配置ZBF路由器的DHCP客户端或服务器

目录

简介

本文档介绍如何使用基于区域的防火墙(ZBF)功能配置充当动态主机控制协议(DHCP)服务器或DHCP客户端的路由器。由于同时启用DHCP和ZBF的情况非常常见，这些配置提示有助于确保这些功能正确交互。

先决条件

要求

Cisco建议您了解Cisco IOS®软件基于区域的防火墙。有关详细信息，请参阅基于区域的策略防火墙设计和应用指南。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

功能信息

在IOS路由器上启用ZBF时，默认情况下在IOS 15.x代码系列中允许任何发往自身区域的流量（即发往路由器管理平面的流量）。

如果已为任何区域（如“inside”或“outside”）创建到自身区域（out-to-self策略）或反向（self-to-out策略）的策略，则必须在连接到这些区域的策略中明确定义允许的流量。使用inspect或pass操作定义允许的流量。

数据分析

DHCP使用广播用户数据报协议(UDP)数据包来完成DHCP过程。路由器可能会丢弃指定这些广播UDP数据包的检查操作的基于区域的防火墙配置，并且DHCP进程可能会失败。您还可能看到以下日志消息：

```
%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
```

请参阅Cisco Bug ID CSCso53376“ZBF inspect does not work for broadcast traffic”中描述的问题。

为了避免此问题，请修改基于区域的防火墙配置，以便对DHCP流量应用传递操作而非检查操作。

注：仅当策略应用于路由器上的自身区域时，才需要此项。

基于区域的防火墙作为DHCP客户端，对UDP流量执行传递操作

配置

对于进出路由器的所有UDP流量，此示例配置使用传递操作集，而不是策略映射中的检查操作。

```
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
```

验证

检查系统日志，验证路由器是否成功获取了DHCP地址。

当同时配置出向自己和出向自策略以传递UDP流量时，路由器可以从DHCP获取IP地址，如以下系统日志所示：

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

当仅将自外区域策略配置为传递UDP流量时，路由器也可以从DHCP获取IP地址，并创建以下系统日志：

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

当仅将自转出区域策略配置为传递UDP流量时，路由器可以从DHCP获取IP地址，并创建以下系统日志：

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

对DHCP流量执行传递操作的基于区域的防火墙

配置

此示例配置显示如何阻止来自某个区域的所有UDP流量进入除DHCP数据包外的路由器自身区域。使用具有特定端口的访问列表以仅允许DHCP流量；在本示例中，指定UDP端口67和UDP端口68匹配。引用访问列表的类映射应用了pass操作。

```
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
```

验证

查看show policy-map type inspect zone-pair sessions命令的输出，以确认路由器允许DHCP流量通过区域防火墙。在此示例输出中，突出显示的计数器表示数据包正在通过区域防火墙。如果这些计数器为零，则说明配置有问题，或者数据包没有到达路由器进行处理。

```
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
```

配置不正确的场景

此示例场景显示当路由器配置错误以指定DHCP流量的检查操作时会发生什么情况。在此场景中，路由器配置为DHCP客户端。路由器发出DHCP发现消息以尝试获取IP地址。基于区域的防火墙配置为检查此DHCP流量。以下是ZBF配置的示例：

```
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
```

使用UDP流量的检查操作配置自输出策略时，DHCP发现数据包将被丢弃，并创建以下系统日志：

```
%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
```

当为UDP流量配置了inspect（检查）操作时，会丢弃DHCP发现数据包，并创建以下系统日志：

```
%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
```

当out-to-self策略启用了inspect（检查）操作，而self-to-out策略启用了UDP流量的传递操作时，在发送DHCP发现数据包之后，会丢弃DHCP提供数据包，并创建以下系统日志：

```
%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
```

路由器作为DHCP服务器

如果路由器的内部接口用作DHCP服务器，并且连接到内部接口的客户端是DHCP客户端，则如果没有内部到自身或自到内部区域策略，则默认情况下允许此DHCP流量。

但是，如果存在这些策略之一，则需要为区域对服务策略中的相关流量（UDP端口67或UDP端口68）配置传递操作。

故障排除

目前没有可用于这些配置的特定故障排除信息。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。