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

Contenu

Introduction

Quand une appliance de sécurité adaptable Cisco (ASA) est au commencement configurée, elle a une stratégie de sécurité par défaut où chacun sur l'intérieur peut sortir, et personne de l'extérieur ne peut entrer. Si votre site exige une stratégie de sécurité différente, vous pouvez permettre à des utilisateurs externes pour se connecter à votre web server par l'ASA.

Une fois que vous établissez la Connectivité de base par Cisco ASA, vous pouvez apporter des modifications de configuration au Pare-feu. Assurez-vous que toutes les modifications de configuration que vous apportez à l'ASA soyez conformément à votre stratégie de sécurité de site.

Reportez-vous à la section PIX/ASA : Établissez et dépannez la Connectivité par l'appliance de sécurité Cisco pour la configuration identique sur Cisco ASA avec des versions 8.2 et antérieures.

Conditions préalables

Conditions requises

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

- ASA 8.3(x) : Connectez un réseau interne simple à l'Internet
- Configurant le PPPoE Client sur une appliance de sécurité adaptable Cisco (ASA)

Composants utilisés

Les informations dans ce document sont basées sur une appliance de sécurité adaptable Cisco (ASA) cette version 8.3 et ultérieures de passages.

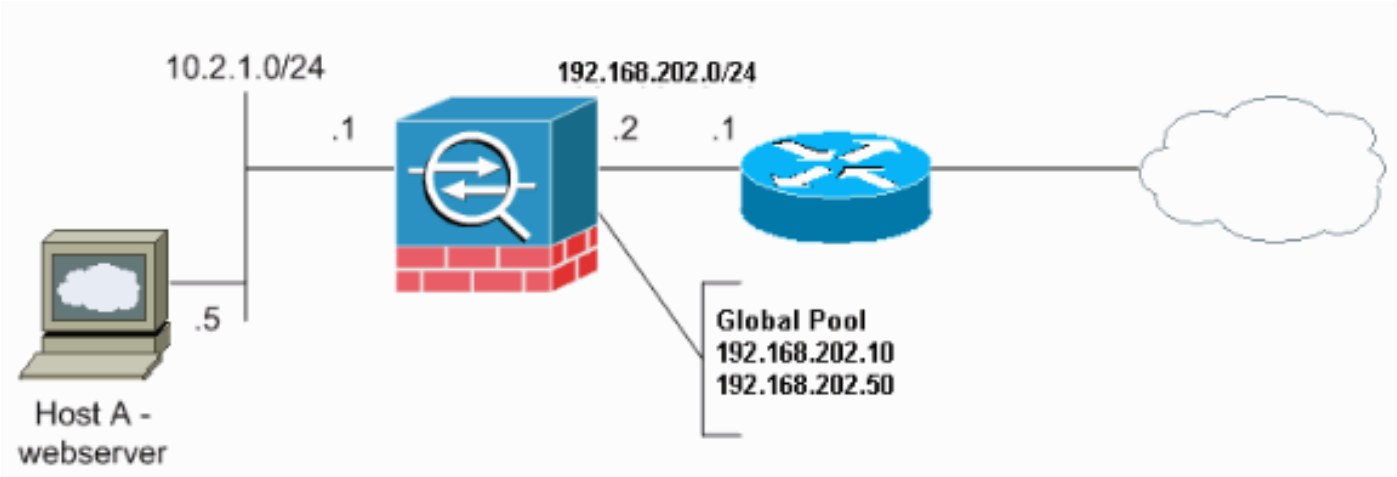
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Comment la Connectivité par l'ASA fonctionne

Dans ce réseau, hébergez A est le web server avec une adresse interne de 10.2.1.5. Le web server est assigné une adresse (traduite) externe de 192.168.202.5. Les internautes doivent indiquer 192.168.202.5 afin d'accéder au web server. L'entrée DNS pour votre web server doit être cette adresse. On ne permet aucune autre connexion de l'Internet.



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

Configurez la Connectivité par Cisco ASA

Terminez-vous ces étapes afin de configurer la Connectivité par l'ASA :

1. Créez un objet de réseau qui définit un sous-réseau interne et un objet de réseau différent pour la chaîne de pool d'IP. Configurez le NAT utilisant ces objets de réseau :
   ```
   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. Assignez une adresse traduite par charge statique pour l'hôte interne auquel les internautes 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** de permettre des utilisateurs externes par Cisco ASA. Utilisez toujours 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
```

Permettez le trafic de diffusion ARP

Les dispositifs de sécurité connectent le même réseau sur ses interfaces internes et externes. Puisque le Pare-feu n'est pas un saut conduit, vous pouvez facilement introduire un Pare-feu transparent à un réseau existant. L'IP réadressant n'est pas nécessaire. On permet le trafic d'ipv4 par le Pare-feu transparent automatiquement d'une interface à sécurité plus élevée à une interface à niveau de sécurité inférieur, sans liste d'accès. On permet des protocoles ARP (ARPs) par 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 la couche 3 qui voyage d'un bas à une interface de sécurité élevée, une liste d'accès étendue est exigée.

Remarque: Les dispositifs de sécurité de mode transparent ne passent des paquets de Protocole CDP (Cisco Discovery Protocol) ou des paquets d'IPv6, ou aucun paquet qui n'ont pas un EtherType supérieur ou égal à un 0x600 valides. Par exemple, vous ne pouvez pas passer des paquets IS-IS. Une exception est faite pour les Bridges Protocol Data Unit (BPDU), qui sont pris en charge.

Adresses MAC autorisées

Ces adresses MAC de destination ont la permission de passer à travers le pare-feu transparent. Des adresses MAC pas sur cette liste sont abandonnées :

- 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 de MAC multicast d'AppleTalk de 0900.0700.0000 à 0900.07FF.FFFF

Le trafic non permis pour passer dans le mode routeur

Dans le mode routeur, quelques types de trafic ne peuvent pas traverser les dispositifs de sécurité même si vous les permettez dans une liste d'accès. Le Pare-feu transparent, cependant, peut permettre presque n'importe quel trafic en utilisant une liste d'accès étendue (pour le trafic IP) ou une liste d'accès d'EtherType (pour le trafic non-IP).

Par exemple, vous pouvez établir des contiguïtés de protocole de routage par un Pare-feu transparent. Vous pouvez permettre le trafic de Protocole OSPF (Open Shortest Path First), de Protocole RIP (Routing Information Protocol), de Protocole EIGPR (Enhanced Interior Gateway Routing Protocol), ou de Protocole BGP (Border Gateway Protocol) basé sur une liste 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 traverser les dispositifs de sécurité.

Le trafic Non-IP (par exemple, AppleTalk, IPX, BPDU, et MPLS) peut être configuré pour passer en utilisant une liste d'accès d'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, à l'aide d'une liste d'accès étendue, vous pouvez permettre le trafic du protocole DHCP (DHCP) (au lieu de la caractéristique non vérifiée de relais DHCP) ou le trafic de multidiffusion comme cela créé par IP/TV.

Dépannez les problèmes de Connectivité

Si les internautes ne peuvent pas accéder à votre site Web, terminez-vous ces étapes :

1. Veillez-vous pour avoir introduit des adresses de configuration correctement :Adresse externe valideAdresse interne correcteLes DN externes a traduit l'adresse
2. Vérifiez l'interface extérieure pour des erreurs.L'appliance de sécurité Cisco est préconfigurée automatique-pour détecter les configurations de la vitesse et le duplex sur une interface. Cependant, plusieurs situations existent qui peuvent faire échouer le processus de négociation automatique. Ceci a comme conséquence la vitesse ou les conflits du mode bidirectionnel (et les problèmes de performance). 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 périphériques généralement ne se déplacent pas autour. Par conséquent, si vous les configurez correctement, vous ne devriez pas devoir les changer.**Exemple :**`asa(config)#interface ethernet 0/0 asa(config-if)#duplex full asa(config-if)#speed 100 asa(config-if)#exit` Dans certaines situations, coder en dur les configurations de la vitesse et le duplex mène à la génération des erreurs. Par conséquent, vous devez configurer l'interface à la valeur par défaut de automatique-détectez le comme indiqué dans cet exemple de mode :**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 reçoit par l'interface de l'ASA ou du routeur de headend, essai pour effacer les statistiques d'ARP.`asa#clear arp`
4. Utilisez l'**objet de passage d'exposition** et **affichez que les** commandes **statiques de passage** s'assuraient 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 extérieure est utilisée comme adresse IP tracée pour le web server.
   `nat (inside,outside) source dynamic 10.2.1.5 interface service 1025 www`
5. Vérifiez pour voir que le default route sur le web server indique l'interface interne de l'ASA.
6. Vérifiez la table de traduction utilisant la commande de show xlate afin de voir si la traduction était créée.
7. Employez la commande de logging buffered afin de vérifier les fichiers journal pour voir si refuse se produisent. (En recherchez l'adresse traduite et voyez si vous voyez refuse.)
8. Utilisez l'ordre de capture :
   `access-list webtraffic permit tcp any host 192.168.202.5 capture capture1 access-list webtraffic interface outside` **Remarque:** Cette commande génère une importante quantité de sortie. Il peut faire arrêter ou recharger un routeur sous des charges de trafic intense.
9. Si les paquets le font à l'ASA, assurez-vous que votre artère au web server de l'ASA est correcte. (Vérifiez les commandes d'artère dans votre configuration ASA.)
10. Vérifiez pour voir si le proxy ARP est désactivé. Émettez la commande de sysopt de show running-config dans ASA 8.3.Ici, le proxy ARP est désactivé par le **noproxyarp de sysopt en dehors de la** commande :`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, sélectionnez cette commande en mode de configuration globale :`ciscoasa(config)#`**`no sysopt noproxyarp outside`** Quand un hôte envoie le trafic IP à un autre périphérique sur le même réseau Ethernet, les besoins d'hôte de connaître l'adresse MAC du périphérique. L'ARP est un protocole de la couche 2 qui résout une adresse IP à une adresse MAC. Un hôte envoie une demande d'ARP et demande « qui est cette adresse IP ? ». Le périphérique qui possède l'adresse IP répond, « je possèdent cette adresse IP ; voici mon adresse MAC. »Le proxy ARP permet aux dispositifs de sécurité pour répondre à une demande d'ARP au nom des hôtes derrière lui. Il fait ceci en répondant aux demandes d'ARP des adresses tracées par charge statique de ces hôtes. Les dispositifs de sécurité répondent à la demande avec sa propre adresse MAC, puis en avant les paquets IP à l'hôte interne approprié.Par exemple, dans le diagramme dans ce document, quand une demande d'ARP est faite pour l'adresse IP globale du web server, 192.168.202.5, les dispositifs de sécurité répond avec sa propre adresse MAC. Si le proxy ARP n'est pas activé dans cette situation, les hôtes sur le réseau extérieur des dispositifs de sécurité ne peuvent pas atteindre le web server en émettant une demande d'ARP de l'adresse 192.168.202.5. Référez-vous à la référence de commandes pour plus d'informations sur la commande de **sysopt**.
11. Si tout semble être correct, et les utilisateurs ne peuvent pas encore accéder au web server, ouvrez une valise avec le support technique de Cisco.

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

Quelques hôtes ne peuvent pas se connecter à l'Internet et au `message d'erreur - %ASA-4-407001 :` **`Deny traffic for local-host interface_name:`** `des inside_address, limite de permis de` message d'erreur `dépassé par nombre` est reçus 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, améliorez le permis à un nombre supérieur d'utilisateurs. Ceci peut être 50, 100, ou permis illimité d'utilisateur au besoin.

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Notes de terrain relatives aux produits de sécurité (appliance de sécurité adaptable Cisco y compris (ASA))
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems