El evitar/que bloquea en el IPS por el ejemplo de la configuración del router ASA/PIX/IOS

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Antecedentes
Configure el sensor para manejar a los routeres Cisco
Configure los perfiles del usuario
Routers y ACL
Routeres Cisco de la configuración que usan el CLI
Configure el sensor para manejar los Firewall de Cisco
El bloque con EVITA en el PIX/ASA
Información Relacionada

Introducción

Este documento describe cómo configurar evitar en un router IOS PIX/ASA/Cisco con la ayuda del IPS de Cisco. El ARCO, la aplicación de bloqueo en el sensor, comienza y los bloques de las paradas en el Routers, Cisco 5000 RS y los Catalyst 6500 Series Switch, los Firewall PIX, el FWSM, y el ASA. El ARCO publica un bloque o lo evita al dispositivo administrado para la dirección IP malévola. El ARCO envía el mismo bloque a todos los dispositivos que el sensor maneje. Si se configura un sensor del bloqueo principal, el bloque se remite a y se publica de este dispositivo. ARC monitorea el tiempo para el bloque y elimina el bloque una vez que caduca.

Cuando usted utiliza IPS 5.1, el particular cuidado debe ser tomado cuando el evitar a los Firewall en el modo de contexto múltiple como ninguna información de VLAN se envía con la petición del evitar.

Nota: El bloqueo no se soporta en el contexto admin de un contexto múltiple FWSM.

Hay tres tipos de bloques:

- Bloque del host — Bloquea todo el tráfico de una dirección IP dada.
- Bloque de la conexión — Los bloques trafican de una dirección IP de origen dada a una dirección IP y a un puerto destino del destino determinado.Los bloques de la conexión múltiple de la misma dirección IP de origen a un diverso IP Address de destino o al puerto destino conmutan automáticamente el bloque de un bloque de la conexión a un bloque del host.**Nota:** Los bloques de la conexión no son soportados por los dispositivos de seguridad.

Bloques del host del soporte de los dispositivos de seguridad solamente con la información de puerto y protocolo opcional.
- Bloque de la red — Bloquea todo el tráfico de una red dada.Usted puede iniciar los bloques del host y de la conexión manualmente o automáticamente cuando se acciona una firma. Usted puede iniciar solamente los bloques de la red manualmente.

Para los bloques automáticos, usted debe elegir el host del bloque de petición o la conexión del bloque de petición como la acción del evento para las firmas determinadas, de modo que SensorApp envíe una petición del bloque DE FORMAR ARCOS cuando se acciona la firma. Una vez que el ARCO recibe la petición del bloque de SensorApp, pone al día las configuraciones del dispositivo para bloquear el host o la conexión. Refiera a asignar las acciones a las firmas, pagine 5-22 para más información sobre el procedimiento para agregar las acciones del host del bloque de petición o del evento de conexión del bloque de petición a la firma. Refiera a configurar la acción del evento reemplaza, pagina 7-15 para más información sobre el procedimiento para la configuración de reemplaza que agrega las acciones del host del bloque de petición o del evento de conexión del bloque de petición a las alarmas de los grados de riesgo específicos.

En los routeres Cisco y los Catalyst 6500 Series Switch, el ARCO crea los bloques aplicando los ACL o los VACL. Los ACL y los VACL aplican los filtros a las interfaces, que incluye la dirección, y a los VLA N, respectivamente para tráfico del permit or deny. El firewall PIX, el FWSM, y el ASA no utilizan los ACL o los VACL. El accesorio **evita** y no se utiliza a **ningún comando shun**.

Esta información se requiere para la configuración del ARCO:

- Inicie sesión la identificación del usuario, si el dispositivo se configura con el AAA
- Contraseña de inicio de sesión
- Contraseña habilitada, que no es necesaria si el usuario tiene privilegios del permiso
- Interfaces que se manejarán, por ejemplo, ethernet0, vlan100
- Cualquier información existente ACL o VACL que usted quiera aplicado al principio (PRE-bloque ACL o VACL) o final (Poste-bloque ACL o VACL) del ACL o del VACL se crea que. Esto no se aplica a un firewall PIX, a un FWSM, o a un ASA porque no utilizan los ACL o los VACL para bloquear.
- Si usted utiliza Telnet o SSH para comunicar con el dispositivo
- IP Addresses (host o rango de los host) que usted nunca quiere bloqueado
- Cuánto tiempo usted quisiera que los bloques duraran

prerrequisitos

Requisitos

Antes de que usted configure el ARCO para bloquear o valore la limitación, usted debe completar estas tareas:

- Analice su topología de red para entender qué dispositivos deben ser bloqueados por los cuales el sensor, y que dirige debe nunca ser bloqueado.
- Recolecte los nombres de usuario, las contraseñas del dispositivo, las contraseñas habilitadas, y los tipos de conexiones (Telnet o SSH) necesitaron iniciar sesión a cada dispositivo.
- Conozca los nombres de la interfaz en los dispositivos.
- Conozca los nombres del PRE-bloque ACL o VACL y el Poste-bloque ACL o VACL si es

necesario.
- Entienda qué interfaces deben y no deben ser bloqueadas y en qué dirección (en o hacia fuera).

Componentes Utilizados

La información en este documento se basa en el Cisco Intrusion Prevention System 5.1 y posterior.

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.

Nota: Por abandono, el ARCO se configura para un límite de 250 entradas de bloque. Refiera a los dispositivos del soporte para más información sobre la lista de dispositivos de bloqueo soportados por el ARCO.

Convenciones

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

Antecedentes

Utilice el panel de propiedades de bloqueo para configurar las configuraciones básicas requeridas para habilitar el bloqueo y para valorar la limitación.

El ARCO controla el bloqueo y valora la limitación de las acciones en los dispositivos administrados.

Usted debe ajustar su sensor para identificar los host y las redes que deben nunca ser bloqueados. Es posible que el tráfico de un dispositivo confiable encienda una firma. Si esta firma se configura para bloquear el atacante, el tráfico de la red legítimo puede ser afectado. La dirección IP del dispositivo se puede nunca enumerar en la lista del bloqueo para prevenir este escenario.

Un netmask especificado en nunca una entrada de bloque nunca se aplica al direccionamiento de bloque. Si no se especifica ningún netmask, una máscara de /32 del valor por defecto es aplicada.

Nota: Por abandono, el sensor no se permite para publicar un bloque para su propia dirección IP mientras que éste interfiere con la comunicación entre el sensor y el dispositivo de bloqueo. Pero, esta opción es configurable por el usuario.

Una vez que el ARCO se configura para manejar un dispositivo de bloqueo, el dispositivo de bloqueo evita y los ACL/los VACL que se utilizan para bloquear no se deben alterar manualmente. Esto puede causar una interrupción del servicio del ARCO y puede dar lugar a los bloques futuros que no son publicados.

Nota: Por abandono, solamente el bloqueo se soporta en los dispositivos Cisco IOS. Usted puede reemplazar el valor por defecto de bloqueo si usted elige la tarifa que limita o que bloquea más la

limitación de la tarifa.

Para publicar o alterar los bloques, el usuario IPS debe tener el papel del administrador o del operador.

Configure el sensor para manejar a los routeres Cisco

Esta sección describe cómo configurar el sensor para manejar a los routeres Cisco. Contiene estos temas:

- Perfiles del usuario de la configuración
- Routers y ACL
- Routeres Cisco de la configuración que usan el CLI

Perfiles del usuario de la configuración

El sensor maneja los otros dispositivos con el comando del *profile_name de los* **perfiles del usuario** para configurar los perfiles del usuario. Los perfiles del usuario contienen el userid, la contraseña, y la información de contraseña habilitada. Por ejemplo, el Routers que todo comparte las mismas contraseñas y nombres de usuario puede estar bajo un perfil del usuario.

Nota: Usted **debe** crear un perfil del usuario antes de que usted configure el dispositivo de bloqueo.

Complete estos pasos para configurar los perfiles del usuario:

1. Inicie sesión al CLI con una cuenta que tenga privilegios de administrador.
2. Ingrese el modo de acceso a la red.`sensor#`**`configure terminal`** `sensor(config)#`**`service network-access`** `sensor(config-net)#`
3. Cree el nombre del perfil del usuario.`sensor(config-net)#`**`user-profiles`** *`PROFILE1`*
4. Teclee el nombre de usuario para ese perfil del usuario.`sensor(config-net-use)#`**`username`** *`username`*
5. Especifique la contraseña para el usuario.`sensor(config-net-use)#` **`password`** `Enter password[]: ******** Re-enter password ********`
6. Especifique la contraseña habilitada para el usuario.`sensor(config-net-use)#` **`enable-password`** `Enter enable-password[]: ******** Re-enter enable-password ********`
7. Verifique las configuraciones.`sensor(config-net-use)#`**`show settings`** `profile-name: PROFILE1 ---------------------------------------------- enable-password: <hidden> password: <hidden> username: jsmith default: ---------------------------------------------- sensor(config-net-use)#`
8. Salga el submode del acceso a la red.`sensor(config-net-use)#`**`exit`** `sensor(config-net)#`**`exit`** `Apply Changes:?[yes]:`
9. Presione ENTER para aplicar los cambios o ingresar no para desecharlos.

Routers y ACL

Cuando el ARCO se configura con un dispositivo de bloqueo que utilice los ACL, los ACL se componen de esta manera:

1. Una línea del permiso con la dirección IP del sensor o, si está especificado, el direccionamiento NAT del sensor**Nota:** Si usted permite que el sensor sea bloqueado, esta

línea no aparece en el ACL.
2. PRE-bloque ACL (si está especificado)Este ACL debe existir ya en el dispositivo.**Nota:** El ARCO lee las líneas en el ACL preconfigurado y copia estas líneas al comienzo del bloque ACL.
3. Cualquier bloques activos
4. Cualquiera: IP cualquier ninguno del permiso ACL/del Poste-bloque- Poste-**bloque ACL** (si está especificado)Este ACL debe existir ya en el dispositivo.**Nota:** El ARCO lee las líneas en el ACL y copia estas líneas al final del ACL.**Nota:** Aseegurese la línea más reciente del ACL es IP cualquier ninguno del permiso si usted quisiera que todos los paquetes incomparables fueran permitidos.- **IP cualquier ninguno del permiso** (no utilizado si se especifica un Poste-bloque el ACL)

Nota: Los ACL que el ARCO hace se debe nunca modificar por usted o cualquier otro sistema. Estos ACL son temporales y los nuevos ACL son creados constantemente por el sensor. Las únicas modificaciones que usted puede hacer están al PRE y al Poste-bloque ACL.

Si usted necesita modificar el PRE-bloque o el Poste-bloque ACL, complete estos pasos:

1. Inhabilite el bloqueo en el sensor.
2. Realice los cambios a la configuración del dispositivo.
3. Reenable que bloquea en el sensor.

Cuando se vuelve a permitir el bloqueo, el sensor lee la nueva configuración del dispositivo.

Nota: Un solo sensor puede manejar los dispositivos múltiples, pero los sensores múltiples no pueden manejar un único dispositivo. En caso de que los bloques publicados de los sensores múltiples se signifiquen para un solo dispositivo de bloqueo, un sensor del bloqueo principal se debe incorporar en el diseño. Un sensor de bloqueo principal recibe el bloqueo de las peticiones de los sensores múltiples y publica todas las peticiones de bloqueo al dispositivo de bloqueo.

Usted crea y salva el PRE-bloque y el Poste-bloque ACL en su configuración del router. Estos ACL deben ser el IP ampliado ACL, nombrado o numerado. Vea su documentación del router para más información sobre cómo crear los ACL.

Nota: El PRE-bloque y el Poste-bloque ACL no se aplican para valorar la limitación.

Los ACL son de arriba hacia abajo evaluado y se toman medidas de la primero-coincidencia. El PRE-bloque ACL puede contener un permiso que tomaría la precedencia sobre una negación que resultó de un bloque.

El Poste-bloque ACL se utiliza para explicar cualquier condición no manejada por el PRE-bloque ACL o los bloques. Si usted tiene un ACL existente en la interfaz y en la dirección que los bloques se publican, ese ACL se puede utilizar como el Poste-bloque ACL. Si usted no tiene un Poste-bloque ACL, los separadores de millares del sensor permiten el IP cualquier en el final del nuevo ACL.

Cuando el sensor empieza para arriba, lee el contenido de los dos ACL. Crea un tercer ACL con estas entradas:

- Una línea del permiso para la dirección IP del sensor
- Copias de todas las líneas de configuración del PRE-bloque ACL
- Una línea de la negación para cada direccionamiento que es bloqueado por el sensor
- Copias de todas las líneas de configuración del Poste-bloque ACL

El sensor aplica el nuevo ACL a la interfaz y la dirección que usted señala.

Nota: Cuando el nuevo bloque ACL se aplica a una interfaz del router, en una dirección particular, substituye cualquier ACL preexistente en esa interfaz en esa dirección.

Routeres Cisco de la configuración que usan el CLI

Complete estos pasos para configurar un sensor para manejar a un router Cisco para realizar el bloqueo y para valorar la limitación:

1. Inicie sesión al CLI con una cuenta que tenga privilegios de administrador.
2. Ingrese el submode del acceso a la red.`sensor#`**`configure terminal`** `sensor(config)#`**`service network-access`** `sensor(config-net)#`
3. Especifique la dirección IP para el router controlado por el ARCO.`sensor(config-net)#`**`router-devices`** *`ip_address`*
4. Ingrese el nombre de dispositivo lógico que usted creó cuando usted configuró el perfil del usuario.`sensor(config-net-rou)#`**`profile-name`** *`user_profile_name`* El ARCO valida cualquier cosa que usted ingresa. No marca para ver si existe el perfil del usuario.
5. Especifique el método usado para acceder el sensor.`sensor(config-net-rou)#` **`communication {telnet | ssh-des | ssh-3des}`** Si está sin especificar, se utiliza SSH 3DES.**Nota:** Si usted utiliza el DES o el 3DES, usted debe utilizar el **comando ip_address de la clave de host del ssh** para validar la clave de SSH del dispositivo.
6. Especifique el direccionamiento del sensor NAT.`sensor(config-net-rou)#`**`nat-address`** *`nat_address`* **Nota:** Esto cambia la dirección IP en la primera línea del ACL del direccionamiento del sensor al direccionamiento NAT. El direccionamiento NAT es el direccionamiento del sensor, poste-NAT, traducido por un dispositivo intermediario, situado entre el sensor y el dispositivo de bloqueo.
7. Especifique si el router realiza el bloqueo, valore la limitación, o ambas.**Nota:** El valor por defecto está bloqueando. Usted no tiene que configurar las capacidades de la respuesta si usted quisiera que el router realizara el bloqueo solamente.Tarifa que limita solamente`sensor(config-net-rou)#`**`response-capabilities rate-limit`** Bloqueando y valore la limitación`sensor(config-net-rou)#`**`response-capabilities block|rate-limit`**
8. Especifique el nombre y la dirección de la interfaz.`sensor(config-net-rou)#`**`block-interfaces`** *`interface_name`* **`{in | out}`** **Nota:** El nombre de la interfaz debe ser una abreviatura que el router reconoce cuando está utilizado después del **comando interface**.
9. (Opcional) agregue el nombre PRE-ACL (que bloquea solamente).`sensor(config-net-rou-blo)#`**`pre-acl-name`** *`pre_acl_name`*
10. (Opcional) agregue el nombre poste-ACL (que bloquea solamente).`sensor(config-net-rou-blo)#`**`post-acl-name`** *`post_acl_name`*
11. Verifique las configuraciones.`sensor(config-net-rou-blo)#`**`exit`** `sensor(config-net-rou)#`**`show settings`** `ip-address: 10.89.127.97 --- communication: ssh-3des default: ssh-3des nat-address: 19.89.149.219 default: 0.0.0.0 profile-name: PROFILE1 block-interfaces (min: 0, max: 100, current: 1) ------------------- ---------------------------- interface-name: GigabitEthernet0/1 direction: in ------------ ---------------------------------- pre-acl-name: <defaulted> post-acl-name: <defaulted> - --- -- ---- response-capabilities: block|rate-limit default: block ------------------------------ ---------------- sensor(config-net-rou)#`
12. Salga el submode del acceso a la red.`sensor(config-net-rou)#`**`exit`** `sensor(config-net)#`**`exit`** `sensor(config)#`**`exit`** `Apply Changes:?[yes]:`
13. Presione ENTER para aplicar los cambios o ingresar **no** para desecharlos.

Configure el sensor para manejar los Firewall de Cisco

Complete estos pasos para configurar el sensor para manejar los Firewall de Cisco:

1. Inicie sesión al CLI con una cuenta que tenga privilegios de administrador.
2. Ingrese el submode del acceso a la red.`sensor#`**`configure terminal`** `sensor(config)#`**`service network-access`** `sensor(config-net)#`
3. Especifique la dirección IP para el Firewall controlado por el ARCO.`sensor(config-net)#`**`firewall-devices`** *`ip_address`*
4. Ingrese el nombre del perfil del usuario que usted creó cuando usted configuró el perfil del usuario.`sensor(config-net-fir)#`**`profile-name`** *`user_profile_name`* El ARCO valida cualquier cosa que usted teclea. No marca para ver si existe el dispositivo lógico.
5. Especifique el método usado para acceder el sensor.`sensor(config-net-fir)#`**`communication {telnet | ssh-des | ssh-3des}`** Si está sin especificar, se utiliza SSH 3DES.**Nota:** Si usted utiliza el DES o el 3DES, usted debe utilizar el **comando ip_address de la clave de host del ssh** para validar la clave o el ARCO no puede conectar con el dispositivo.
6. Especifique el direccionamiento del sensor NAT.`sensor(config-net-fir)#`**`nat-address`** *`nat_address`* **Nota:** Esto cambia la dirección IP en la primera línea del ACL de la dirección IP del sensor al direccionamiento NAT. El direccionamiento NAT es el direccionamiento del sensor, poste-NAT, traducido por un dispositivo intermediario, situado entre el sensor y el dispositivo de bloqueo.
7. Salga el submode del acceso a la red.`sensor(config-net-fir)#`**`exit`** `sensor(config-net)#`**`exit`** `sensor(config)#`**`exit`** `Apply Changes:?[yes]:`
8. Presione ENTER para aplicar los cambios o ingresar **ningún** para desecharlos.

El bloque con EVITA en el PIX/ASA

La publicación del **comando shun** bloquea las conexiones de un host que ataca. Se caen y se registran los paquetes que hacen juego los valores en el comando hasta que se quite la función de bloqueo. **El evitar** es aplicado sin importar si una conexión con la dirección de host especificada está actualmente - el active.

Si usted especifica la dirección destino, los puertos de origen y de destino, y el protocolo, usted estrecha el evitar a las conexiones que hacen juego esos parámetros.

Usted puede solamente tener un **comando shun** para cada dirección IP de origen.

Porque utilizan al **comando shun** de bloquear los ataques dinámicamente, no se visualiza en la configuración del dispositivo de seguridad.

Siempre que se quite una interfaz, toda evita que se asocia a esa interfaz también se quita.

Este ejemplo muestra que el host que ofende (10.1.1.27) hace una conexión con la víctima (10.2.2.89) al TCP. La conexión en la tabla de conexiones del dispositivo de seguridad lee como sigue:

```
TCP outside:10.1.1.27/555 inside:10.2.2.89/666
```

Para bloquear las conexiones de un host que ataca, utilice el **comando shun** en el modo EXEC privilegiado. Aplique el **comando shun** con estas opciones:

```
hostname#shun 10.1.1.27 10.2.2.89 555 666 tcp
```

El comando borra la conexión de la tabla de conexiones del dispositivo de seguridad y también previene los paquetes a partir de la 10.1.1.27:555 al (TCP) de 10.2.2.89:666 de pasar a través del dispositivo de seguridad.

Información Relacionada

- Configurar el sensor para manejar los Catalyst 6500 Series Switch y a los Cisco 7600 Series Router
- Configurar el regulador de la respuesta a ataques para bloquear y valora la limitación usando IDM 7.0
- Soporte Técnico y Documentación - Cisco Systems