如何配置在思科多层交换机或路由器的基于策略的路由(PBR)转发流量到WSA ？

目录

问题：

问题：

如何配置在思科多层交换机或路由器的基于策略的路由(PBR)转发流量到WSA ？

环境： 思科Web安全工具(WSA)，透明模式- L4交换机

使用L4交换机时，当WSA在透明模式配置，配置在WSA没有必要。重定向是由L4交换机(或路由器)控制的。

使用基于策略的路由(PBR)重定向Web流量到WSA是可能的。这通过匹配正确流量(根据TCP端口)和提示路由器/交换机重定向此流量达到到WSA。

在以下示例中， WSA的数据/代理接口(M1或P1根据配置)在多层交换机/路由器的专用VLAN接口(VLAN 3)和互联网路由器在专用VLAN接口(Vlan4)。客户端是在Vlan1和Vlan2。

初始配置(仅相关部分显示)
接口Vlan1 desc用户VLAN 1 ip address 10.1.1.1 255.255.255.0 ! 接口Vlan2 desc用户VLAN 2 IP地址10.1.2.1 255.255.255.0 ! 接口VLAN3 desc思科WSA专用VLAN IP地址192.168.1.1 255.255.255.252 ! 接口Vlan4 desc互联网路由器专用VLAN IP地址192.168.2.1 255.255.255.252 ! ip route 0.0.0.0 0.0.0.0 192.168.2.2

给上述有示例和的思科WSA 192.168.1.2的IP地址，您会添加以下命令设置基于策略的路由(PBR)

:

步骤 1：定义Web流量
!匹配HTTP数据流 access-list 100 permit tcp 10.1.1.0 0.0.0.255任何eq 80 access-list 100 permit tcp 10.1.2.0 0.0.0.255任何eq 80 *!匹配HTTPS流量* access-list 100 permit tcp 10.1.1.0 0.0.0.255任何eq 443 access-list 100 permit tcp 10.1.2.0 0.0.0.255任何eq 443
步骤 2：定义路由映射控制输出的地方数据包。
route-map ForwardWeb permit 10 匹配IP地址100 set ip next-hop 192.168.1.2
步骤 3：应用路由映射对正确接口。
! 注意应该应用这到源接口(客户端) 建立接口Vlan1 ip策略route-map ForwardWeb ! 接口Vlan2 ip策略route-map ForwardWeb

Note:此方法流量重定向(PBR)有一些限制。与此方法的主要问题是流量永远将重定向对WSA，即使设备不可及的例如(由于网络问题)。因此，没有故障切换选项。

对应急方案此缺乏，您可以配置之一的下列：

1. **与跟踪选项的PBR，**当使用Cisco路由器时。此功能用于在重定向流量前验证下一跳的可用性。

   在以下条款的更多详细信息：
   具有多个跟踪选项功能策略路由的配置示例
2. 跟踪选项为思科Catalyst交换机请勿是可用的。然而，有达到同一种行为的一先进的应急方案联机。

   详细信息可以在以下思科维基找到：
   与跟踪的基于策略的路由(PBR) Catalyst 3xxx交换机的-一应急方案使用EEM