Ejemplo de Configuración de ASA Versión 9.x de Conexión de Tres Redes Internas con Internet

Contenido

Introducción

Este documento proporciona información sobre cómo configurar Cisco Adaptive Security Appliance (ASA) versión 9.1(5) para su uso con tres redes internas. Las rutas estáticas se utilizan en los routers para simplificar.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en la versión 9.1(5) del Cisco Adaptive Security Appliance (ASA).

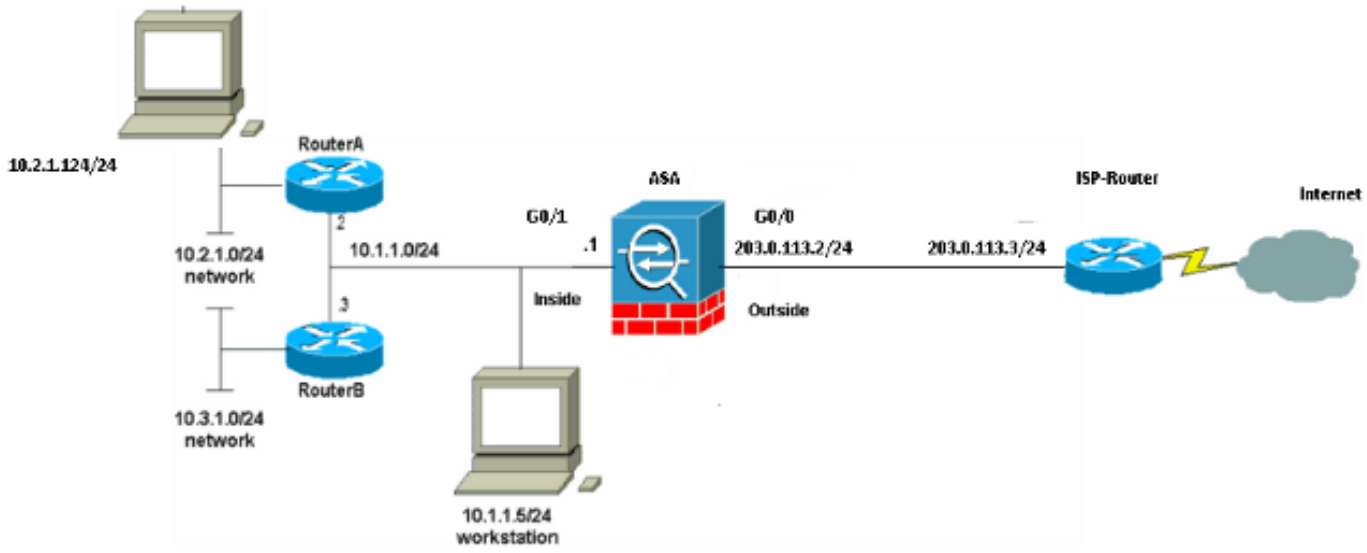
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

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

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

Diagrama de la red



> **Nota:** 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 de ASA 9.1

Este documento usa estas configuraciones. Si tiene el resultado de un comando **write terminal** de su dispositivo Cisco, puede utilizar Output Interpreter (sólo para clientes registrados) para mostrar posibles problemas y soluciones.

Configuraciones

- Configuración del router A
- Configuración del Router B
- Configuración de ASA Revision 9.1 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 ASA Revision 9.1 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 de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

Intente acceder a un sitio web a través de HTTP con un navegador web. Este ejemplo utiliza un sitio alojado en 198.51.100.100. Si la conexión se realiza correctamente, este resultado se puede ver en la CLI de ASA.

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 firewall con información de estado y se permite el retorno del tráfico desde el servidor web a través del firewall porque coincide con una ***conexión*** en la tabla de conexión del firewall. El tráfico que coincide con una conexión que existe previamente se permite a través del firewall y no está bloqueado por una ACL de interfaz.

En la salida anterior, el cliente de la interfaz interna estableció una conexión con el host 198.51.100.100 fuera de la interfaz externa. Esta conexión se realiza con el protocolo TCP y ha estado inactiva durante seis segundos. Los indicadores de conexión indican el estado actual de esta conexión. Puede encontrar más información sobre los indicadores de conexión en Indicadores de conexión TCP de 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 de ASA genera syslogs durante el funcionamiento normal. El nivel de detalle de los syslogs depende de la configuración de registro. El resultado muestra dos syslogs que se ven en el nivel seis, o en el nivel 'informativo'.

En este ejemplo, se generan dos syslogs. El primero es un mensaje de registro que indica que el firewall ha creado una traducción, específicamente una traducción TCP dinámica (PAT). Indica la dirección IP de origen y el puerto y la dirección IP traducida a medida que el tráfico atraviesa desde el interior a las interfaces externas.

El segundo syslog indica que el firewall ha creado una conexión en su tabla de conexiones para este tráfico específico entre el cliente y el servidor. Si el firewall se configuró para bloquear este intento de conexión, o algún otro factor inhibió la creación de esta conexión (restricciones de recursos o una posible configuración incorrecta), el firewall no generaría un registro que indique que la conexión se creó. En su lugar, registraría una razón para que se negara la conexión o una indicación sobre qué factor impedía que se creara la conexión.

Traducciones 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, PAT se configura para traducir las direcciones IP del host interno a las direcciones que son enrutables en Internet. Para confirmar que se crean estas traducciones, puede verificar la tabla de traducciones NAT (xlate). El comando **show xlate,** cuando se combina 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 actualmente construida para este host entre las interfaces interna y externa. La IP y el puerto del host interno se traducen a la dirección 203.0.113.2 según nuestra configuración.

Los indicadores listados, r i, indican que la traducción es **dinámica** y un **portmap**. Se puede encontrar más información sobre las diferentes configuraciones de NAT en Información sobre NAT.

Troubleshoot

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

ASA proporciona varias herramientas con las que resolver problemas de conectividad. Si el problema persiste después de verificar la configuración y verificar el resultado mencionado anteriormente, estas herramientas y técnicas pueden ayudar a determinar la causa de su falla de conectividad.

Packet Tracer

```
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
```

La función de seguimiento de paquetes en el ASA permite especificar un paquete simulado y ver todos los pasos, verificaciones y funciones que el firewall realiza cuando procesa tráfico. Con esta herramienta, es útil identificar un ejemplo de tráfico que cree que debe permitirse pasar a través del firewall y utilizar ese 5-tupple para simular tráfico. En el ejemplo anterior, se utiliza el rastreador de paquetes para simular un intento de conexión que cumpla con estos criterios:

- El paquete simulado llega al **interior**.
- El protocolo utilizado es **TCP**.
- La dirección IP del cliente simulado es 10.2.1.124.
- El cliente envía el tráfico originado en el puerto **1234**.
- El tráfico se destina a un servidor en la dirección IP 198.51.100.100.
- El tráfico está destinado al puerto 80.

Observe que no hubo mención de la interfaz **externa** en el comando. Esto es por diseño de Packet Tracer. La herramienta le indica cómo el firewall procesa ese tipo de intento de conexión, lo que incluye cómo lo enrutaría y desde qué interfaz. Se puede encontrar más información sobre el rastreador de paquetes en Seguimiento de Paquetes con Packet Tracer.

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 entra o sale de sus interfaces. Esta funcionalidad de captura es fantástica porque puede demostrar definitivamente si el tráfico llega a un firewall o sale de él. El ejemplo anterior mostró la configuración de dos capturas denominadas **capin** y **capout** en las interfaces interna y externa respectivamente. Los comandos capture utilizaron la palabra clave **match**, que le permite ser específico sobre qué tráfico desea capturar.

Para la **capa de** captura**,** se indicó que deseaba hacer coincidir el tráfico visto en la interfaz interna (entrada o salida) que coincide con el **host tcp 10.2.1.124 host 198.51.100.100**. En otras palabras, usted desea capturar cualquier tráfico TCP que se envía desde el **host 10.2.1.124** al **host 198.51.100.100** o **viceversa**. El uso de la palabra clave match permite que el firewall capture ese tráfico bidireccionalmente. El comando capture definido para la interfaz exterior no hace referencia a la dirección IP interna del cliente porque el firewall realiza PAT en esa dirección IP del cliente. Como resultado, no puede coincidir con esa dirección IP de cliente. En cambio, este ejemplo usa **any para indicar que todas las direcciones IP posibles coincidirían con esa condición.**

Después de configurar las capturas, intentaría establecer una conexión de nuevo y procedería a ver las capturas con el comando **show capture *<capture_name>***. En este ejemplo, puede ver que el cliente pudo conectarse con el servidor como se ve en el intercambio de señales TCP de 3 vías visto en las capturas.