El ASA 8.4(x) conecta una sola red interna con el ejemplo de configuración de Internet

Contenido

Introducción

Este documento describe cómo configurar el dispositivo de seguridad adaptante de Cisco (ASA) con la versión 8.4(1) para el uso en una sola red interna.

Consulte PIX/ASA: Conexión sola de la red interna con el ejemplo de configuración de Internet para la misma configuración en el ASA con las versiones 8.2 y anterior.

Prerrequisitos

Requisitos

No hay requisitos previos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el ASA con la versión 8.4(1).

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

> Nota: Para encontrar la información adicional en los comandos usados en este documento, use la Command Lookup Tool (clientes registrados solamente).

Diagrama de la red

En este documento, se utiliza esta configuración de red:

> Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son los direccionamientos del RFC 1918, que se han utilizado en un ambiente de laboratorio.

Configuración ASA 8.4

En este documento, se utilizan estas configuraciones:

- Configuración del router
- Configuración ASA 8.4 y posterior

Configuración del router

```
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
```

Configuración ASA 8.4 y posterior

```
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
```

> Nota: Para más información sobre la configuración del Network Address Translation (NAT) y del Port Address Translation (PAT) en la Versión de ASA 8.4, refiera a la información sobre el NAT.
>
> Para más información sobre la configuración de las Listas de acceso en la Versión de ASA 8.4, refiera a la información sobre las Listas de acceso.

Verificación

Intente acceder un sitio web vía el HTTP con un web browser. Este ejemplo utiliza un sitio que se reciba en 198.51.100.100. Si la conexión es acertada, esta salida se puede considerar en el ASA CLI:

Conexión

```
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
```

El ASA es un escudo de protección con estado, y el tráfico de retorno del servidor Web se permite detrás con el Firewall porque hace juego una ***conexión*** en la tabla de conexiones del Firewall. Trafique que hace juego una conexión que preexista se permita con el Firewall sin el bloqueo por una interfaz ACL.

En la salida anterior, el cliente en la interfaz interior ha establecido una conexión al host de 198.51.100.100 apagado de la interfaz exterior. Esta conexión se hace con el protocolo TCP y ha estado ociosa por seis segundos. Los indicadores de la conexión indican al estado actual de esta conexión. Más información sobre los indicadores de la conexión se puede encontrar en los indicadores de la conexión 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)
```

El Firewall ASA genera los Syslog durante el funcionamiento normal. Los Syslog se extienden en la verbosidad basada en la configuración de registro. La salida muestra dos Syslog que se vean en el nivel seis, o el nivel **"informativo"**.

En este ejemplo, hay dos Syslog generados. El primer es un mensaje del registro que indica que el Firewall ha construido una **traducción**, específicamente una traducción dinámica TCP (PALMADITA). Indica la dirección IP de origen y el puerto y la dirección IP y el puerto traducidos mientras que el tráfico atraviesa del interior a las interfaces exteriores.

El segundo Syslog indica que el Firewall ha construido una **conexión** en su tabla de conexiones para este tráfico específico entre el cliente y servidor. Si el Firewall fuera configurado para bloquear este intento de conexión, o un cierto otro factor inhibiera la creación de esta conexión (las restricciones de recursos o una posible configuración incorrecta), el Firewall no generaría un registro que indica que la conexión fue construida. En lugar registraría una razón de la conexión para ser negado o una indicación sobre qué factor inhibió la conexión de ser creado.

Traducciones de 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
```

Como parte de esta configuración, la PALMADITA se configura para traducir los IP Addresses del host interno a los direccionamientos que son routable en Internet. Para confirmar que estas traducciones están creadas, usted puede marcar la tabla del xlate (traducción). El comando show xlate**,** cuando está combinado con la **palabra clave local** y la dirección IP del host interno, muestra todas las entradas presentes en la tabla de traducción para ese host. La salida anterior muestra que hay una traducción construida actualmente para este host entre las interfaces interior y exterior. El IP del host interior y el puerto se traducen al direccionamiento de 10.165.200.226 por nuestra configuración. Los indicadores enumeraron, r i, indican que la traducción es **dinámica** y un **portmap**. Más información sobre diversas configuraciones del NAT se puede encontrar aquí: Información sobre el NAT.

Troubleshooting

El ASA proporciona las herramientas múltiples con las cuales resolver problemas la Conectividad. Si persiste el problema después de que usted verifique la configuración y marque la salida enumerada previamente, estas herramientas y técnicas pudieron ayudar a determinar la causa de su falla de conectividad.

Paquete-trazalíneas

```
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
```

Las funciones del **trazalíneas del paquete** en el ASA permiten que usted especifique un paquete *simulado* y que considere todos los diversos pasos, controles, y funciones que el Firewall pasa por cuando procesa el tráfico. Con esta herramienta, es útil identificar un ejemplo del tráfico que usted cree *debe* ser permitido pasar con el Firewall, y utiliza que 5-tupple para simular el tráfico. En el ejemplo anterior, el trazalíneas del paquete se utiliza para simular un intento de conexión que cumpla estos criterios:

- El paquete simulado llega en el **interior**.
- El protocolo usado es **TCP**.
- El dirección IP del cliente simulado es **10.1.1.154**.
- El cliente envía el tráfico originado del puerto **1234**.
- El tráfico se destina a un servidor en el IP address **198.51.100.100**.
- El tráfico se destina al puerto **80**.

Note que no había mención de la interfaz **afuera** en el comando. Esto está por el diseño del trazalíneas del paquete. La herramienta le dice cómo los procesos del Firewall que la tentativa del tipo de conexión, que incluye de cómo la rutearía, y fuera de cuál interfaz. Más información sobre el trazalíneas del paquete se puede encontrar en los paquetes del seguimiento con el trazalíneas del paquete.

Captura

```
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>
```

El Firewall ASA puede capturar el tráfico que ingresa o deja sus interfaces. Estas funciones de la captura son fantásticas porque pueden probar definitivo si el tráfico llega, o se van de, un Firewall. El ejemplo anterior mostró la configuración de dos capturas nombradas **capin** y **capout** en las interfaces interior y exterior respectivamente. Los comandos capture utilizaron la palabra clave de la **coincidencia**, que permite que usted sea específico sobre qué tráfico usted quiere capturar.

Para el **capin de la** captura**,** usted indicó que usted quiso hacer juego el tráfico visto en la interfaz interior (ingreso o salida) ese **host 198.51.100.100 de 10.1.1.154 del host tcp de las** coincidencias. Es decir usted quiere capturar tráfico TCP que se envía del **host 10.1.1.154 para recibir 198.51.100.100** o **vice versa**. El uso de la palabra clave de la **coincidencia** permite que el Firewall capture ese tráfico bidireccional. El comando capture definido para la interfaz exterior no se refiere a la dirección IP del cliente interno porque el Firewall conduce la PALMADITA en ese dirección IP del cliente. Como consecuencia, usted no puede **hacer juego** con ese dirección IP del cliente. En lugar, este ejemplo utiliza **ningunos** para indicar que todos los IP Addresses posibles harían juego esa condición.

Después de que usted configure las capturas, usted entonces intentaría el establecimiento una conexión otra vez, y procede a ver las capturas con el comando del ***<capture_name> de la*** **captura de la demostración**. En este ejemplo, usted puede ver que el cliente podía conectar con el servidor como evidente por el apretón de manos de tres vías TCP visto en las capturas.

Información Relacionada

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliances
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems