Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Información sobre la Función](#)
[Análisis de datos](#)
[Firewall Zona-basado como Cliente de DHCP con la acción del paso para el tráfico UDP](#)
[Configurar](#)
[Verificación](#)
[Firewall Zona-basado con la acción del paso para el tráfico del DHCP](#)
[Configurar](#)
[Verificación](#)
[Escenario para las configuraciones incorrectas](#)
[Router como servidor DHCP](#)
[Troubleshooting](#)

Introducción

Este documento describe cómo configurar a un router que esté actuando como un servidor o Cliente de DHCP del (DHCP) del Dynamic Host Control Protocol con la característica zona-basada del Firewall (ZBF). Porque es bastante común hacer el DHCP y ZBF habilitar simultáneamente, estas extremidades de la configuración ayudan a asegurar estas características interactivas correctamente.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento del Firewall zona-basado software del ® del Cisco IOS. Refiera a la guía Zona-basada del diseño y de la aplicación del Firewall de la directiva para los 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). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Información sobre la Función

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

Si usted ha creado una directiva para cualquier zona (tal como “interior” o “afuera ") a la zona del uno mismo (directiva del hacia fuera-a-uno mismo) o al revés (uno mismo--hacia fuera a la directiva), usted debe definir explícitamente el tráfico permitido en las directivas asociado a estas zonas. Utilice la inspección o pase la acción para definir el tráfico permitido.

Análisis de datos

El DHCP utiliza los paquetes del User Datagram Protocol (UDP) del broadcast para completar el proceso DHCP. las configuraciones de escudo de protección Zona-basadas que especifican la acción de la inspección para estos paquetes UDP del broadcast se pudieron caer por el router, y el proceso DHCP pudieron fallar. Usted puede ser que también vea este mensaje del registro:

Refiera al problema descrito en el Id. de bug Cisco CSCso53376, “ZBF examinan no trabaja para el tráfico de broadcast.”

Para evitar este problema, modifique la configuración de escudo de protección zona-basada para aplicar la acción del paso en vez de la acción de la inspección al tráfico del DHCP.

> Nota: Se requiere esto solamente cuando una directiva se aplica a la zona del uno mismo en el router.

Firewall Zona-basado como Cliente de DHCP con la acción del paso para el tráfico UDP

Configurar

Este ejemplo de configuración utiliza el conjunto de la acción del paso en vez de la acción de la inspección en el directiva-mapa para todo el tráfico UDP a o desde el router.

Verificación

Revise los Syslog para verificar que el router obtuvo con éxito un DHCP Address.

Cuando configuran al hacia fuera-a-uno mismo y uno mismo--hacia fuera a las directivas para

pasar el tráfico UDP, el router puede obtener una dirección IP del DHCP tal y como se muestra en de este Syslog:

Cuando solamente la directiva de la zona del hacia fuera-a-uno mismo se configura para pasar el tráfico UDP, el router puede también obtener una dirección IP del DHCP, y se crea este Syslog:

Cuando uno mismo--hacia fuera a la directiva de la zona se configura solamente para pasar el tráfico UDP, el router puede obtener una dirección IP del DHCP, y se crea este Syslog:

Firewall Zona-basado con la acción del paso para el tráfico del DHCP

Configurar

Este ejemplo de configuración muestra cómo prevenir todo el tráfico UDP de una zona en la zona del uno mismo de su router a excepción de los paquetes DHCP. Utilice una lista de acceso con los puertos específicos para permitir apenas el tráfico del DHCP; en este ejemplo, el puerto 67 UDP y el puerto 68 UDP se especifican para ser correspondidos con. Un clase-mapa que se refiere a la lista de acceso tiene la acción del paso aplicada.

```
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

La salida del estudio del **tipo del directiva-mapa de la demostración examina el comando sessions de los zona-pares** para confirmar que el router está permitiendo el tráfico del DHCP con el Firewall de la zona. En esta salida de ejemplo, los contadores resaltados indican que los paquetes se están pasando con el Firewall de la zona. Si estos contadores son cero, hay un problema con la configuración, o los paquetes no están llegando al router para procesar.

```
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
```

Escenario para las configuraciones incorrectas

Este escenario de ejemplo muestra qué sucede cuando configuran al router incorrectamente para especificar la acción de la inspección para el tráfico del DHCP. En este escenario, configuran al router como Cliente de DHCP. El router envía un mensaje DISCOVER DHCP para intentar y para obtener una dirección IP. El Firewall zona-basado se configura para examinar este tráfico del DHCP. Éste es un ejemplo de la configuración ZBF:

```
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
```

Cuando uno mismo--hacia fuera a la directiva se configura con la acción de la inspección para el tráfico UDP, se cae el paquete de detección del DHCP, y se crea este Syslog:

```
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
```

Cuando la directiva ambos uno mismo-a-hacia fuera y del hacia fuera-a-uno mismo se configura con la acción de la inspección para el tráfico UDP, se cae el paquete de detección del DHCP, y se crea este Syslog:

```
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
```

Cuando la directiva del hacia fuera-a-uno mismo tiene la acción de la inspección habilitada, y uno mismo--hacia fuera a la directiva tiene la acción del paso habilitada para el tráfico UDP, se cae el paquete de la oferta de DHCP después de que se envíe el paquete de detección del DHCP, y se crea este Syslog:

```
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
```

Router como servidor DHCP

Si la interfaz interior del Routers está actuando como servidor DHCP y si los clientes que conectan con la interfaz interior son los clientes DHCP, este tráfico del DHCP se permite por abandono si no hay dentro-a-uno mismo o uno mismo-a-dentro de la directiva de la zona.

Sin embargo, si existe cualquiera de esas directivas, usted necesita configurar una acción del paso para el tráfico del interés (puerto 67 UDP o el puerto 68 UDP) en la política de servicio de los pares de la zona.

Troubleshooting

No hay actualmente información de Troubleshooting específica disponible para estas configuraciones.