Configure el ASA para las redes internas duales

Contenido

Introducción

Este documento describe cómo configurar un dispositivo de seguridad adaptante de Cisco (ASA) esa versión de software 9.x de los funcionamientos para el uso de dos redes internas.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en Cisco ASA que funciona con la versión de software 9.x.

La información que contiene este documento se creó a partir de los dispositivos en 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 cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Cuando usted agrega una segunda red interna detrás de un Firewall ASA, considere esta información importante:

- El ASA no soporta el direccionamiento secundario.
- Un router debe ser utilizado detrás del ASA para alcanzar la encaminamiento entre la red actual y la red nuevamente agregada.
- El default gateway para todos los host debe señalar al router interno.
- Usted debe agregar una ruta predeterminado en el router interno esas puntas al ASA.
- Usted debe borrar el caché del Address Resolution Protocol (ARP) en el router interno.

Configurar

Utilice la información que se describe en esta sección para configurar el ASA.

Diagrama de la red

Aquí está la topología que se utiliza para los ejemplos en este documento:

> Nota: Los esquemas de IP Addressing que se utilizan en esta configuración no son legalmente routable en Internet. Son los direccionamientos del RFC 1918 que se utilizan en un ambiente de laboratorio.

Configuración ASA 9.x

Si usted tiene la salida del **comando write terminal de** su dispositivo de Cisco, usted puede utilizar la herramienta del Output Interpreter (clientes registrados solamente) para visualizar los problemas potenciales y los arreglos.

Aquí está la configuración para el ASA que funciona con la versión de software 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
```

No prohiba a host interiores el acceso a las redes externas con la PALMADITA

Si usted se prepone tener los host interiores compartir a una sola dirección pública para la traducción, Port Address Translation (PAT) del uso. Una de las configuraciones más simples de la PALMADITA implica la traducción de todos los host internos de modo que aparezcan ser el IP de la interfaz exterior. Ésta es la configuración típica de la PALMADITA se utiliza que cuando el número de IP Address ruteables que estén disponible desde el ISP se limita solamente a algunos, o apenas uno.

Complete estos pasos para no prohibir a los host interiores el acceso a las redes externas con la PALMADITA:

1. Navegue a la **configuración** > al **Firewall** > a las **reglas NAT**, el tecleo **agrega**, y elige el **objeto de red** para configurar una regla dinámica NAT:

2. Configure la red/el host/el rango para el cual se requiere la PALMADITA dinámica. En este ejemplo, se han seleccionado todos las subredes del interior. Este proceso se debe relanzar para las subredes específicas que usted desea traducir de este modo:

3. Haga clic el **NAT**, marque la casilla de verificación **automática de la regla de traducción de la dirección del agregar**, ingrese **dinámico,** y fije la opción **traducida del addr** de modo que refleje la interfaz exterior. Si usted hace clic los puntos suspensivos, le ayudan para escoger

un objeto preconfigurado, tal como la interfaz exterior:

4. El tecleo **avanzó** para seleccionar una fuente y una interfaz de destino:

5. El Haga Click en OK, y entonces hace clic **se aplica** para aplicar los cambios. Una vez completo, el Administrador de dispositivos de seguridad adaptante (ASDM) muestra la regla NAT:

Configuración del Router B

Aquí está la configuración para el router 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
```

Verificación

Acceda un sitio web vía el HTTP a través de un buscador Web para verificar que su configuración trabaja correctamente.

Este ejemplo utiliza un sitio que se reciba en la dirección IP 198.51.100.100. Si la conexión es acertada, las salidas que se proporcionan en las secciones que siguen se pueden considerar en el ASA CLI.

Conexión

Ingrese el **comando address de la conexión de la demostración** para verificar la conexión:

```
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
```

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. El tráfico que hace juego una conexión que preexista se permite con el Firewall sin el bloqueo por una lista de control de acceso (ACL) de la interfaz.

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.

> Nota: Refiera al documento de Cisco de los indicadores de la conexión TCP ASA (acumulación y desmontaje de la conexión) para más información sobre los indicadores de la conexión.

Troubleshooting

Utilice la información que se describe en esta sección para resolver problemas los problemas de configuración.

Registros del sistema

Ingrese el **comando show log** para ver los 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)
```

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 para indicar que el Firewall ha construido una traducción; específicamente, una traducción dinámica TCP (PALMADITA). Indica la dirección IP de origen y el puerto, así como la dirección IP y el puerto traducidos, pues 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 fue configurado para bloquear este intento de conexión, o un cierto otro factor inhibió la creación de esta conexión (las restricciones de recursos o una posible configuración incorrecta), el Firewall no genera un registro para indicar que la conexión fue construida. En lugar, registra una razón de la conexión para ser negado o una indicación con respecto al factor que inhibió la conexión de ser creado.

Trazalíneas del paquete

Ingrese este comando para habilitar las funciones del trazalíneas del paquete:

```
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
```

Las funciones del trazalíneas del paquete en el ASA permiten que usted especifique un paquete *simulado* y que vea todos los diversos pasos, controles, y funciones que el Firewall complete 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 la interfaz interior.
- El protocolo se utiliza que es TCP.

- El dirección IP del cliente simulado es 192.168.1.5.
- El cliente envía el tráfico que es originado del puerto 1234.
- El tráfico se destina a un servidor en la dirección IP 198.51.100.100.
- El tráfico se destina al puerto 80.

Note que no había mención de la interfaz exterior en el comando. Esto es debido al 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.

> Consejo: Para más información sobre las funciones del trazalíneas del paquete, refiera a los paquetes del seguimiento con la sección del trazalíneas del paquete de la *guía de configuración de las 5500 Series de Cisco ASA que usa el CLI, los 8.4 y los 8.6*.

Captura

Ingrese estos comandos para aplicar una captura:

```
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 198.51.100.100ASA#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 32768ASA#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>
```

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 muestra la configuración de dos capturas nombradas **capin** y **capout** en las interfaces interior y exterior, respectivamente. **Los comandos capture** utilizan la palabra clave de la **coincidencia**, que permite que usted especifique el tráfico que usted quiere capturar.

Por el ejemplo de la captura del *capin*, se indica que usted quiere hacer juego el tráfico que se considera en la interfaz interior (ingreso o salida) ese *host 198.51.100.100 de 192.168.1.5 del host tcp de las* coincidencias. Es decir usted quiere capturar tráfico TCP que se envía del host *192.168.1.5* 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** que se define 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 puede entonces intentar establecer una conexión otra vez y proceder a ver las capturas con la **demostración capture el** comando del ***<capture_name>***. En este ejemplo, usted puede ver que el cliente puede conectar con el servidor, como evidente por el apretón de manos de tres vías TCP que se considera en las capturas.

Información Relacionada

- Cisco Adaptive Security Device Manager
- Firewall de la última generación de las 5500-X Series de Cisco ASA
- Solicitudes de comentarios (RFC)
- Guía de configuración CLI de la serie de Cisco ASA, 9.0 del Â del âÂ configurando los parásitos atmosféricos y las rutas predeterminado
- Cisco Systems del Â del âÂ del Soporte técnico y de la documentación