Conexión de la versión ASA 9.(x) de tres redes internas con el ejemplo de configuración de Internet

Contenido

Introducción

Este documento proporciona la información sobre cómo configurar la versión 9.1(5) adaptante del dispositivo de seguridad de Cisco (ASA) para el uso con tres redes internas. Las rutas estáticas se utilizan en los routers para simplificar.

Prerequisites

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en la versión 9.1(5) adaptante del dispositivo de seguridad de Cisco (ASA).

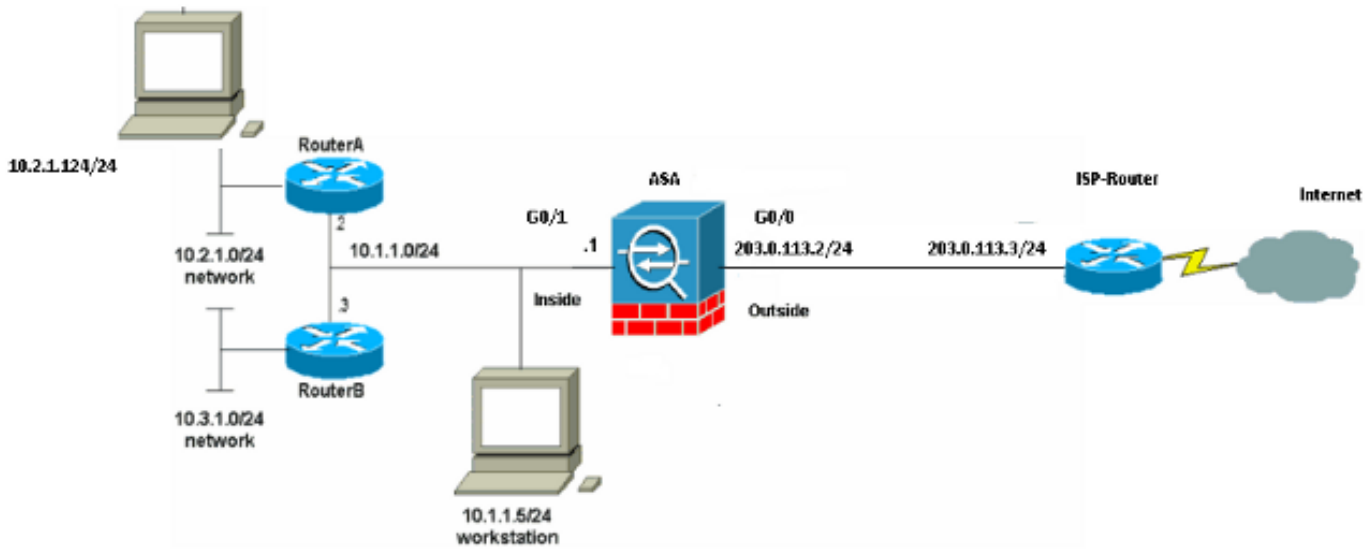
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de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

Configurar

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

> **Note**: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red



> **Note**: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

Configuración ASA 9.1

Este documento usa estas configuraciones. Si usted tiene la salida de un **comando write terminal de** su dispositivo de Cisco, usted puede utilizar el Output Interpreter (clientes registrados solamente) para visualizar los problemas potenciales y los arreglos.

Configuraciones

- Configuración del router A
- Configuración del Router B
- Configuración de la revisión 9.1 ASA y posterior

Configuración del router A

```
RouterA#show running-config
Building configuration...

Current configuration : 1151 bytes
```

```
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
memory-size iomem 25
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.2.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
```

```
!
!
!
line con 0
line 33
no activation-character
no exec
transport preferred none
transport input all
transport output all
line aux 0
line vty 0 4
password ww
login
!
!
end

RouterA#
```

Configuración del Router B

```
RouterB#show running-config
Building configuration...

Current configuration : 1132 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
!
boot-start-marker
boot-end-marker
!
!
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ip domain lookup
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
```

```
!
interface FastEthernet0/0
ip address 10.1.1.3 255.255.255.0
duplex auto
speed auto
no cdp enable
!
interface FastEthernet0/1
ip address 10.3.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
stopbits 1
line 33
no activation-character
no exec
transport preferred none
transport input all
transport output all
line aux 0
line vty 0 4
password cisco
login
!
!
end

RouterB#
```

Configuración de la revisión 9.1 ASA y posterior

```
ASA#show run
: Saved
:
ASA Version 9.1(5)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
```

```
ip address 203.0.113.2 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
boot system disk0:/asa915-k8.bin

ftp mode passive

!--- Enable informational logging to see connection creation events

logging on
logging buffered informational

!--- Output Suppressed

!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- object will get 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

!--- Output Suppressed

!--- Define a default route to the ISP router.


route outside 0.0.0.0 0.0.0.0 203.0.113.3 1

!--- Define a route to the INTERNAL router with network 10.2.1.0.

route inside 10.2.1.0 255.255.255.0 10.1.1.2 1

!--- Define a route to the INTERNAL router with network 10.3.1.0.

route inside 10.3.1.0 255.255.255.0 10.1.1.3 1

: end
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

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 10.2.1.124
16 in use, 918 most used
TCP outside 198.51.100.100:80 inside 10.2.1.124:18711, idle 0:00:16, bytes 1937,
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 y no sea bloqueada 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 | include 10.2.1.124

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.2.1.124/18711 to outside:203.0.113.2/18711

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:10.2.1.124/18711 (203.0.113.2/18711)
```

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

```
ASA(config)# show xlate local 10.2.1.124
2 in use, 180 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:10.2.1.124/18711 to outside:203.0.113.2/18711 flags ri idle
0:12:03 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 de las traducciones de NAT (xlate). 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 203.0.113.2 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 en la información sobre el NAT.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

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.

Trazalíneas del paquete

```
ASA(config)# packet-tracer input inside tcp 10.2.1.124 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 **10.2.1.124**.
- 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 10.2.1.124 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       10.2.1.124.18711 > 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 > 10.2.1.124.18711: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       10.2.1.124.18711 > 198.51.100.100.80: . ack 2123396068
win 32768



ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       203.0.113.2.18711 > 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 > 203.0.113.2.18711: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       203.0.113.2.18711 > 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**,** fue indicado que usted quiso hacer juego el tráfico visto en la interfaz interior (ingreso o salida) ese **host 198.51.100.100 de 10.2.1.124 del host tcp de las** coincidencias. Es decir usted quiere capturar tráfico TCP que se envía del **host 10.2.1.124 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 establecer 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.