ASA 8.3: Establezca y resuelva problemas la Conectividad a través del dispositivo del Cisco Security

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Cómo la Conectividad con el ASA trabaja
Conectividad de la configuración con Cisco ASA
Permita el tráfico de broadcast ARP
Direcciones MAC permitidas
Tráfico no permitido pasar en el modo del router
Resolución de problemas de conectividad
Mensaje de error - %ASA-4-407001:
Información Relacionada

Introducción

Cuando un dispositivo de seguridad adaptante de Cisco (ASA) se configura inicialmente, tiene una política de seguridad predeterminada donde todo el mundo en el interior puede salir, y nadie del 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 que usted establece la conectividad básica con Cisco ASA, usted puede realizar los cambios de configuración al Firewall. Aseegurese cualquier cambio de configuración que usted realice al ASA está de acuerdo con su política de seguridad del sitio.

Consulte PIX/ASA: Establezca y resuelva problemas la Conectividad a través del dispositivo del Cisco Security para la configuración idéntica en Cisco ASA con las versiones 8.2 y anterior.

prerrequisitos

Requisitos

Este documento asume que algunas configuraciones básicas se han completado ya en Cisco ASA. Refiera a estos documentos por ejemplos de una configuración inicial ASA:

- ASA 8.3(x): Conecte una sola red interna con Internet
- Configurando al Cliente de PPPoE en un dispositivo de seguridad adaptante de Cisco (ASA)

Componentes Utilizados

La información en este documento se basa en un dispositivo de seguridad adaptante de Cisco (ASA) esa versión 8.3 y posterior de los funcionamientos.

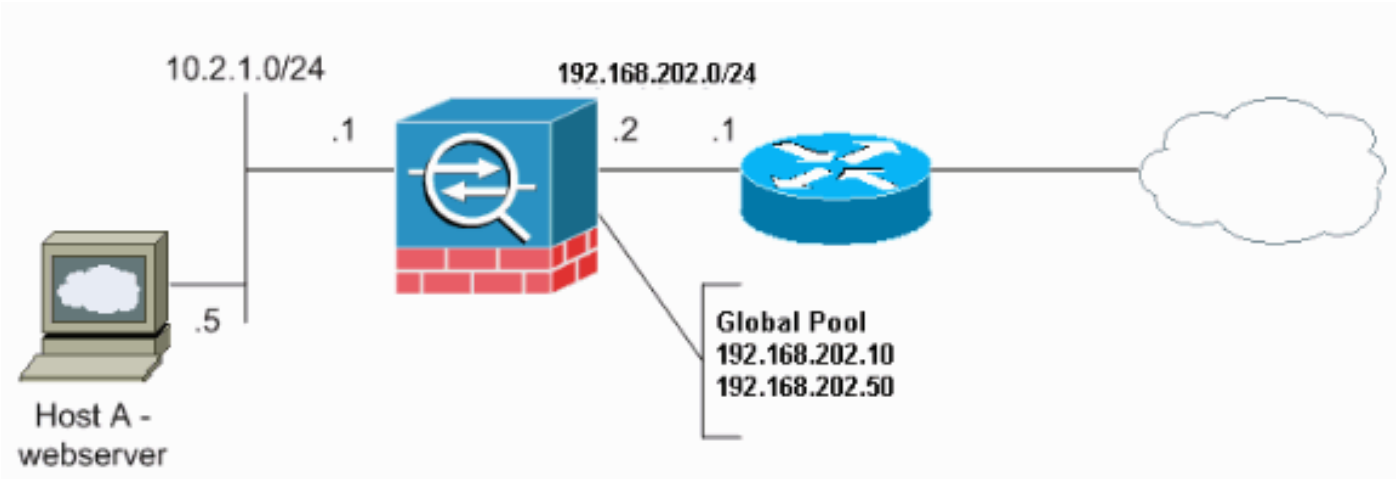
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de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

Cómo la Conectividad con el ASA trabaja

En esta red, el Host A es el servidor de la Web con una dirección interna de 10.2.1.5 Asignan el servidor Web un direccionamiento (traducido) externo de 192.168.202.5. Los usuarios de Internet deben señalar a 192.168.202.5 para acceder al servidor Web. La entrada DNS para su servidor Web necesita ser ese direccionamiento. No se permiten otras conexiones desde Internet.



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.

Conectividad de la configuración con Cisco ASA

Complete estos pasos para configurar la Conectividad con el ASA:

1. Cree un objeto de red que defina la subred interna y otro objeto de red para el rango de la agrupación IP. Configure el NAT usando 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 a una dirección estática traducida para el host interno al cual los usuarios de Internet tienen acceso.
```
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** de permitir a los usuarios externos con 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
```

Permita el tráfico de broadcast ARP

El dispositivo de seguridad conecta la misma red en sus interfaces interior y exterior. Porque el Firewall no es un salto ruteado, usted puede introducir fácilmente un Firewall transparente a una red existente. El IP que cambia la dirección no es necesario. El tráfico del IPv4 se permite con el Firewall transparente automáticamente de una interfaz de mayor seguridad a una interfaz de menor seguridad, sin una lista de acceso. Los protocolos Protocolo de resolución de la dirección (ARP) (ARP) se permiten con el Firewall transparente en las ambas direcciones sin una lista de acceso. El tráfico ARP se puede controlar por la inspección ARP. Para el tráfico de la capa 3 que viaja de un punto bajo a una interfaz de la gran seguridad, se requiere una lista de acceso ampliada.

Nota: El dispositivo de seguridad del modo transparente no pasa los paquetes del Cisco Discovery Protocol (CDP) o los paquetes del IPv6, o ninguna paquetes que no tengan un Ethertype mayor o igual un 0x600 válidos. Por ejemplo, usted no puede pasar los paquetes IS-IS. Una excepción se hace para las Unidades (BPDU), se soportan que.

Direcciones MAC permitidas

Estos direccionamientos del MAC de destino se permiten con el Firewall transparente. Las direcciones MAC no en esta lista se caen:

- VERDAD la dirección MAC del destino del broadcast igual al FFFF.FFFF.FFFF
- Multicast MAC Address del IPv4 de 0100.5E00.0000 a 0100.5EFE.FFFF
- Direcciones MAC del Multicast IPv6 a partir del 3333.0000.0000 a 3333.FFFF.FFFF
- Dirección Multicast BPDU igual a 0100.0CCC.CCCD
- Multicast MAC Address del APPLETALK a partir de la 0900.0700.0000 a 0900.07FF.FFFF

Tráfico no permitido pasar en el modo del router

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

Por ejemplo, usted puede establecer las adyacencias del Routing Protocol con un Firewall transparente. Usted puede permitir el tráfico del Open Shortest Path First (OSPF), del Routing Information Protocol (RIP), del Enhanced Interior Gateway Routing Protocol (EIGRP), o del Border Gateway Protocol (BGP) basado a través en una lista de acceso ampliada. Semejantemente, los protocolos tales como Hot Standby Router Protocol (HSRP) o el Virtual Router Redundancy Protocol (VRRP) pueden pasar a través del dispositivo de seguridad.

El tráfico no IP (por ejemplo, APPLETALK, IPX, BPDU, y MPLS) se puede configurar para pasar con usar una lista de acceso del Ethertype.

Para las características que no se soportan directamente en el Firewall transparente, usted puede permitir que el tráfico pase a través de modo que el Routers en sentido ascendente y descendente pueda soportar las funciones. Por ejemplo, usando una lista de acceso ampliada, usted puede permitir el tráfico del Protocolo de configuración dinámica de host (DHCP) (en vez de la función de Relay DHCP sin apoyo) o el tráfico Multicast tal como eso creada por el IP/TV.

Resolución de problemas de conectividad

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

1. Aseegurese le haber ingresado a las direcciones de configuración correctamente:Dirección externa válidaDirección interna correctaEl DNS externo tradujo la dirección
2. Marque la interfaz exterior para los errores.El dispositivo del Cisco Security se preconfigura auto-para detectar las configuraciones de la velocidad y dúplex en una interfaz. Sin embargo, varias situaciones existen que pueden hacer el proceso de negociación automática fallar. Esto da lugar a la velocidad o las discordancias dúplex (y los 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 no se mueven generalmente alrededor. Por lo tanto, si usted los configura correctamente, usted no debe necesitar 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, poner en hard-code las configuraciones de la velocidad y dúplex llevan a la generación de errores. Por lo tanto, usted necesita configurar la interfaz a la configuración predeterminada de auto-detecta el modo mientras que este ejemplo muestra:**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 ni recibe a través de la interfaz del ASA o del router de cabecera, intente borrar las estadísticas ARP.`asa#clear arp`
4. Utilice el **objeto del funcionamiento de la demostración** y **muestre los comandos static del funcionamiento** para aseegurarse que la traducción estática está 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, el IP Address externo se utiliza como la dirección IP asociada para el servidor Web.
   `nat (inside,outside) source dynamic 10.2.1.5 interface service 1025 www`
5. Marque para ver que la ruta predeterminado en el servidor Web señala a la interfaz interior del ASA.
6. Marque la tabla de traducción usando el comando show xlate para ver si la traducción fue creada.
7. Utilice el comando logging buffered para marcar los archivos del registro para ver si niega ocurren. (Busque a la dirección traducida y vea si usted ve ningunos niega.)
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 a un router colgar o recargar bajo cargas de tráfico intenso.

9. Si los paquetes lo hacen al ASA, aseegurese su ruta al servidor Web del ASA está correcto. (Marque los comandos route en su configuración ASA.)
10. Marque para ver si se inhabilita el proxy ARP. Publique el comando show running-config sysopt en ASA 8.3.Aquí, el proxy ARP es inhabilitado por el **noproxyarp del sysopt fuera del** comando:`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 permitir el proxy ARP, ingrese este comando en el modo de configuración global:`ciscoasa(config)#`**`no sysopt noproxyarp outside`** Cuando un host envía el tráfico IP a otro dispositivo en la misma red Ethernet, las necesidades del host de conocer la dirección MAC del dispositivo. El ARP es un protocolo de la capa 2 que resuelve una dirección IP a una dirección MAC. Un host envía un pedido ARP y pide “quién es esta dirección IP?”. El dispositivo que posee la dirección IP contesta, “poseo esa dirección IP; aquí está mi dirección MAC.”El proxy ARP permite que el dispositivo de seguridad conteste a un pedido ARP en nombre de los host detrás de él. Hace esto contestando a los pedidos ARP para los direccionamientos asociados los parásitos atmosféricos de esos host. El dispositivo de seguridad responde a la petición con su propia dirección MAC, entonces adelante los paquetes del IP al host interior apropiado.Por ejemplo, en el diagrama en este documento, cuando un pedido ARP se hace para el IP Address global del servidor Web, 192.168.202.5, el dispositivo de seguridad responde con su propia dirección MAC. Si el proxy ARP no se habilita en esta situación, los host en la red externa del dispositivo de seguridad no pueden alcanzar al servidor Web publicando un pedido ARP para el direccionamiento 192.168.202.5. Refiera a la referencia de comandos para más información sobre el comando sysopt.
11. Si todo aparece estar 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 host no pueden conectar con Internet y el `mensaje de error - %ASA-4-407001: Negar el tráfico para el interface_name del host local: los inside_address, límite de la licencia de` mensaje de error `excedido número` se reciben 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 número más elevado de los usuarios. Ésta puede ser 50, 100, o licencia del usuario ilimitado como sea necesario.

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Field Notice de seguridad del producto (dispositivo de seguridad adaptante incluyendo de Cisco (ASA))
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems