Configurez l'ASA pour de doubles réseaux internes

Contenu

Introduction

Ce document décrit comment configurer une appliance de sécurité adaptable Cisco (ASA) cette version de logiciel 9.x de passages pour l'usage de deux réseaux internes.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur Cisco ASA qui exécute la version de logiciel

9.x.

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.

Informations générales

Quand vous ajoutez un deuxième réseau interne derrière un Pare-feu ASA, considérez ces informations importantes :

- L'ASA ne prend en charge pas l'adressage secondaire.
- Un routeur doit être utilisé derrière l'ASA afin de réaliser le routage entre le réseau en cours et le réseau nouvellement ajouté.
- La passerelle par défaut pour tous les hôtes doit indiquer le routeur interne.
- Vous devez ajouter un default route sur le routeur interne ces points à l'ASA.
- Vous devez effacer le cache de Protocole ARP (Address Resolution Protocol) sur le routeur interne.

Configurez

Utilisez les informations qui sont décrites dans cette section afin de configurer l'ASA.

Diagramme du réseau

Voici la topologie qui est utilisée pour les exemples dans tout ce document :

> Remarque: Les schémas d'adressage IP qui sont utilisés dans cette configuration ne sont pas légalement routable sur l'Internet. Ils sont les adresses RFC 1918 qui sont utilisées dans un environnement de travaux pratiques.

Configuration ASA 9.x

Si vous avez la sortie de la commande de **write terminal de** votre périphérique de Cisco, vous

pouvez utiliser l'outil d'Output Interpreter (clients enregistrés seulement) afin d'afficher des éventuels problèmes et des difficultés.

Voici la configuration pour l'ASA qui exécute la version de logiciel 9.x :

```
ASA Version 9.3(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- This is the configuration for the outside interface.

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0

!--- This is the configuration for the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!

boot system disk0:/asa932-smp-k8.bin

!--- This creates an object called OBJ_GENERIC_ALL.
!--- Any host IP address that does not already match another configured
!--- object will get PAT to the outside interface IP address
!--- on the ASA (or 10.1.5.1), for Internet-bound traffic.


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
!
route inside 192.168.1.0 255.255.255.0 192.168.0.254 1
route outside 0.0.0.0 0.0.0.0 203.0.113.1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
```

```
no threat-detection statistics tcp-intercept
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```

Permettez à des hôtes internes Access aux réseaux extérieurs avec PAT

Si vous avez l'intention de faire partager aux hôtes internes une annonce publique simple pour la traduction, translation d'adresses d'adresse du port d'utilisation (PAT). Une des configurations PAT les plus simples comporte la traduction de tous les hôtes internes de sorte qu'ils semblent être l'IP extérieur d'interface. C'est la configuration PAT typique qui est utilisée quand le nombre d'adresses IP routable qui sont fournies par l'ISP est limité seulement à quelques uns, ou juste un.

Terminez-vous ces étapes afin de permettre aux hôtes internes l'accès aux réseaux extérieurs avec PAT :

1. Naviguez vers la **configuration** > le **Pare-feu** > les **règles NAT**, cliquez sur Add, et choisissez l'**objet de réseau** afin de configurer une règle NAT dynamique :

2. Configurez le réseau/hôte/plage pour laquelle PAT dynamique est prié. Dans cet exemple, tous des sous-réseaux d'intérieur ont été sélectionnés. Ce processus devrait être répété pour les sous-réseaux spécifiques que vous souhaitez traduire de cette manière :

3. Cliquez sur **NAT**, cochez la case **automatique de règle de traduction d'adresses d'ajouter**,

entrez dans **dynamique,** et placez l'option **traduite d'adr** de sorte qu'elle reflète l'interface extérieure. Si vous cliquez sur le bouton de points de suspension, il vous aide pour sélectionner un objet préconfiguré, tel que l'interface extérieure :

4. Cliquez sur **avancé** afin de sélectionner une source et une interface de destination :

5. Cliquez sur OK, et puis cliquez sur Apply afin d'appliquer les modifications. Une fois complet, Adaptive Security Device Manager (ASDM) affiche la règle NAT :

Configuration du routeur B

Voici la configuration pour le routeur B :

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router B
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet0/1

!--- This assigns an IP address to the ASA-facing Ethernet interface.

ip address 192.168.0.254 255.255.255.0
no ip directed-broadcast

ip classless

!--- This route instructs the inside router to forward all of the
!--- non-local packets to the ASA.
```

```
ip route 0.0.0.0 0.0.0.0 192.168.0.1
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

Vérifiez

Accédez à un site Web par l'intermédiaire du HTTP par un navigateur Web afin de vérifier que votre configuration fonctionne correctement.

Cet exemple utilise un site qui est hébergé à l'adresse IP *198.51.100.100*. Si la connexion est réussie, les sorties qui sont fournies dans les sections qui suivent peuvent être vues sur l'ASA CLI.

Connexion

Sélectionnez la commande d'**adresse de show connection** afin de vérifier la connexion :

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 192.168.1.5:58799, idle 0:00:06, bytes 937,
flags UIO
```

L'ASA est un pare-feu dynamique, et le trafic de retour du web server est permis de retour par le Pare-feu parce qu'il apparie une ***connexion*** dans la table de connexion de Pare-feu. On permet le trafic qui apparie une connexion qui préexiste par le Pare-feu sans être bloqué par une liste de contrôle d'accès d'interface (ACL).

Dans la sortie précédente, le client sur l'interface interne a établi une connexion à l'hôte de 198.51.100.100 hors fonction de l'interface extérieure. Ce rapport est établi avec le protocole TCP et a été de veille pendant six secondes. Les indicateurs de connexion indiquent l'état actuel de cette connexion.

> Remarque: Référez-vous au document Cisco d'indicateurs de connexion TCP ASA (habillage et désinstallation de connexion) pour plus d'informations sur des indicateurs de connexion.

Dépannez

Utilisez les informations qui sont décrites dans cette section afin de dépanner des questions de configuration.

Syslog

Sélectionnez le **show log command** afin de visualiser les Syslog :

```
ASA(config)# show log | in 192.168.1.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
192.168.1.5/58799 to outside:203.0.113.2/58799

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:192.168.1.5/58799 (203.0.113.2/58799)
```

Le Pare-feu ASA génère des Syslog pendant le fonctionnement normal. Les Syslog s'étendent dans la verbosité basée sur la configuration de journalisation. La sortie affiche deux Syslog qui sont vus au niveau six, ou le niveau *informationnel*.

Dans cet exemple, il y a deux Syslog générés. Le premier est un message de log pour indiquer que le Pare-feu a établi une traduction ; spécifiquement, une traduction dynamique de TCP (PAT). Il indique l'adresse IP source et le port, aussi bien que l'adresse IP et le port traduits, car le trafic traverse de l'intérieur aux interfaces extérieures.

Le deuxième Syslog indique que le Pare-feu a établi une connexion dans sa table de connexion pour ce trafic spécifique entre le client et serveur. Si le Pare-feu était configuré afin de bloquer cette tentative de connexion, ou un autre facteur empêchait la création de cette connexion (des contraintes de ressource ou une mauvaise configuration possible), le Pare-feu ne génère pas un log pour indiquer que la connexion a été établie. Au lieu de cela, il se connecte une raison pour que la connexion soit refusée ou une indication en vue de le facteur qui a empêché la connexion de l'création.

Traceurs de paquet

Sélectionnez cette commande afin d'activer la fonctionnalité de traceur de paquet :

```
ASA(config)# packet-tracer input inside tcp 192.168.1.5 1234 198.51.100.100 80


--Omitted--

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

La fonctionnalité de traceur de paquet sur l'ASA te permet pour spécifier un paquet *simulé* et pour visualiser tous les divers étapes, contrôles, et fonctions que le Pare-feu se termine quand il traite le trafic. Avec cet outil, il est utile d'identifier un exemple du trafic que vous croyez *devriez* être laissé traverser le Pare-feu, et utilisez que 5-tupple afin de simuler le trafic. Dans l'exemple précédent, le traceur de paquet est utilisé afin de simuler une tentative de connexion qui répond à ces critères :

- Le paquet simulé arrive sur l'interface interne.

- Le protocole qui est utilisé est TCP.
- L'adresse IP simulée de client est 192.168.1.5.
- Le client envoie le trafic qui est originaire du port 1234.
- Le trafic est destiné à un serveur à l'adresse IP 198.51.100.100.
- Le trafic est destiné au port 80.

Notez qu'il n'y avait aucune mention de l'interface extérieure dans la commande. C'est dû à la conception de traceur de paquet. L'outil vous indique comment les processus de Pare-feu qui type de tentative de connexion, qui inclut comment elle la conduirait, et hors de quelle interface.

> **Conseil** : Pour plus d'informations sur la fonctionnalité de traceur de paquet, référez-vous aux paquets de suivi avec la section de Packet Tracer du *guide de configuration de gamme de Cisco ASA 5500 utilisant le CLI, les 8.4 et les 8.6*.

Capture

Sélectionnez ces commandes afin d'appliquer une capture :

```
ASA# capture capin interface inside match tcp host 192.168.1.5 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100 ASA#show capture capin

3 packets captured

1: 11:31:23.432655 192.168.1.5.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712518 198.51.100.100.80 > 192.168.1.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 192.168.1.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768 ASA#show capture capout

3 packets captured

1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

Le Pare-feu ASA peut capturer le trafic qui écrit ou laisse ses interfaces. Cette fonctionnalité de capture est fantastique parce qu'elle peut définitivement prouver à si le trafic arrive, ou des feuilles de, un Pare-feu. L'exemple précédent affiche la configuration de deux captures nommées **capin** et **capout** sur les interfaces internes et externes, respectivement. Les ordres de **capture** utilisent le mot clé de **correspondance**, qui te permet pour spécifier le trafic que vous voulez capturer.

Pour l'exemple de capture de *capin*, on l'indique que vous voulez apparier le trafic qui est vu sur l'interface interne (d'entrée ou de sortie) cet *hôte 198.51.100.100 de 192.168.1.5 d'hôte de TCP de* correspondances. En d'autres termes, vous voulez capturer n'importe quel trafic TCP qui est envoyé de l'hôte *192.168.1.5* pour héberger *198.51.100.100*, ou vice versa. L'utilisation du mot clé de **correspondance** permet au Pare-feu pour capturer ce trafic bidirectionnel. L'ordre de **capture**

qui est défini pour l'interface extérieure ne met pas en référence l'adresse IP de client interne parce que les attitudes PAT de Pare-feu sur cette adresse IP de client. En conséquence, vous ne pouvez pas être assortie avec cette adresse IP de client. Au lieu de cela, cet exemple en emploie afin d'indiquer que toutes les adresses IP possibles apparieraient cette condition.

Après que vous configuriez les captures, vous pouvez alors tenter d'établir une connexion de nouveau et poursuivre pour visualiser les captures avec le ***<capture_name> de*** **show capture** commandez. Dans cet exemple, vous pouvez voir que le client peut se connecter au serveur, comme évident par la prise de contact à trois voies de TCP qui est vue dans les captures.

Informations connexes

- Cisco Adaptive Security Device Manager
- Pare-feu de la deuxième génération de gamme 5500-X de Cisco ASA
- Demandes des commentaires (RFC)
- Guide de configuration CLI de gamme de Cisco ASA, 9.0 du Â d'âÂ configurant la charge statique et les default route
- Cisco Systems du Â d'âÂ de Soutien technique et de documentation