Cliente ou servidor DHCP com configuração do roteador ZBF

Contents

Introduction

Este documento descreve como configurar um roteador que esteja atuando como um servidor DHCP (Dynamic Host Control Protocol) ou cliente DHCP com o recurso de firewall baseado em zona (ZBF). Como é bastante comum ter DHCP e ZBF ativados simultaneamente, essas dicas de configuração ajudam a garantir que esses recursos interajam corretamente.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do firewall baseado em zona do software Cisco IOS®. Consulte o Guia de projeto e aplicação de firewall de política baseada em zona para obter detalhes.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Informações de recurso

Quando o ZBF é habilitado em um roteador IOS, qualquer tráfego para a autozona (ou seja, o tráfego destinado ao plano de gerenciamento do roteador) é permitido por padrão no trem de código IOS 15.x.

Se você tiver criado uma política para qualquer zona (como 'inside' ou 'outside') para a zona própria (política de saída para si mesmo) ou inversa (política de autoexclusão), deverá definir explicitamente o tráfego permitido nas políticas anexadas a essas zonas. Use a ação inspect ou pass para definir o tráfego permitido.

Análise de dados

O DHCP usa pacotes UDP (User Datagram Protocol) de broadcast para concluir o processo DHCP. As configurações de firewall baseadas em zona que especificam a ação de inspeção para esses pacotes UDP de broadcast podem ser descartadas pelo roteador e o processo DHCP pode falhar. Você também pode ver esta mensagem de log:

```
%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 o problema descrito no bug da Cisco ID CSCso53376, "ZBF inspect não funciona para tráfego de broadcast."

Para evitar esse problema, modifique a configuração do firewall baseado em zona para que a ação de aprovação em vez da ação de inspeção seja aplicada ao tráfego DHCP.

> **Observação**: isso é necessário apenas quando uma política é aplicada à autozona no roteador.

Firewall baseado em zona como cliente DHCP com ação de aprovação para tráfego UDP

Configurar

Esta configuração de exemplo utiliza o conjunto de ações de passagem em vez da ação de inspeção no mapa de políticas para todo o tráfego UDP de ou para o roteador.

```
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
```

Verificar

Revise os syslogs para verificar se o roteador obteve com êxito um endereço DHCP.

Quando as políticas out-to-self e self-to-out são configuradas para passar o tráfego UDP, o roteador pode obter um endereço IP do DHCP como mostrado neste syslog:

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

Quando somente a política de zona de saída para autoatendimento é configurada para passar o tráfego UDP, o roteador também pode obter um endereço IP do DHCP e este syslog é criado:

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

Quando apenas a política de zona autoextraível é configurada para passar o tráfego UDP, o roteador pode obter um endereço IP do DHCP e este syslog é criado:

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

Firewall baseado em zona com ação de passagem para tráfego DHCP

Configurar

Esta configuração de exemplo mostra como impedir todo o tráfego UDP de uma zona para a zona própria do roteador, exceto para pacotes DHCP. Use uma lista de acesso com portas específicas para permitir apenas o tráfego DHCP; neste exemplo, a porta UDP 67 e a porta UDP 68 são especificadas para serem combinadas. Um mapa de classe que faz referência à lista de acesso tem a ação de aprovação 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
```

Verificar

Revise a saída do comando **show policy-map type inspect zone-pair sessions** para confirmar se o roteador está permitindo o tráfego DHCP através do firewall de zona. Nesta saída de exemplo, os contadores destacados indicam que os pacotes estão sendo passados pelo firewall da região. Se esses contadores forem zero, há um problema com a configuração ou os pacotes não estão chegando ao roteador para processamento.

```
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
```

Cenário para configurações incorretas

Este exemplo de cenário mostra o que acontece quando o roteador está configurado incorretamente para especificar a ação de inspeção para o tráfego DHCP. Neste cenário, o roteador é configurado como um cliente DHCP. O roteador envia uma mensagem de descoberta DHCP para tentar obter um endereço IP. O firewall baseado em zona é configurado para inspecionar esse tráfego DHCP. Este é um exemplo da configuração 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
```

Quando a política self-to-out é configurada com a ação de inspeção para tráfego UDP, o pacote

de descoberta DHCP é descartado e este syslog é criado:

```
%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
```

Quando as políticas self-to-out e out-to-self são configuradas com a ação de inspeção para tráfego UDP, o pacote de descoberta DHCP é descartado e este syslog é criado:

```
%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
```

Quando a política out-to-self tem a ação de inspeção habilitada e a política self-to-out tem a ação de aprovação habilitada para tráfego UDP, o pacote de oferta DHCP é descartado após o pacote de descoberta DHCP ser enviado e este syslog é criado:

```
%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
```

Roteador como servidor DHCP

Se a interface interna dos roteadores estiver atuando como um servidor DHCP e se os clientes que se conectam à interface interna forem os clientes DHCP, esse tráfego DHCP será permitido por padrão se não houver política de zona interna para própria ou interna para própria.

No entanto, se uma dessas políticas existir, você precisará configurar uma ação de passagem para o tráfego de interesse (porta UDP 67 ou porta UDP 68) na política de serviço de par de zonas.

Troubleshoot

No momento, não há informações específicas de Troubleshooting disponíveis para essas configurações.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.