Exemple de configuration d'ASA 8.4(x) connecte un seul réseau interne à Internet

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Configuration
Diagramme du réseau
Configuration ASA 8.4
Configuration du routeur
ASA 8.4 et versions ultérieures
Vérification
Connexion
Syslog
Traductions NAT (Xlate)
Dépannage
Packet Tracer
Saisir
Informations connexes

Introduction

Ce document explique comment configurer le Dispositif de sécurité adaptatif (ASA) dédié Cisco avec la version 8.4(1) pour un usage sur un seul réseau interne.

Reportez-vous à la section PIX/ASA : Exemple de configuration de la connexion d'un seul réseau interne à Internet pour la même configuration sur l'ASA avec les versions 8.2 et antérieures.

Conditions préalables

Conditions requises

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

Components Used

Les informations de 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. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

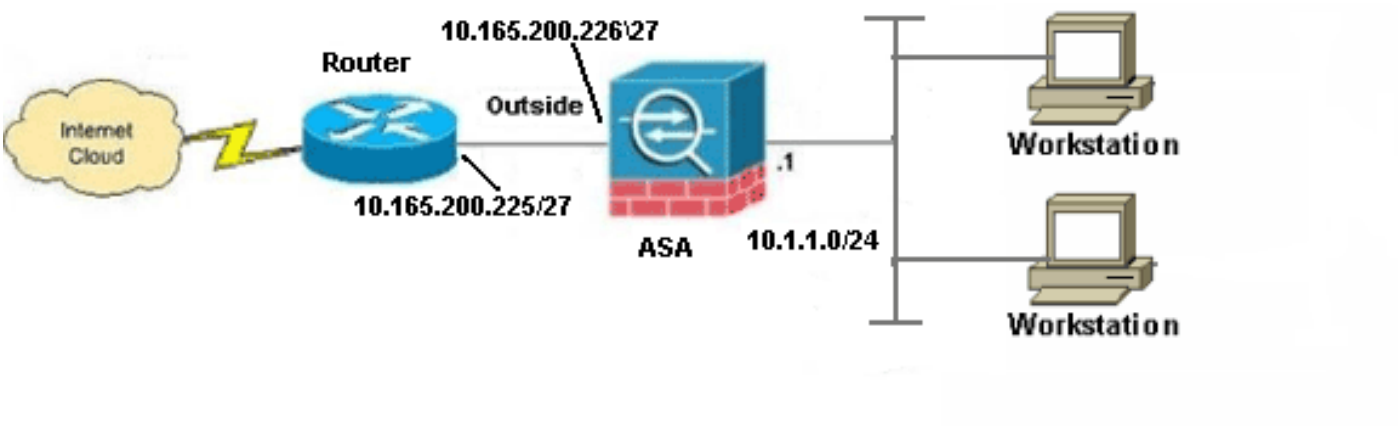
Configuration

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

> **Note**: 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 :



> **Note**: 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 versions ultérieures

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 versions ultérieures

```
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
```

Note: Pour plus d'informations sur la configuration de la traduction d'adresses de réseau (NAT) et de la traduction d'adresses de port (PAT) sur ASA version 8.4, référez-vous à Informations sur NAT.

Pour plus d'informations sur la configuration des listes d'accès sur ASA version 8.4, référez-vous à Informations sur les listes d'accès.

Vérification

Essayez d'accéder à un site Web via HTTP à l'aide d'un navigateur Web. Cet exemple utilise un site hébergé à l'adresse 198.51.100.100. Si la connexion réussit, cette sortie peut être vue sur l'interface de ligne de commande ASA :

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 serveur Web est autorisé à revenir par le pare-feu car il correspond à une ***connexion*** dans la table de connexion du pare-feu. Le trafic qui

correspond à une connexion qui existe déjà est autorisé à travers le pare-feu sans être bloqué par une liste de contrôle d'accès d'interface.

Dans la sortie précédente, le client sur l'interface interne a établi une connexion à l'hôte 198.51.100.100 à partir de l'interface externe. Cette connexion se fait avec le protocole TCP et est inactive depuis six secondes. Les indicateurs de connexion précisent l'état actuel de la connexion. Vous trouverez plus d'informations sur les indicateurs de connexion dans les 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 de l'ASA génère des SYSLOG pendant le fonctionnement normal. Les SYSLOG varient en verbosité selon la configuration de la journalisation. Le résultat montre deux syslogs qui sont vus au niveau 6, ou **'informationnel'**.

Dans cet exemple, deux SYSLOG sont générés. Le premier est un message de journal qui indique que le pare-feu a construit une **traduction**, en particulier une traduction TCP dynamique (PAT). Il indique l'adresse IP source et le port, ainsi que l'adresse IP et le port traduits lorsque le trafic traverse de l'intérieur vers l'extérieur.

Le deuxième SYSLOG indique que le pare-feu a établi une connexion dans sa table de connexions précisément pour ce trafic, entre le client et le serveur. Si le pare-feu a été configuré afin de bloquer cette tentative de connexion, ou si un autre facteur a empêché la création de cette connexion (contraintes de ressources ou une éventuelle erreur de configuration), le pare-feu ne génère pas de journal indiquant que la connexion a été créée. Au lieu de cela, il consigne une raison pour laquelle la connexion est refusée ou une indication sur le facteur qui empêche la création de la connexion.

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
```

Dans le cadre de cette configuration, la PAT est configurée afin de traduire les adresses IP d'hôte internes en adresses routables sur Internet. Afin de confirmer que ces traductions sont créées, vous pouvez vérifier la table xlate (traduction). La commande **show xlate,** lorsqu'elle est associée au mot clé **local** et à l'adresse IP de l'hôte interne, affiche toutes les entrées présentes dans la table de traduction de cet hôte. La sortie précédente montre qu'une traduction est actuellement créée pour cet hôte entre les interfaces interne et externe. L'adresse IP et le port de l'hôte interne sont traduits en l'adresse 10.165.200.226 selon notre configuration. Les indicateurs répertoriés, r i,

indiquent que la traduction est **dynamique** et une **portmap**. Vous trouverez plus d'informations sur les différentes configurations NAT ici : Informations sur NAT.

Dépannage

L'ASA fournit plusieurs outils pour dépanner la connectivité. Si le problème persiste après que vous ayez vérifié la configuration et vérifié le résultat indiqué précédemment, ces outils et techniques peuvent vous aider à déterminer la cause de votre échec de connectivité.

Packet Tracer

```
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 **packet tracer** de l'ASA vous permet de spécifier un paquet *simulé* et de voir toutes les étapes, vérifications et fonctions que le pare-feu exécute lorsqu'il traite le trafic. Avec cet outil, il est utile d'identifier un exemple de trafic que vous pensez *devoir* être autorisé à traverser le pare-feu, et d'utiliser ce 5-tupple afin de simuler le trafic. Dans l'exemple précédent, Packet Tracer est utilisé pour simuler une tentative de connexion qui répond aux critères suivants :

- Le paquet simulé arrive à l'**intérieur**.
- Le protocole utilisé est **TCP**.
- L'adresse IP du client simulé est 10.1.1.154.
- Le client envoie le trafic provenant du port **1234**.
- Le trafic est destiné à un serveur ayant l'adresse IP 198.51.100.100.
- Le trafic est destiné au port 80.

Notez qu'il n'y a pas eu de mention de l'interface **externe** dans la commande. C'est par conception Packet Tracer. L'outil vous indique comment le pare-feu traite ce type de tentative de connexion et indiquera comment il l'acheminera et à partir de quelle interface. Vous trouverez plus d'informations sur packet tracer dans le traçage des paquets avec Packet Tracer.

Saisir

```
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 entrant ou sortant de ses interfaces. Cette fonctionnalité de capture est fantastique car elle peut prouver de manière définitive si le trafic arrive à un pare-feu ou s'il en sort. L'exemple précédent montre la configuration de deux captures nommées **capin** et **capout** respectivement sur les interfaces interne et externe. Les commandes de capture ont utilisé le mot clé **match**, qui vous permet d'être précis sur le trafic que vous voulez capturer.

Pour la **chaîne** de capture**,** vous avez indiqué que vous vouliez faire correspondre le trafic vu sur l'interface interne (entrée ou sortie) qui correspond à l'**hôte tcp 10.1.1.154 hôte 198.51.100.100**. En d'autres termes, vous voulez capturer tout trafic TCP qui est envoyé de **l'hôte 10.1.1.154** à **l'hôte 198.51.100.100** ou **vice versa**. L'utilisation du mot-clé match permet au pare-feu de capter ce trafic dans les deux sens. La commande capture définie pour l'interface externe ne fait pas référence à l'adresse IP du client interne, car le pare-feu effectue la PAT sur cette adresse IP du client. Par conséquent, vous ne pouvez pas associer cette adresse IP au client. Plutôt, cet exemple utilise **any pour indiquer que toutes les adresses IP possibles correspondent à cette condition.**

Une fois les captures configurées, vous tentez de rétablir une connexion et de les afficher à l'aide de la commande **show capture *<capture_name>***. Dans cet exemple, vous pouvez voir que le client a été en mesure de se connecter au serveur comme le montre la connexion TCP en trois étapes 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