Cliente DHCP o servidor con configuración de router ZBF

Contenido

Introducción

Este documento describe cómo configurar un router que actúa como servidor DHCP (Dynamic Host Control Protocol) o cliente DHCP con la función de firewall basado en zonas (ZBF). Debido a que es bastante común tener DHCP y ZBF habilitados simultáneamente, estas sugerencias de configuración ayudan a garantizar que estas funciones interactúen correctamente.

Prerequisites

Requirements

Cisco recomienda que conozca el firewall basado en zonas del software Cisco IOS®. Consulte la Guía de diseño y aplicación de firewall de políticas basadas en zonas para obtener más detalles.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de

hardware.

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). If your network is live, make sure that you understand the potential impact of any command.

Información sobre la Función

Cuando se habilita ZBF en un router IOS, cualquier tráfico a la zona automática (es decir, el tráfico destinado al plano de administración del router) se permite de forma predeterminada en el tren de código de IOS 15.x.

Si ha creado una política para cualquier zona (como 'interna' o 'externa') para la zona propia (política de salida a sí misma) o la inversa (política de salida a sí misma), debe definir explícitamente el tráfico permitido en las políticas asociadas a estas zonas. Utilice la acción de inspección o paso para definir el tráfico permitido.

Análisis de datos

DHCP utiliza paquetes de protocolo de datagramas de usuario (UDP) de difusión para completar el proceso DHCP. Las configuraciones de firewall basadas en zonas que especifican la acción de inspección para estos paquetes UDP de difusión pueden ser descartadas por el router y el proceso DHCP puede fallar. Es posible que también vea este mensaje de registro:

```
%FW-6-DROP_PKT: Dropping udp session 0.0.0.0:68 255.255.255.255:67 on zone-pair
self-out class dhcp with ip ident 0
```

Consulte el problema descrito en Cisco bug ID CSCso53376, "ZBF inspect does't work for broadcast traffic" (La inspección de ZBF no funciona para el tráfico de broadcast).

Para evitar este problema, modifique la configuración de firewall basada en zonas de modo que la acción de pasar en lugar de la acción de inspeccionar se aplique al tráfico DHCP.

> **Nota**: Esto sólo es necesario cuando se aplica una política a la zona automática en el router.

Firewall basado en zona como cliente DHCP con acción de paso para tráfico UDP

Configurar

Este ejemplo de configuración utiliza el conjunto de acciones de pase en lugar de la acción de inspección en el policy-map para todo el tráfico UDP hacia o desde el router.

```
zone security outside
zone security inside

interface Ethernet0/1
zone-member security outside
interface Ethernet0/2
zone-member security inside

class-map type inspect match-all dhcp
match protocol udp

policy-map type inspect out-to-self
class type inspect dhcp
pass
class class-default
drop
policy-map type inspect self-to-out
class type inspect dhcp
pass
class class-default
drop

zone-pair security out-to-self source outside destination self
service-policy type inspect out-to-self
zone-pair security self-to-out source self destination outside
service-policy type inspect self-to-out
```

Verificación

Revise los registros del sistema para verificar que el router obtuvo una dirección DHCP de manera satisfactoria.

Cuando las políticas out-to-self y self-to-out se configuran para pasar el tráfico UDP, el router puede obtener una dirección IP de DHCP como se muestra en este syslog:

```
%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1/0 assigned DHCP address 192.168.1.5,
mask 255.255.255.0
```

Cuando solamente la política de zona de salida hacia sí misma se configura para pasar el tráfico UDP, el router también puede obtener una dirección IP de DHCP, y se crea este syslog:

```
%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1/0 assigned DHCP address 192.168.1.6,
mask 255.255.255.0
```

Cuando sólo se configura la política de zona de autodesconexión para pasar el tráfico UDP, el router puede obtener una dirección IP de DHCP y se crea este syslog:

```
%DHCP-6-ADDRESS_ASSIGN: Interface Ethernet1/0 assigned DHCP address 192.168.1.7,
mask 255.255.25
```

Firewall basado en zona con acción Pass para tráfico DHCP

Configurar

Este ejemplo de configuración muestra cómo evitar todo el tráfico UDP de una zona a la zona automática del router, excepto los paquetes DHCP. Utilice una lista de acceso con puertos específicos para permitir solamente el tráfico DHCP; en este ejemplo, se especifica que coincidan el puerto UDP 67 y el puerto UDP 68. Un mapa de clase que hace referencia a la lista de acceso tiene aplicada la acción de paso.

```
access-list extended 111
 10 permit udp any any eq 67

access-list extended 112
 10 permit udp any any eq 68

class-map type inspect match-any self-to-out
match access-group 111
class-map type inspect match-any out-to-self
match access-group 112

zone security outside
zone security inside

interface Ethernet0/1
zone-member security outside
interface Ethernet0/2
zone-member security inside

policy-map type inspect out-to-self
class type inspect out-to-self
pass
class class-default
drop
policy-map type inspect self-to-out
class type inspect self-to-out
pass
class class-default
drop

zone-pair security out-to-self source outside destination self
service-policy type inspect out-to-self
zone-pair security self-to-out source self destination outside
service-policy type inspect self-to-out
```

Verificación

Revise el resultado del comando **show policy-map type inspect zone-pair sessions** para confirmar que el router está permitiendo el tráfico DHCP a través del firewall de zona. En este ejemplo de salida, los contadores resaltados indican que los paquetes están siendo pasados a través del firewall de zona. Si estos contadores son cero, hay un problema con la configuración o los paquetes no llegan al router para su procesamiento.

```
router#show policy-map type inspect zone-pair sessions

policy exists on zp out-to-self
Zone-pair: out-to-self
Service-policy inspect : out-to-self
Class-map: out-to-self (match-any)
Match: access-group 112
3 packets, 924 bytes
30 second rate 0 bps
```

```
Pass
6 packets, 1848 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes

policy exists on zp self-to-out
Zone-pair: self-to-out
Service-policy inspect : self-to-out
Class-map: self-to-out (match-any)
Match: access-group 111
6 packets, 3504 bytes
30 second rate 0 bps
Pass
6 packets, 3504 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
```

Situación para configuraciones incorrectas

Este escenario de ejemplo muestra lo que sucede cuando el router está configurado incorrectamente para especificar la acción de inspección para el tráfico DHCP. En este escenario, el router se configura como un cliente DHCP. El router envía un mensaje de detección DHCP para intentar obtener una dirección IP. El firewall basado en zonas está configurado para inspeccionar este tráfico DHCP. Este es un ejemplo de la configuración de ZBF:

```
zone security outside
zone security inside

interface Ethernet0/1
zone-member security outside

interface Ethernet0/2
zone-member security inside

class-map type inspect match-all dhcp
match protocol udp

policy-map type inspect out-to-self
class type inspect dhcp
inspect
class class-default
drop
policy-map type inspect self-to-out
class type inspect dhcp
inspect
class class-default
drop

zone-pair securiy out-to-self source outside destination self
service-policy type inspect out-to-self
zone-pair security self-to-out source self destination outside
service-policy type inspect self-to-out
```

Cuando la política de auto-to-out se configura con la acción de inspección para el tráfico UDP, el

paquete de detección DHCP se descarta y se crea este syslog:

```
%FW-6-DROP_PKT: Dropping udp session 0.0.0.0:68 255.255.255.255:67 on zone-pair
self-out class dhcp with ip ident 0
```

Cuando tanto la política auto-to-out como la política out-to-self se configuran con la acción de inspección para el tráfico UDP, el paquete de detección DHCP se descarta y se crea este syslog:

```
%FW-6-DROP_PKT: Dropping udp session 0.0.0.0:68 255.255.255.255:67 on zone-pair
self-out class dhcp with ip ident 0
```

Cuando la política de auto-envío tiene habilitada la acción de inspección y la política de auto-envío tiene habilitada la acción de pase para el tráfico UDP, el paquete de oferta DHCP se descarta después de que se envíe el paquete de detección DHCP y se crea este syslog:

```
%FW-6-DROP_PKT: Dropping udp session 192.168.1.1:67 255.255.255.255:68 on zone-pair
out-self class dhcp with ip ident 0
```

Router como servidor DHCP

Si la interfaz interna de los routers actúa como un servidor DHCP y si los clientes que se conectan a la interfaz interna son los clientes DHCP, este tráfico DHCP se permite de forma predeterminada si no existe una política de zona de autocomunicación o autocomunicación interna.

Sin embargo, si alguna de estas políticas existe, debe configurar una acción de transferencia para el tráfico de interés (puerto UDP 67 o puerto UDP 68) en la política de servicio de par de zonas.

Troubleshoot

Actualmente no hay información específica de solución de problemas disponible para estas configuraciones.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).