如何在思科多層交換機或路由器上配置基於策略的路由(PBR)以將流量轉發到WSA?

目錄

問題：

如何在思科多層交換機或路由器上配置基於策略的路由(PBR)以將流量轉發到WSA?

環境: 思科網路安全裝置(WSA)，透明模式 — L4交換機

當使用L4交換機在透明模式下配置WSA時，無需在WSA上進行配置。重新導向由L4交換器（或路由器）控制。

可以使用原則型路由(PBR)將網路流量重新導向到WSA。這是通過匹配正確的流量（基於tcp埠）並指示路由器/交換機將此流量重定向到WSA來實現的。

在以下示例中，WSA的資料/代理介面（M1或P1，具體取決於配置）位於多層交換機/路由器(Vlan 3)的專用VLAN介面上，Internet路由器也位於專用VLAN介面(Vlan4)上。 客戶端位於Vlan1和Vlan2上。

初始配置（僅顯示相關部分）
interface Vlan1 desc使用者VLAN 1 ip address 10.1.1.1 255.255.255.0 ! interface Vlan2 desc使用者VLAN 2 ip address 10.1.2.1 255.255.255.0 ! interface Vlan3 desc Cisco WSA專用VLAN ip address 192.168.1.1 255.255.255.252 ! interface Vlan4 desc Internet路由器專用VLAN ip address 192.168.2.1 255.255.255.252 ! ip route 0.0.0.0 0.0.0.0 192.168.2.2

鑑於上述示例，並且Cisco WSA的IP地址為192.168.1.2，您需要新增以下命令來設定基於策略的路由(PBR):

第1步：定義Web流量

```
!匹配HTTP流量
access-list 100 permit tcp 10.1.1.0 0.0.0.255 any eq 80
access-list 100 permit tcp 10.1.2.0 0.0.0.255 any eq 80
!匹配HTTPS流量
access-list 100 permit tcp 10.1.1.0 0.0.0.255 any eq 443
access-list 100 permit tcp 10.1.2.0 0.0.0.255 any eq 443
```

第2步：定義路由對映以控制資料包的輸出位置。

```
route-map ForwardWeb permit 10
match ip address 100
set ip next-hop 192.168.1.2
```

步驟3:將路由對映應用到正確的介面。

```
！請注意，這一點應該應用到源介面（客戶端）
interface Vlan1
ip policy route-map ForwardWeb
!
interface Vlan2
ip policy route-map ForwardWeb
```

附註：這種流量重新導向(PBR)方法有一些限制。此方法的主要問題是即使裝置無法訪問（例如，由於網路問題），流量也始終重定向到WSA。 因此，沒有故障切換選項。

要解決此缺陷，您可以配置以下任一選項：

1. **PBR與跟蹤選項**配合使用。此功能用於在重定向流量之前驗證下一躍點的可用性。

   有關以下文章的更多詳細資訊：
   使用多個跟蹤選項功能配置策略的路由示例
2. Cisco Catalyst交換機沒有跟蹤選項。但是，有一個高級解決方法可用於實現相同行為。

   詳細資訊可在以下Cisco Wiki中找到：
   針對Catalyst 3xxx交換機的基於策略的路由(PBR) — 使用EEM的解決方法