ASA 7.x/PIX 6.x y Versiones Posteriores: Ejemplo de Configuración para Abrir o Bloquear los Puertos

Contenido

Introducción

Este documento proporciona un ejemplo de configuración sobre cómo abrir o bloquear los puertos para diversos tipos de tráfico, tales como http o ftp, en el dispositivo Security Appliance.

Nota: Los términos “que abren el puerto” y “que permiten el puerto” entregan el mismo significado. Del mismo modo, "bloqueando el puerto" y "restringiendo el puerto" también significan lo mismo.

prerrequisitos

Requisitos

Este documento supone que PIX/ASA está configurado y funciona correctamente.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- El dispositivo de seguridad adaptante de las Cisco 5500 Series (ASA) ese funciona con la

versión 8.2(1)
- Versión 6.3(5) del Cisco Adaptive Security Device Manager (ASDM)

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.

Productos Relacionados

Esta configuración también se puede utilizar con el Cisco 500 Series PIX Firewall Appliance con la versión de software 6.x o posteriores.

Convenciones

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

Configurar

Cada interfaz debe tener un nivel de seguridad de 0 (más bajo) a 100 (más alto). Por ejemplo, usted debe asignar su red más segura, tal como la red del host interior, al nivel 100. Mientras que la red externa que está conectada con Internet puede ser el nivel 0, otras redes, tales como DMZ, se pueden colocar mientras tanto. Puede asignar múltiples interfaces al mismo nivel de seguridad.

De forma predeterminada, todos los puertos se bloquean en la interfaz externa (nivel de seguridad 0) y todos los puertos se abren en la interfaz interna (nivel de seguridad 100) del dispositivo de seguridad. De este modo, todo el tráfico saliente puede pasar a través del dispositivo de seguridad sin necesidad de una configuración, pero el acceso del tráfico entrante debe autorizarse mediante la configuración de la lista de acceso y los comandos estáticos en el dispositivo de seguridad.

Nota: Todos los puertos se bloquean generalmente de la zona de Seguridad más baja a la zona de mayor seguridad, y todos los puertos están abiertos de la zona de mayor seguridad a la zona de Seguridad más baja que proporciona a que la inspección con estado está habilitada para ambos tráfico entrante y saliente.

Esta sección comprende las siguientes subsecciones:

- Diagrama de la red
- Configuración de Bloqueo de los Puertos
- Configuración de Apertura de los Puertos

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

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Configuración de Bloqueo de los Puertos

El dispositivo de seguridad permite cualquier tráfico saliente, excepto que esté explícitamente bloqueado por una lista de acceso extendido.

Una lista de acceso está conformada por una o más Access Control Entries (ACE). Según el tipo de lista de acceso, usted puede especificar las direcciones de origen y destino, el protocolo, los puertos (para TCP o UDP), el tipo ICMP (para ICMP) o EtherType.

Nota: Para los protocolos sin conexión, tales como ICMP, el dispositivo de seguridad establece las sesiones unidireccionales, así que usted o necesita las Listas de acceso permitir el ICMP en las ambas direcciones (por la aplicación de las Listas de acceso a la fuente y a las interfaces de destino), o usted necesita habilitar el motor de la inspección icmp. El motor de inspección del ICMP trata las sesiones del ICMP como conexiones bidireccionales.

Siga estos pasos para bloquear los puertos, que generalmente se aplican al tráfico que se origina desde la zona interna (zona de seguridad más alta) a la DMZ (zona de seguridad más baja) o desde la DMZ a la zona externa.

1. Cree una Access Control List (ACL) de forma que bloquee el tráfico del puerto especificado.
   access-list <name> extended deny <protocol> <source-network/source IP> <source-netmask> <destination-network/destination IP> <destinamtion-netmask> eq <port number> access-list <name> extended permit ip any any
2. Luego vincule la lista de acceso con el comando **access-group** para activarla.
   access-group <access list name> in interface <interface name>

Ejemplos:

1. **Bloqueo del tráfico del puerto HTTP:** Para bloquear el acceso de la red interna 10.1.1.0 al http (servidor Web) con IP 172.16.1.1 ubicada en la red DMZ, cree una ACL como se indica a continuación:`ciscoasa(config)#`**`access-list 100 extended deny tcp 10.1.1.0 255.255.255.0 host 172.16.1.1 eq 80`** `ciscoasa(config)#`**`access-list 100 extended permit ip any any`** `ciscoasa(config)#`**`access-group 100 in interface inside`** **Nota:** Utilice **ningún** seguido por los comandos access list para quitar el bloqueo del puerto.
2. **Bloqueo del tráfico del puerto FTP:** Para bloquear el acceso de la red interna 10.1.1.0 al FTP (servidor de archivos) con IP 172.16.1.2 ubicada en la red DMZ, cree una ACL como se indica a continuación:`ciscoasa(config)#`**`access-list 100 extended deny tcp 10.1.1.0 255.255.255.0 host 172.16.1.2 eq 21`** `ciscoasa(config)#`**`access-list 100 extended permit ip any any`** `ciscoasa(config)#`**`access-group 100 in interface inside`**

Nota: Refiera a los puertos IANA para aprender más información sobre las asignaciones de puertos.

La configuración gradual para realizar esto con el ASDM se muestra en esta sección.

1. Vaya a la **configuración > al Firewall > a las reglas de acceso**. El tecleo **agrega la regla de acceso** para crear la lista de acceso.
2. Defina la fuente y el destino y la acción de la regla de acceso junto con la interfaz que esta regla de acceso será asociada. Seleccione los detalles elegir el puerto específico para bloquear.
3. Elija el **HTTP de la** lista de puertos disponibles, después haga clic la **AUTORIZACIÓN** para invertir de nuevo a la ventana de la regla de acceso del agregar.
4. Haga Click en OK para completar la configuración de la regla de acceso.

5. **Separador de millares del** tecleo **después** para agregar una regla de acceso a la misma lista de acceso.
6. Permita que el tráfico de “” a “” prevenga el “implícito niegan”. Entonces, **AUTORIZACIÓN del** tecleo a completar agregando esta regla de acceso.
7. La lista de acceso configurada se puede considerar en las reglas de acceso que el tecleo de cuadro **se aplica** para enviar esta configuración al dispositivo de seguridad.La configuración enviada del ASDM da lugar a este conjunto de comandos en el comando line interface(cli) del ASA.`access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq www`
`access-list inside_access_in extended permit ip any any`
`access-group inside_access_in in interface inside`Con estos pasos, el ejemplo 1 se ha realizado con el ASDM para bloquear la red de 10.1.1.0 de acceder al servidor Web, 172.16.1.1. El ejemplo 2 se puede también alcanzar de la misma manera para bloquear la red entera de 10.1.1.0 de acceder al servidor FTP, 172.16.1.2. La única diferencia estará actualmente elegir el puerto.**Nota:** Esta configuración por ejemplo 2 de la regla de acceso se asume para ser una configuración nueva.
8. Defina la regla de acceso para bloquear el tráfico FTP, después haga clic la lengueta de los **detalles** para elegir el puerto destino.
9. Elija el puerto **ftp** y haga clic la **AUTORIZACIÓN** para invertir de nuevo a la ventana de la regla de acceso del agregar.
10. Haga Click en OK para completar la configuración de la regla de acceso.
11. Agregue otra regla de acceso para permitir cualquier otro tráfico. Si no, el implícitos niegan la regla bloquearán todo el tráfico en esta interfaz.
12. La configuración de la lista de acceso completa parece esto bajo lengueta de las reglas de acceso.
13. El tecleo **se aplica** para enviar la configuración al ASA. La configuración CLI equivalente parece esto:`access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq ftp`
`access-list inside_access_in extended permit ip any any`
`access-group inside_access_in in interface inside`

Configuración de Apertura de los Puertos

El dispositivo de seguridad no permite ningún tráfico entrante, excepto que esté explícitamente autorizado por una lista de acceso extendido.

Si desea permitir el acceso de un host externo a un host interno, puede aplicar una lista de acceso entrante en la interfaz externa. Debe especificar la dirección traducida del host interno en la lista de acceso porque esta dirección es la que puede utilizarse en la red externa. Siga estos pasos para abrir los puertos desde la zona de seguridad más baja a la zona de seguridad más alta. Por ejemplo, permita el tráfico desde la interfaz externa (zona de seguridad más baja) a la interna (zona de seguridad más alta) o desde la DMZ a la interfaz interna.

1. El NAT estático crea una traducción fija de una dirección real a un direccionamiento asociado. Esta dirección asignada es una dirección que los hosts en Internet pueden utilizar para acceder al servidor de la aplicación de la DMZ sin necesidad de conocer la dirección real del servidor.
`static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask] | access-list access_list_name | interface}` Consulte la sección NAT Estática de Referencia de comandos para PIX/ASA para obtener más información.

2. Cree una ACL para permitir el tráfico del puerto específico.
   access-list <name> extended permit <protocol> <source-network/source IP> <source-netmask> <destination-network/destination IP> <destinamtion-netmask> eq <port number>
3. Vincule la lista de acceso con el comando **access-group** para activarla.
   access-group <access-list name> in interface <interface name>

Ejemplos:

1. **Apertura del tráfico del puerto SMTP:** Abra el puerto **tcp 25** para permitir que los hosts externos (Internet) accedan al servidor de correo ubicado en la red DMZ.El comando **Static** asigna la dirección externa 192.168.5.3 a la dirección DMZ real 172.16.1.3.`ciscoasa(config)#`**`static (DMZ,Outside) 192.168.5.3 172.16.1.3 netmask 255.255.255.255`** `ciscoasa(config)#`**`access-list 100 extended permit tcp any host 192.168.5.3 eq 25`** `ciscoasa(config)#`**`access-group 100 in interface outside`**
2. **Apertura del tráfico del puerto HTTPS:** Abra el puerto **tcp 443** para permitir que los hosts externos (Internet) accedan al servidor Web (seguro) ubicado en la red DMZ.`ciscoasa(config)#`**`static (DMZ,Outside) 192.168.5.5 172.16.1.5 netmask 255.255.255.255`** `ciscoasa(config)#`**`access-list 100 extended permit tcp any host 192.168.5.5 eq 443`** `ciscoasa(config)#`**`access-group 100 in interface outside`**
3. **Autorización del tráfico de DNS:** Abra el puerto **udp 53** para permitir a los hosts externos (Internet) acceder al servidor DNS (seguro) ubicado en la red DMZ.`ciscoasa(config)#`**`static (DMZ,Outside) 192.168.5.4 172.16.1.4 netmask 255.255.255.255`** `ciscoasa(config)#`**`access-list 100 extended permit udp any host 192.168.5.4 eq 53`** `ciscoasa(config)#`**`access-group 100 in interface outside`**

Nota: Refiera a los puertos IANA para aprender más información sobre las asignaciones de puertos.

Configuración con el ASDM

Un acercamiento gradual para realizar las tareas antedichas con el ASDM se muestra en esta sección.

1. Cree la regla de acceso para permitir el tráfico smtp al servidor de 192.168.5.3.
2. Defina la fuente y el destino de la regla de acceso, y la interfaz los lazos de esta regla con. También, defina la acción como **permiso**.
3. Elija el **S TP** como el puerto, después haga clic la **AUTORIZACIÓN**.
4. Haga Click en OK a completar configurando la regla de acceso.
5. Configure el NAT estática para traducir 172.16.1.3 a 192.168.5.3Va a la **configuración > al Firewall > la regla NAT estática a las reglas NAT > Add** para agregar una entrada NAT estática.Seleccione la fuente original y la dirección IP traducida junto con sus interfaces asociadas, después haga clic la **AUTORIZACIÓN** para acabar de configurar la regla NAT estática.Esta imagen representa las tres reglas estáticas que se enumeran en la sección de los ejemplos:Esta imagen representa las tres reglas de acceso que se enumeran en la sección de los ejemplos:

Verificación

Puede verificar con determinados comandos **show**, como se indica a continuación:

- **show xlate**: muestra la información de la traducción actual
- **show access-list**: muestra los contadores de aciertos para las políticas de acceso

- **show logging**: muestra los registros en el buffer

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- PIX/ASA 7.x: Comunicación del permiso/de la neutralización entre las interfaces
- PIX 7.0 y puerto adaptante Redirection(Forwarding) del dispositivo de seguridad con nacional, global, estático, el conducto, y los comandos access-list
- Usando nacional, global, estático, conducto, y comandos access-list y redirección de puerto (expedición) en el PIX
- PIX/ASA 7.x: El permiso FTP/TFTP mantiene el ejemplo de configuración
- PIX/ASA 7.x: Ejemplo de configuración de los servicios del permiso VoIP (SIP,MGCP,H323,SCCP)
- PIX/ASA 7.x: Acceso del mail server en el ejemplo de la configuración de DMZ
- Soporte Técnico y Documentación - Cisco Systems