採用ZBF路由器配置的DHCP客戶端或伺服器

目錄

簡介

本文說明如何使用區域型防火牆(ZBF)功能將充當動態主機控制協定(DHCP)伺服器或DHCP客戶端的路由器進行配置。由於同時啟用DHCP和ZBF的現象相當普遍，因此這些配置提示有助於確保這些功能正確互動。

必要條件

需求

思科建議您瞭解Cisco IOS®軟體區域型防火牆。有關詳細資訊，請參閱基於區域的策略防火牆設計和應用指南。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

功能資訊

在IOS路由器上啟用ZBF後，IOS 15.x系列代碼中預設允許任何發往自身區域的流量（即發往路由器管理平面的流量）。

如果已經為任何區域（如「inside」或「outside」）建立了到自身區域（外向內策略）或反向（自向外策略）的策略，則必須在連線到這些區域的策略中明確定義允許的流量。使用inspect或pass操作定義允許的流量。

資料分析

DHCP使用廣播使用者資料包協定(UDP)資料包來完成DHCP過程。為廣播UDP資料包指定檢查操作的基於區域的防火牆配置可能會被路由器丟棄，並且DHCP進程可能會失敗。您還可能看到以下日誌消息：

```
%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
```

請參閱Cisco錯誤ID CSCso53376「ZBF inspect dots not work for broadcast traffic」中描述的問題。

為了避免此問題，請修改基於區域的防火牆配置，以便對DHCP流量應用通過操作而不是檢查操作。

註：僅當策略應用於路由器上的自帶區域時，才需要此功能。

作為DHCP客戶端且對UDP流量執行傳遞操作的基於區域的防火牆

設定

對於進出路由器的所有UDP流量，此示例配置使用傳遞操作集，而不是策略對映中的inspect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
```

驗證

檢查系統日誌，驗證路由器是否成功獲取了DHCP地址。

當外向和自向出策略都配置為傳遞UDP流量時，路由器可以從DHCP獲取IP地址，如以下系統日誌所示：

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

當僅將自外區域策略配置為傳遞UDP流量時，路由器還可以從DHCP獲取IP地址，並建立以下系統日誌：

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

當僅將自輸出區域策略配置為傳遞UDP流量時，路由器可以從DHCP獲取IP地址，並建立以下系統日誌：

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

針對DHCP流量執行傳遞操作的分割槽型防火牆

設定

此示例配置顯示如何阻止除DHCP資料包以外的所有UDP流量從區域進入路由器的自有區域。使用具有特定埠的訪問清單以僅允許DHCP流量；在本示例中，指定UDP埠67和UDP埠68匹配。引用訪問清單的類對映應用了傳遞操作。

```
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
```

驗證

檢視**show policy-map type inspect zone-pair sessions**命令的輸出，以確認路由器允許DHCP流量通過區域防火牆。在此示例輸出中，突出顯示的計數器表示資料包正在通過區域防火牆。如果這些計數器為零，則說明配置有問題，或者資料包沒有到達路由器進行處理。

```
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
```

配置不正確的場景

此示例場景顯示當路由器配置錯誤以指定DHCP流量的檢查操作時會發生的情況。在此案例中，路由器被配置為DHCP客戶端。路由器發出DHCP發現消息以嘗試獲取IP地址。基於區域的防火牆配置為檢查此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
```

當使用用於UDP流量的inspect（檢查）操作配置自出策略時，DHCP發現資料包將被丟棄，並且建立以下系統日誌：

```
%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
```

當為UDP流量配置了inspect（檢查）操作的自傳和自傳策略時，將丟棄DHCP發現資料包，並建立以下系統日誌：

```
%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
```

當自外策略啟用了檢查操作，而自外策略為UDP流量啟用了傳遞操作時，在傳送DHCP發現資料包後會丟棄DHCP提供資料包，並建立以下系統日誌：

```
%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
```

作為DHCP伺服器的路由器

如果路由器的內部介面充當DHCP伺服器，並且連線到內部介面的客戶端是DHCP客戶端，則如果沒有內部到自身或自內部區域策略，則預設允許此DHCP流量。

但是，如果存在其中任一策略，則需要為區域對服務策略中的關注流量（UDP埠67或UDP埠68）配置傳遞操作。

疑難排解

目前尚無適用於這些組態的具體疑難排解資訊。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。