目录

简介

本文描述如何配置作为一个动态主机控制协议的路由器(DHCP)服务器或DHCP客户端与基于区域的防火墙(ZBF)功能。由于它是相当普遍的安排DHCP和ZBF同时启用，这些配置提示帮助保证这些功能正确地呼应。

先决条件

要求

思科建议您有Cisco IOS软件基于区域的防火墙的知识。参考基于区域的策略防火墙设计和应用程序指南关于详细信息。

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。

以信息为特色

当ZBF在IOS路由器时启用，对自身区域(即流量的所有流量被注定对路由器的管理层面)默认情况下在代码IOS 15.x系列允许。

如果创建任何区域的一项策略(例如'里面'或'外部')对自身区域(外对赛弗策略)或反向(赛弗对策略)，您必须明确地定义在策略的可允许流量附加对这些区域。请使用Inspect或用通过操作为了定义可允许流量。

数据分析

DHCP使用广播用户数据报协议(UDP)数据包为了完成DHCP过程。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也许由路由器和DHCP过程丢弃也许发生故障。您也许也发现此日志消息：

参考在Cisco Bug ID描述的问题CSCso53376， "ZBF Inspect不为广播数据流工作"。

为了避免此问题，请修改基于区域的防火墙配置，以便而不是检查操作的用通过操作应用对DHCP流量。

> **注意**：只有当策略应用对在路由器时的自身区域这要求。

基于区域的防火墙作为与用通过操作的DHCP客户端UDP流量的

配置

此配置示例为所有UDP流量使用用通过操作设置而不是在策略映射的检查操作到/从路由器。

验证

查看Syslog为了验证路由器顺利地获取DHCP地址。

当外对赛弗和赛弗对策略配置通过UDP流量时，如此Syslog所显示，路由器能从DHCP获取IP地址：

当仅外对赛弗区域策略配置通过UDP流量时，路由器能从DHCP也获取IP地址，并且此Syslog创建：

当赛弗对区域策略只配置通过UDP流量时，路由器能从DHCP获取IP地址，并且此Syslog创建：

与用通过操作的基于区域的防火墙DHCP流量的

配置

此配置示例显示如何防止所有UDP流量区域到您的路由器的自身区域除了DHCP信息包。请使用access-list以特定端口为了允许DHCP流量;在本例中， UDP端口67和UDP端口68指定匹配。参考access-list的类映射有应用的用通过操作。

```
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

查看从sessions命令的show policy-map type inspect zone-pair的输出为了确认路由器通过区域防火墙允许DHCP流量。在此示例输出中，选中项目计数器表明数据包通过区域防火墙通过。如果这些计数器是零，有与配置的一问题，或者数据包不到达到处理的路由器。

```
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
```

不正确的配置的方案

此示例情景显示发生了什么，当路由器不正确地配置指定DHCP流量的时检查操作。在此方案中，路由器配置作为DHCP客户端。路由器派出DHCP DISCOVER信息尝试和获取IP地址。基于区域的防火墙配置检查此DHCP流量。这是ZBF配置的示例：

```
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
```

当赛弗对策略配置与UDP流量的时检查操作， DHCP发现信息包丢弃，并且此Syslog创建：

```
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
```

当两个赛弗对和外对赛弗策略配置与UDP流量的时检查操作， DHCP发现信息包丢弃，并且此Syslog创建：

```
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
```

当外对赛弗策略有启用时的检查操作，并且赛弗对策略有为UDP流量启用的用通过操作， DHCP提供数据包丢弃，在DHCP发现信息包发送后，并且此Syslog创建：

```
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
```

路由器作为DHCP服务器

如果路由器的内部接口作为DHCP服务器，并且，如果连接对内部接口的客户端是DHCP客户端，此DHCP流量允许默认情况下，如果没有在里面对赛弗或赛弗对在区域策略里面。

然而，如果那些策略之一存在，您需要配置流量的一用通过操作利益(UDP端口67或UDP端口68)在区域对服务策略。

故障排除

当前没有这些配置的特定故障排除信息联机。