ASA 8.3: Establecer y solucionar problemas de conectividad a través del dispositivo de seguridad de Cisco

Contenido

Introducción

Cuando se configura inicialmente un dispositivo de seguridad adaptable (ASA) de Cisco, tiene una política de seguridad predeterminada según la cual todos los que se encuentran en el interior pueden salir y nadie desde el exterior puede entrar. Si su sitio requiere una política de seguridad diferente, puede permitir que los usuarios externos se conecten con su servidor Web a través del ASA.

Una vez establecida la conectividad básica a través de Cisco ASA, puede realizar cambios en la configuración del firewall. Asegúrese de que los cambios de configuración que realice en el ASA cumplen con la política de seguridad del sitio.

Consulte PIX/ASA: Establezca y solucione problemas de conectividad a través de Cisco Security Appliance para la configuración idéntica en Cisco ASA con las versiones 8.2 y anteriores.

Prerequisites

Requirements

Este documento asume que algunas configuraciones básicas ya se han completado en Cisco ASA. Consulte estos documentos para ver ejemplos de una configuración ASA inicial:

- ASA 8.3(x): Conexión de una única red interna a Internet
- Configuración del cliente PPPoE en un Cisco Adaptive Security Appliance (ASA)

Componentes Utilizados

La información de este documento se basa en un Cisco Adaptive Security Appliance (ASA) que ejecuta la versión 8.3 y posteriores.

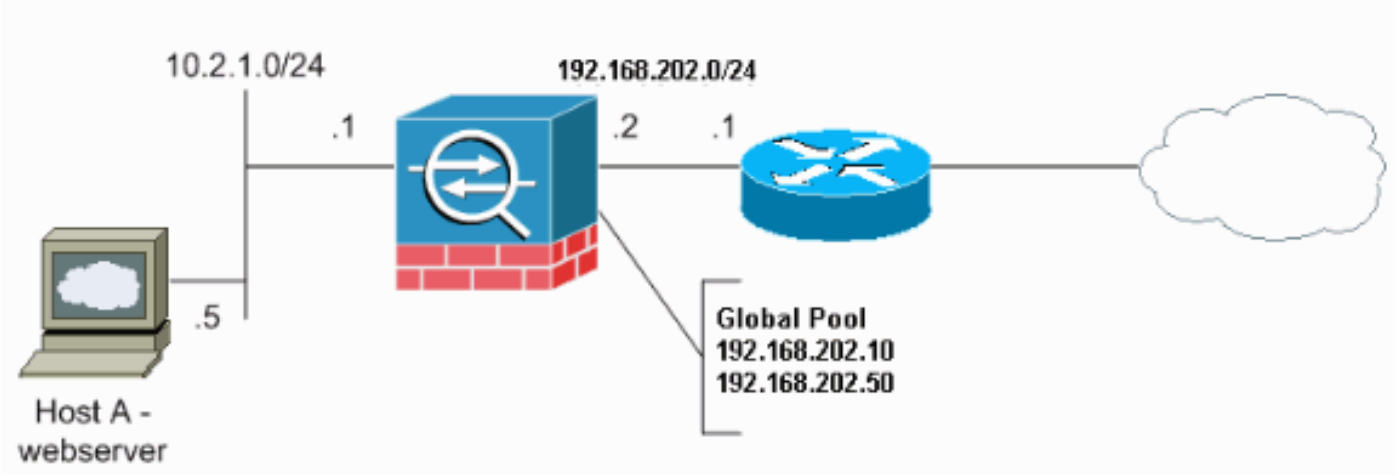
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

Cómo funciona la conectividad a través de ASA

En esta red, el Host A es el servidor de la Web con una dirección interna de 10.2.1.5 Al servidor web se le asigna una dirección externa (traducida) de 192.168.202.5. Los usuarios de Internet deben señalar a 192.168.202.5 para acceder al servidor web. La entrada DNS del servidor web debe ser esa dirección. No se permiten otras conexiones desde Internet.



Nota: Los esquemas de direccionamiento IP utilizados en esta configuración no son legalmente enrutables en Internet. Son direcciones RFC 1918 que se han utilizado en un entorno de laboratorio.

Configuración de la conectividad a través de Cisco ASA

Complete estos pasos para configurar la conectividad a través del ASA:

1. Cree un objeto de red que defina la subred interna y otro objeto de red para el intervalo del conjunto IP. Configure la NAT utilizando estos objetos de red:

```
object network inside-net
subnet 0.0.0.0 0.0.0.0
```

```
object network outside-pat-pool
range 192.168.202.10 192.168.202.50
nat (inside,outside) source dynamic inside-net  outside-pat-pool
```

2. Asigne una dirección estática traducida para el host interno al que tienen acceso los usuarios de Internet.

```
object network obj-10.2.1.5
  host 10.2.1.5
  nat (inside,outside) static 192.168.202.5
```

3. Utilice el comando **access-list** para permitir a los usuarios externos a través de Cisco ASA. Use siempre la dirección traducida en el comando access-list.

```
access-list 101 permit tcp any host 192.168.202.5 eq www
  access-group 101 in interface outside
```

Permitir Tráfico de Broadcast ARP

El dispositivo de seguridad conecta la misma red en sus interfaces internas y externas. Dado que el firewall no es un salto enrutado, puede introducir fácilmente un firewall transparente en una red existente. El redireccionamiento IP no es necesario. El tráfico IPv4 se permite a través del firewall transparente automáticamente desde una interfaz de mayor seguridad a una interfaz de menor seguridad, sin una lista de acceso. Los protocolos de resolución de direcciones (ARP) se permiten a través del firewall transparente en ambas direcciones sin una lista de acceso. El tráfico ARP se puede controlar mediante la inspección ARP. Para el tráfico de Capa 3 que viaja de una interfaz de seguridad baja a una de alta seguridad, se requiere una lista de acceso ampliada.

Nota: El dispositivo de seguridad de modo transparente no pasa paquetes de protocolo de detección de Cisco (CDP) o paquetes de IPv6, ni ningún paquete que no tenga un EtherType válido mayor o igual a 0x600. Por ejemplo, no puede pasar paquetes IS-IS. Se realiza una excepción para las unidades de datos de protocolo de puente (BPDU), que se admiten.

Direcciones MAC permitidas

Estas direcciones MAC de destino se permiten a través del firewall transparente. Las direcciones MAC que no están en esta lista se descartan:

- Dirección MAC de destino de broadcast verdadera igual a FFFF.FFFF.FFFF
- Direcciones MAC de multidifusión IPv4 desde 0100.5E00.0000 a 0100.5EFE.FFFF
- Direcciones MAC de multidifusión IPv6 desde 333.0000.0000 a 333.FFFF.FFFF
- Dirección de multidifusión BPDU igual a 0100.0CCC.CCCD
- Appletalk Multicast MAC Addresses desde 0900.0700.0000 a 0900.07FF.FFFF

Tráfico no permitido para pasar en modo de router

En el modo de router, algunos tipos de tráfico no pueden pasar a través del dispositivo de seguridad incluso si lo permite en una lista de acceso. El firewall transparente, sin embargo, puede permitir casi cualquier tráfico mediante una lista de acceso ampliada (para tráfico IP) o una

lista de acceso EtherType (para tráfico que no es IP).

Por ejemplo, puede establecer adyacencias de protocolo de ruteo a través de un firewall transparente. Puede permitir el tráfico Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP) o Border Gateway Protocol (BGP) a través de una lista de acceso ampliada. Asimismo, protocolos como el protocolo de router en espera en caliente (HSRP) o el protocolo de redundancia de router virtual (VRRP) pueden pasar a través del dispositivo de seguridad.

El tráfico que no es de IP (por ejemplo, AppleTalk, IPX, BPDU y MPLS) se puede configurar para pasar a través de una lista de acceso EtherType.

Para las funciones que no se soportan directamente en el firewall transparente, puede permitir que el tráfico pase para que los routers ascendentes y descendentes puedan soportar la funcionalidad. Por ejemplo, mediante una lista de acceso ampliada, puede permitir el tráfico del protocolo de configuración dinámica de host (DHCP) (en lugar de la función de relé DHCP no admitida) o el tráfico multidifusión, como el creado por IP/TV.

Resolución de problemas de conectividad

Si los usuarios de Internet no pueden acceder a su sitio web, siga estos pasos:

1. Asegúrese de haber ingresado las direcciones de configuración correctamente:Dirección externa válidaDirección interna correctaEl DNS externo tradujo la dirección
2. Verifique la interfaz exterior para ver si hay errores.El dispositivo de seguridad de Cisco está preconfigurado para detectar automáticamente los parámetros de velocidad y dúplex en una interfaz. Sin embargo, existen varias situaciones que pueden hacer que el proceso de negociación automática falle. Esto provoca discordancias de velocidad o dúplex (y problemas de rendimiento). Para la infraestructura de red de misión crítica, Cisco codifica manualmente la velocidad y el dúplex en cada interfaz para que no haya posibilidad de error. Estos dispositivos generalmente no se mueven. Por lo tanto, si los configura correctamente, no debe tener que cambiarlos.**Ejemplo:**
   ```
   asa(config)#interface ethernet 0/0
   asa(config-if)#duplex full
   asa(config-if)#speed 100
   asa(config-if)#exit
   ```

   En algunas situaciones, codificar la configuración de velocidad y dúplex conduce a la generación de errores. Por lo tanto, debe configurar la interfaz con la configuración predeterminada del modo de detección automática como muestra este ejemplo:**Ejemplo:**
   ```
   asa(config)#interface ethernet 0/0
   asa(config-if)#duplex auto
   asa(config-if)#speed auto
   asa(config-if)#exit
   ```

3. Si el tráfico no envía o recibe a través de la interfaz del ASA o del router de cabecera, intente borrar las estadísticas ARP.
   ```
   asa#clear arp
   ```

4. Utilice los comandos **show run object** y **show run static** para asegurarse de que la traducción estática esté habilitada.**Ejemplo:**

```
object service www
service tcp source eq www
object network 192.168.202.2
host 192.168.202.2
object network 10.2.1.5
host 10.2.1.5
object service 1025
service tcp source eq 1025
nat (inside,outside) source static 10.2.1.5 192.168.202.2 service 1025 www
```

En este escenario, la dirección IP externa se utiliza como la dirección IP asignada para el servidor web.

```
nat (inside,outside) source dynamic 10.2.1.5 interface service 1025 www
```

5. Verifique que la ruta predeterminada en el servidor web apunte a la interfaz interna del ASA.
6. Verifique la tabla de traducción usando el comando show xlate para ver si se creó la traducción.
7. Utilice el comando logging buffered para verificar los archivos de registro para ver si se producen negaciones. (Busque la dirección traducida y vea si ve negaciones.)
8. Utilice el comando capture:

```
access-list webtraffic permit tcp any host 192.168.202.5

capture capture1 access-list webtraffic interface outside
```

Nota: Este comando genera una cantidad significativa de resultados. Puede hacer que un router cuelgue o recargue bajo cargas de tráfico pesadas.

9. Si los paquetes llegan al ASA, asegúrese de que su ruta al servidor web desde el ASA sea correcta. (Verifique los comandos route en su configuración ASA.)
10. Verifique si el ARP proxy está inhabilitado. Ejecute el comando show running-config sysopt en ASA 8.3.Aquí, el ARP proxy es inhabilitado por el comando **sysopt noproxyarp outside**:

```
ciscoasa#show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt noproxyarp outside
sysopt connection permit-vpn
```

Para volver a habilitar el ARP proxy, ingrese este comando en el modo de configuración global:

```
ciscoasa(config)#no sysopt noproxyarp outside
```

Cuando un host envía tráfico IP a otro dispositivo en la misma red Ethernet, el host necesita conocer la dirección MAC del dispositivo. ARP es un protocolo de Capa 2 que resuelve una dirección IP en una dirección MAC. Un host envía una solicitud ARP y pregunta "¿Quién es esta dirección IP?". El dispositivo que posee la dirección IP responde: "Soy propietario de esa dirección IP; aquí está mi dirección MAC".Proxy ARP permite que el dispositivo de seguridad responda a una solicitud ARP en nombre de los hosts detrás de ella. Esto se hace respondiendo a las solicitudes ARP para las direcciones asignadas

estáticas de esos hosts. El dispositivo de seguridad responde a la solicitud con su propia dirección MAC y luego reenvía los paquetes IP al host interno apropiado.Por ejemplo, en el diagrama de este documento, cuando se hace una solicitud ARP para la dirección IP global del servidor web, 192.168.202.5, el dispositivo de seguridad responde con su propia dirección MAC. Si el ARP proxy no está habilitado en esta situación, los hosts de la red externa del dispositivo de seguridad no pueden alcanzar el servidor web al emitir una solicitud ARP para la dirección 192.168.202.5. Refiérase a la referencia de comandos para obtener más información sobre el comando **sysopt**.

11. Si todo parece ser correcto y los usuarios todavía no pueden acceder al servidor web, abra un caso con el Soporte Técnico de Cisco.

Mensaje de error - %ASA-4-407001:

Algunos hosts no pueden conectarse a Internet y el `mensaje de error - %ASA-4-407001: Denegar tráfico para el nombre_de_interfaz de host local:dirección_interna, el límite de licencia del número excedido` se recibe en el syslog. ¿Cómo se resuelve este error?

Se recibe este mensaje de error cuando el número de usuarios excede el límite del usuario de la licencia usada. Para resolver este error, actualice la licencia a un mayor número de usuarios. Puede ser una licencia para 50, 100 o una licencia de usuario ilimitada, según sea necesario.

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Avisos de campo de productos de seguridad (incluido Cisco Adaptive Security Appliance (ASA))
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems