ASA 8.4(x) connecte un réseau interne simple à l'exemple de configuration d'Internet

Contenu

Introduction

Ce document décrit comment installer l'appliance de sécurité adaptable Cisco (ASA) avec la version 8.4(1) pour l'usage sur un réseau interne simple.

Reportez-vous à la section PIX/ASA : Connecter le réseau interne simple à l'exemple de configuration d'Internet pour la même configuration sur l'ASA avec des versions 8.2 et antérieures.

Conditions préalables

Conditions requises

Aucune condition préalable spécifique n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur l'ASA avec la version 8.4(1).

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

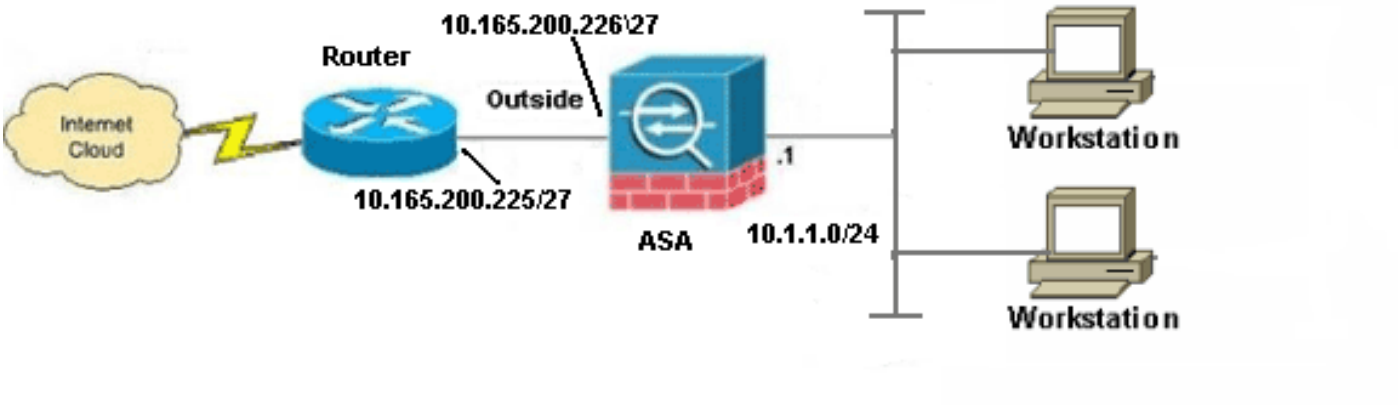
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

> Remarque: Pour obtenir plus d'informations sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés uniquement).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



> 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 utilisées dans un environnement de laboratoire.

Configuration ASA 8.4

Ce document utilise les configurations suivantes :

- Configuration du routeur
- ASA 8.4 et configuration plus récente

Configuration du routeur

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R3640_out
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/1
ip address 10.165.200.225 255.255.255.224
no ip directed-broadcast

!
ip classless
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
```

ASA 8.4 et configuration plus récente

```
ASA#show run
: Saved
:
ASA Version 8.4(1)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- Configure the outside interface.

!
interface GigabitEthernet0/0
nameif outside
```

```
security-level 0
ip address 10.165.200.226 255.255.255.224

!--- Configure the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
management-only
!
boot system disk0:/asa841-k8.bin

ftp mode passive
!
!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- NAT rule will Port Address Translate (PAT) to the outside interface IP
!--- on the ASA (or 10.165.200.226) for Internet bound traffic.
!
object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
!
nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface
!
route outside 0.0.0.0 0.0.0.0 10.165.200.225
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
```

> Remarque: Pour plus d'informations sur la configuration du Traduction d'adresses de réseau (NAT) et de la traduction d'adresses de port (TAPOTEMENT) sur la version 8.4 ASA, référez-vous aux informations sur NAT.
>
> Pour plus d'informations sur la configuration des Listes d'accès sur la version 8.4 ASA, référez-vous aux informations sur des Listes d'accès.

Vérifiez

Essayez d'accéder à un site Web par l'intermédiaire du HTTP avec un web browser. Cet exemple utilise un site qui est hébergé chez 198.51.100.100. Si la connexion est réussie, cette sortie peut être vue sur l'ASA CLI :

Connexion

```
ASA(config)# show connection address 10.1.1.154
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 10.1.1.154:58799, 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. Trafiquez qu'apparie une connexion qui préexiste est autorisée par le Pare-feu sans être bloqué par un ACL d'interface.

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. Plus d'informations sur des indicateurs de connexion peuvent être trouvées dans des indicateurs de connexion TCP ASA.

Syslog

```
ASA(config)# show log | in 10.1.1.154

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.1.1.154/58799 to outside:10.165.200.226/58799

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:10.1.1.154/58799 (10.165.200.226/58799)
```

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 de niveau **« informationnel »**.

Dans cet exemple, il y a deux Syslog générés. Le premier est un message de log qui indique que le Pare-feu a établi une **traduction**, spécifiquement une traduction dynamique de TCP (PAT). Il indique l'adresse IP source et le port et l'adresse IP et le port traduits pendant que 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 génèrerait pas un log qui indique que la connexion a été établie. Au lieu de cela il se connecterait une raison pour que la connexion soit refusée ou une indication au sujet de quel facteur a empêché la connexion de l'création.

Traductions NAT (Xlate)

```
ASA(config)# show xlate local 10.1.1.154
3 in use, 80 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.1.1.154/58799 to outside:10.165.200.226/58799 flags ri idle
0:02:42 timeout 0:00:30
```

En tant qu'élément de cette configuration, PAT est configuré afin de traduire les adresses IP internes d'hôte aux adresses qui sont routable sur l'Internet. Afin de confirmer que ces traductions sont créées, vous pouvez vérifier la table de xlate (traduction). **Le show xlate de** commande**,** une fois combiné avec le mot clé **local** et l'adresse IP interne de l'hôte, affiche toutes les entrées actuelles dans la table de traduction pour cet hôte. La sortie précédente prouve qu'il y a une traduction actuellement établie pour cet hôte entre les interfaces internes et externes. L'IP d'hôte interne et le port sont traduits à l'adresse de 10.165.200.226 par notre configuration. Les indicateurs les ont répertorié, r i, indiquent que la traduction est **dynamique** et un **portmap**. Plus d'informations sur différentes configurations NAT peuvent être trouvées ici : Informations sur NAT.

Dépannez

L'ASA fournit les plusieurs outils avec lesquels pour dépanner la Connectivité. Si la question persiste après que vous vérifiiez la configuration et vérifiiez la sortie répertoriée précédemment, ces techniques et outil pourraient aider à déterminer la cause de votre panne de Connectivité.

Traceur de paquets

```
ASA(config)# packet-tracer input inside tcp 10.1.1.154 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 voir tous les divers étapes, contrôles, et fonctions par lesquelles le Pare-feu passe 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 l'utilise 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'**intérieur**.
- Le protocole utilisé est **TCP**.
- L'adresse IP simulée de client est **10.1.1.154**.
- Le client envoie le trafic originaire du port **1234**.
- Le trafic est destiné à un serveur à l'IP address **198.51.100.100**.
- Le trafic est destiné au port **80**.

Notez qu'il n'y avait aucune mention de l'interface **dehors** dans la commande. C'est par 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. Plus d'informations sur le traceur de paquet peuvent être trouvées en paquets de suivi avec Packet Tracer.

Capture

```
ASA# capture capin interface inside match tcp host 10.1.1.154 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       10.1.1.154.58799 > 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 > 10.1.1.154.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       10.1.1.154.58799 > 198.51.100.100.80: . ack 2123396068
win 32768
```

```
ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       10.165.200.226.58799 > 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 > 10.165.200.226.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       10.165.200.226.58799 > 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 si le trafic arrive à, ou des feuilles de, un Pare-feu. L'exemple précédent a affiché la configuration de deux captures nommées **capin** et **capout** sur les interfaces internes et externes respectivement. Les ordres de capture ont utilisé le mot clé de **correspondance**, qui te permet pour être spécifique au sujet de quel trafic vous voulez capturer.

Pour le **capin de** capture**,** vous avez indiqué que vous avez voulu apparier le trafic vu sur l'interface interne (d'entrée ou de sortie) cet **hôte 198.51.100.100 de 10.1.1.154 d'hôte de TCP de** correspondances. En d'autres termes, vous voulez capturer n'importe quel trafic TCP qui est envoyé de l'**hôte 10.1.1.154 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 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 tenteriez alors l'établissement une connexion de nouveau, et poursuivez pour visualiser les captures avec la commande de ***<capture_name> de* show capture**. Dans cet exemple, vous pouvez voir que le client pouvait se connecter au serveur comme évident par la prise de contact à trois voies de TCP vue dans les captures.

Informations connexes

- Cisco Adaptive Security Device Manager
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems