de l'appliance de sécurité ne peuvent pas atteindre le serveur Web en émettant une requête ARP pour l'adresse 192.168.202.5. Reportez-vous à la référence de la commande pour plus d'informations sur la commande sysopt.

11. Si tout semble correct et que les utilisateurs ne peuvent toujours pas accéder au serveur Web, ouvrez un dossier auprès de l'assistance technique Cisco.

Message d'erreur - %ASA-4-407001 :

Quelques hôtes ne peuvent pas se connecter à Internet et au `message d'erreur - %ASA-4-407001 : Refuser le trafic pour local-host interface_name:inside_address, le` message d'erreur `limite de licence dépassée` est reçu dans le syslog. Comment cette erreur est-elle résolue ?

Ce message d'erreur est reçu quand le nombre d'utilisateurs dépasse la limite d'utilisateurs de la licence utilisée. Afin de résoudre cette erreur, mettez à niveau la licence vers un plus grand nombre d'utilisateurs. Il peut s'agir d'une licence utilisateur de 50, 100 ou illimitée, selon les besoins.

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Avis sur le terrain des produits de sécurité (y compris Cisco Adaptive Security Appliance (ASA))
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems