Ejemplo de Configuración de Shunning/Blocking en IPS para el Router ASA/PIX/IOS

Contenido

Introducción

Este documento describe cómo configurar el rechazo en un router PIX/ASA/Cisco IOS con la ayuda de Cisco IPS. ARC, la aplicación de bloqueo en el sensor, inicia y detiene los bloqueos en los routers, los switches Cisco serie 5000 RSM y Catalyst serie 6500, los firewalls PIX, FWSM y ASA. ARC emite un bloqueo o rechazo al dispositivo administrado para la dirección IP malintencionada. ARC envía el mismo bloque a todos los dispositivos que administra el sensor. Si se configura un sensor de bloqueo primario, el bloque se reenvía a este dispositivo y se emite desde él. ARC monitorea el tiempo para el bloque y elimina el bloque una vez que caduca.

Cuando utiliza IPS 5.1, se debe tener especial cuidado al rechazar los firewalls en el modo de contexto múltiple, ya que no se envía información de VLAN con la solicitud de rechazo.

> **Nota:** El bloqueo no se soporta en el contexto de administración de un FWSM de contexto múltiple.

Hay tres tipos de bloques:

- Bloque de host: bloquea todo el tráfico de una dirección IP determinada.
- Bloque de conexión: bloquea el tráfico de una dirección IP de origen dada a una dirección IP de destino y puerto de destino dados. Varios bloques de conexión de la misma dirección IP de origen a una dirección IP de destino diferente o a un puerto de destino conmutan automáticamente el bloque de un bloque de conexión a un bloque host.**Nota:** Los dispositivos de seguridad no admiten los bloques de conexión. Los dispositivos de seguridad solo admiten bloques de host con información de protocolo y puerto opcional.
- Bloqueo de red: bloquea todo el tráfico de una red determinada. Puede iniciar los bloques de

host y conexión manual o automáticamente cuando se activa una firma. Solo puede iniciar los bloques de red manualmente.

Para los bloques automáticos, debe elegir Request Block Host (Solicitar bloqueo de host) o Request Block Connection (Solicitar bloqueo de conexión) como acción de evento para firmas concretas, de modo que SensorApp envíe una solicitud de bloqueo a ARC cuando se active la firma. Una vez que ARC recibe la solicitud de bloqueo de SensorApp, actualiza las configuraciones del dispositivo para bloquear el host o la conexión. Consulte Asignación de Acciones a las Firmas, página 5-22 para obtener más información sobre el procedimiento para agregar las acciones de evento Request Block Host o Request Block Connection a la firma. Refiérase a Configuración de las Sustituciones de Acción de Evento, página 7-15 para obtener más información sobre el procedimiento para la configuración de las anulaciones que agregan las acciones de evento Request Block Host o Request Block Connection a alarmas de clasificaciones de riesgo específicas.

En los routers Cisco y los switches Catalyst serie 6500, ARC crea bloques aplicando ACL o VACL. Las ACL y las VACL aplican filtros a las interfaces, que incluyen la dirección, y las VLAN, respectivamente, para permitir o denegar el tráfico. . El firewall PIX, FWSM y ASA no utilizan ACL o VACL. Se utilizan los comandos **shun** y **no shun** integrados.

Esta información es necesaria para la configuración de ARC:

- ID de usuario de inicio de sesión, si el dispositivo está configurado con AAA
- Contraseña de inicio de sesión
- Habilitar contraseña, que no es necesaria si el usuario dispone de privilegios de habilitación
- Interfaces que se deben administrar, por ejemplo, ethernet0, vlan100
- Cualquier información de ACL o VACL existente que desee aplicar al principio (ACL de bloqueo previo o VACL) o al final (ACL o VACL posteriores al bloqueo) de la ACL o VACL que se crea. Esto no se aplica a un firewall PIX, FWSM o ASA porque no utilizan ACL o VACL para bloquear.
- Si utiliza Telnet o SSH para comunicarse con el dispositivo
- Direcciones IP (host o intervalo de hosts) que nunca desea bloquear
- Cuánto tiempo desea que los bloques duren

Prerequisites

Requirements

Antes de configurar ARC para bloqueo o limitación de velocidad, debe completar estas tareas:

- Analice su topología de red para comprender qué dispositivos deben estar bloqueados por qué sensor y qué direcciones no deben bloquearse nunca.
- Recopile los nombres de usuario, las contraseñas del dispositivo, las contraseñas de activación y los tipos de conexiones (Telnet o SSH) necesarios para iniciar sesión en cada dispositivo.
- Conozca los nombres de la interfaz en los dispositivos.
- Conozca los nombres de la ACL o VACL de bloqueo previo y la ACL o VACL posterior al bloqueo si es necesario.
- Entender qué interfaces deben y no deben bloquearse y en qué dirección (entrada o salida).

Componentes Utilizados

La información de este documento se basa en Cisco Intrusion Prevention System 5.1 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.

> **Nota:** De forma predeterminada, ARC se configura para un límite de 250 entradas de bloque. Refiérase a Dispositivos Soportados para obtener más información sobre la lista de dispositivos bloqueantes soportados por ARC.

Convenciones

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

Antecedentes

Utilice la página Bloqueo para configurar los parámetros básicos necesarios para habilitar el bloqueo y la limitación de velocidad.

ARC controla las acciones de bloqueo y limitación de velocidad en los dispositivos administrados.

Debe ajustar el sensor para identificar los hosts y las redes que nunca deben bloquearse. Es posible que el tráfico de un dispositivo de confianza active una firma. Si esta firma se configura para bloquear al atacante, el tráfico de red legítimo puede verse afectado. La dirección IP del dispositivo se puede enumerar en la lista Nunca bloquear para evitar este escenario.

Se aplica una máscara de red especificada en una entrada Never Block a la dirección Never Block. Si no se especifica ninguna máscara de red, se aplica una máscara /32 predeterminada.

> **Nota:** De forma predeterminada, no se permite al sensor emitir un bloque para su propia dirección IP, ya que esto interfiere con la comunicación entre el sensor y el dispositivo de bloqueo. Sin embargo, el usuario puede configurar esta opción.

Una vez que ARC se configura para administrar un dispositivo de bloqueo, las ACL/VACL que se utilizan para el bloqueo no se deben modificar manualmente. Esto puede causar una interrupción del servicio ARC y puede dar lugar a que no se emitan futuros bloqueos.

> **Nota:** De forma predeterminada, sólo se admite el bloqueo en los dispositivos Cisco IOS. Puede reemplazar el valor predeterminado de bloqueo si elige limitar o bloquear velocidad más limitación de velocidad.

Para ejecutar o modificar bloques, el usuario de IPS debe tener la función de administrador u

operador.

Configure el sensor para administrar los routers de Cisco

Esta sección describe cómo configurar el sensor para administrar los routers de Cisco. Contiene estos temas:

- Configurar perfiles de usuario
- Routers y ACL
- Configuración de routers de Cisco mediante CLI

Configurar perfiles de usuario

El sensor administra los otros dispositivos con el comando **user-profiles** *profile_name* para configurar perfiles de usuario. Los perfiles de usuario contienen el ID de usuario, la contraseña y la información de activación de contraseña. Por ejemplo, los routers que comparten las mismas contraseñas y nombres de usuario pueden estar bajo un perfil de usuario.

> **Nota:** Debe crear un perfil de usuario antes de configurar el dispositivo de bloqueo.

Complete estos pasos para configurar los perfiles de usuario:

1. Inicie sesión en la CLI con una cuenta que tenga privilegios de administrador.
2. Introduzca el modo de acceso a la red.
   ```
   sensor#configure terminal
   sensor(config)#service network-access
   sensor(config-net)#
   ```
3. Cree el nombre del perfil de usuario.
   ```
   sensor(config-net)#user-profiles PROFILE1
   ```
4. Escriba el nombre de usuario para ese perfil de 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 de activación para el usuario.
   ```
   sensor(config-net-use)# enable-password
   Enter enable-password[]: ********
   Re-enter enable-password ********
   ```
7. Verifique los parámetros.
   ```
   sensor(config-net-use)#show settings
      profile-name: PROFILE1
      ----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: jsmith default:
      ----------------------------------------------
   sensor(config-net-use)#
   ```
8. Salga del submodo de acceso a la red.

```
sensor(config-net-use)#exit
sensor(config-net)#exit
Apply Changes:?[yes]:
```

9. Presione **Enter** para aplicar los cambios o ingrese no para descartarlos.

Routers y ACL

Cuando ARC se configura con un dispositivo de bloqueo que utiliza ACL, las ACL se componen de esta manera:

1. Línea de permiso con la dirección IP del sensor o, si se especifica, la dirección NAT del sensor**Nota:** Si permite que se bloquee el sensor, esta línea no aparece en la ACL.
2. ACL de bloqueo previo (si se especifica): Esta ACL ya debe existir en el dispositivo.**Nota:** ARC lee las líneas en la ACL preconfigurada y copia estas líneas al inicio de la ACL de bloque.
3. Cualquier bloque activo
4. **ACL Post-Block** o **permit ip any**:**ACL posterior al bloqueo** (si se especifica):Esta ACL ya debe existir en el dispositivo.**Nota:** ARC lee las líneas en la ACL y copia estas líneas al final de la ACL.**Nota:** Asegúrese de que la última línea de la ACL sea permit ip any any si desea que se permitan todos los paquetes no coincidentes.**permit ip any any** (no se utiliza si se especifica una ACL Post-Block)

   Nota: Las ACL que hace ARC nunca deben ser modificadas por usted ni por ningún otro sistema. Estas ACL son temporales y el sensor crea constantemente nuevas ACL. Las únicas modificaciones que puede realizar son las ACL anteriores y posteriores al bloqueo.

Si necesita modificar la ACL de bloqueo previo o posterior al bloqueo, complete estos pasos:

1. Desactive el bloqueo en el sensor.
2. Realice los cambios en la configuración del dispositivo.
3. Vuelva a activar el bloqueo en el sensor.

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

Nota: Un único sensor puede gestionar varios dispositivos, pero varios sensores no pueden gestionar un único dispositivo. En el caso de que los bloques emitidos a partir de varios sensores estén diseñados para un único dispositivo de bloqueo, se debe incorporar un sensor de bloqueo primario en el diseño. Un sensor de bloqueo primario recibe solicitudes de bloqueo de varios sensores y emite todas las solicitudes de bloqueo al dispositivo de bloqueo.

Cree y guarde ACL de bloqueo previo y posterior al bloqueo en la configuración del router. Estas ACL deben ser ACL IP extendidas, nombradas o numeradas. Consulte la documentación del router para obtener más información sobre cómo crear ACL.

Nota: Las ACL de bloqueo previo y posterior al bloque no se aplican a la limitación de velocidad.

Las ACL se evalúan de arriba hacia abajo y se realiza la primera acción de coincidencia. La ACL de bloque previo puede contener un permiso que tendría prioridad sobre una negación resultante

de un bloque.

La ACL Post-Block se utiliza para contabilizar cualquier condición no manejada por la ACL Pre-Block o los bloques. Si tiene una ACL existente en la interfaz y en la dirección en la que se ejecutan los bloques, esa ACL se puede utilizar como la ACL Post-Block. Si no tiene una ACL Post-Block, el sensor inserta permit ip any al final de la nueva ACL.

Cuando se inicia el sensor, lee el contenido de las dos ACL. Crea una tercera ACL con estas entradas:

- Una línea de permiso para la dirección IP del sensor
- Copias de todas las líneas de configuración de la ACL de bloque previo
- Una línea de denegación para cada dirección bloqueada por el sensor
- Copias de todas las líneas de configuración de la ACL Post-Block

El sensor aplica la nueva ACL a la interfaz y dirección que usted designe.

> **Nota:** Cuando la nueva ACL de bloque se aplica a una interfaz del router, en una dirección determinada, reemplaza cualquier ACL preexistente en esa interfaz en esa dirección.

Configuración de routers de Cisco mediante CLI

Complete estos pasos para configurar un sensor para que administre un router Cisco para realizar bloqueos y limitación de velocidad:

1. Inicie sesión en la CLI con una cuenta que tenga privilegios de administrador.
2. Ingrese al submodo de 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 ARC.
   ```
   sensor(config-net)#router-devices ip_address
   ```
4. Introduzca el nombre de dispositivo lógico que creó al configurar el perfil de usuario.
   ```
   sensor(config-net-rou)#profile-name user_profile_name
   ```
   Nota: ARC acepta cualquier cosa que introduzca. No comprueba si el perfil de usuario existe.
5. Especifique el método utilizado para acceder al sensor.
   ```
   sensor(config-net-rou)# communication {telnet | ssh-des | ssh-3des}
   ```
   Si no se especifica, se utiliza SSH 3DES.**Nota:** Si utiliza DES o 3DES, debe utilizar el comando **ssh host-key ip_address** para aceptar la clave SSH del dispositivo.
6. Especifique la dirección NAT del sensor.
   ```
   sensor(config-net-rou)#nat-address nat_address
   ```
   Nota: Esto cambia la dirección IP en la primera línea de la ACL de la dirección del sensor a la dirección NAT. La dirección NAT es la dirección del sensor, post-NAT, traducida por un dispositivo intermediario, ubicado entre el sensor y el dispositivo de bloqueo.
7. Especifique si el router realiza el bloqueo, la limitación de velocidad o ambos.**Nota:** El valor predeterminado es bloqueo. No es necesario configurar las capacidades de respuesta si desea que el router realice solamente el bloqueo.Sólo límite de velocidad
   ```
   sensor(config-net-rou)#response-capabilities rate-limit
   ```

Bloqueo y limitación de velocidad

```
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 se utiliza después del comando **interface**.

9. (Opcional) Agregue el nombre pre-ACL (sólo bloqueo).

```
sensor(config-net-rou-blo)#pre-acl-name pre_acl_name
```

10. (Opcional) Agregue el nombre post-ACL (sólo bloqueo).

```
sensor(config-net-rou-blo)#post-acl-name post_acl_name
```

11. Verifique los parámetros.

```
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 del submodo de 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 ingrese **no** para descartarlos.

Configure el sensor para administrar los firewalls de Cisco

Complete estos pasos para configurar el sensor para administrar los firewalls de Cisco:

1. Inicie sesión en la CLI con una cuenta que tenga privilegios de administrador.
2. Ingrese al submodo de 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 ARC.

```
sensor(config-net)#firewall-devices ip_address
```

4. Introduzca el nombre de perfil de usuario que creó al configurar el perfil de usuario.

```
sensor(config-net-fir)#profile-name user_profile_name
```

Nota: ARC acepta cualquier cosa que escriba. No comprueba si existe el dispositivo lógico.

5. Especifique el método utilizado para acceder al sensor.
   ```
   sensor(config-net-fir)#communication {telnet | ssh-des | ssh-3des}
   ```
   Si no se especifica, se utiliza SSH 3DES.**Nota:** Si utiliza DES o 3DES, debe utilizar el comando **ssh host-key ip_address** para aceptar la clave o ARC no puede conectarse al dispositivo.
6. Especifique la dirección NAT del sensor.
   ```
   sensor(config-net-fir)#nat-address nat_address
   ```
   Nota: Esto cambia la dirección IP en la primera línea de la ACL de la dirección IP del sensor a la dirección NAT. La dirección NAT es la dirección del sensor, post-NAT, traducida por un dispositivo intermediario, ubicado entre el sensor y el dispositivo de bloqueo.
7. Salga del submodo de 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 ingrese **no** para descartarlos.

Bloquear con SHUN en PIX/ASA

La ejecución del comando **shun** bloquea las conexiones de un host atacante. Los paquetes que coinciden con los valores del comando se descartan y registran hasta que se elimina la función de bloqueo. El **shun** se aplica independientemente de si una conexión con la dirección host especificada está actualmente activa.

Si especifica la dirección de destino, los puertos de origen y de destino y el protocolo, el rechazo se limita a las conexiones que coinciden con esos parámetros. Sólo puede tener un **comando shun** para cada dirección IP de origen.

Debido a que el comando **shun** se utiliza para bloquear ataques dinámicamente, no se muestra en la configuración del dispositivo de seguridad.

Siempre que se elimina una interfaz, también se eliminan todos los rechazos conectados a esa interfaz.

Este ejemplo muestra que el host infractor (10.1.1.27) realiza una conexión con la víctima (10.2.2.89) al TCP. La conexión en la tabla de conexión del dispositivo de seguridad es la siguiente:

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

Para bloquear las conexiones de un host atacante, 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 elimina la conexión de la tabla de conexión del dispositivo de seguridad y también evita que los paquetes pasen a través del dispositivo de seguridad de 10.1.1.27:555 a 10.2.2.89:666 (TCP).

Información Relacionada

- Configuración del Sensor para Administrar los Catalyst 6500 Series Switches y Cisco 7600 Series Routers
- Soporte Técnico y Documentación - Cisco Systems