

问题描述

【MVS】Cisco Control Plane Policing (CoPP) 的配置及其举例

解决方法

Control Plane Policing (CoPP) 是一种在 Cisco 设备上应用于控制平面流量的安全机制。以下是一个简单的 CoPP 配置示例，用于限制到达控制平面的 ICMP (ping) 请求和 SNMP 流量，同时允许路由协议流量通过。

```
`` cisco
! 第一步：定义访问控制列表 (ACLs) 来分类流量
access-list 100 permit icmp any any echo-reply
access-list 100 permit icmp any any time-exceeded
access-list 100 permit icmp any any unreachable
access-list 101 permit udp any any eq snmp
access-list 102 permit tcp any any eq bgp
access-list 102 permit tcp any any eq ospf

! 第二步：创建一个类映射来匹配 ACL
class-map match-any ICMP-TRAFFIC
match access-group 100
class-map match-any SNMP-TRAFFIC
match access-group 101
class-map match-any ROUTING-TRAFFIC
match access-group 102

! 第三步：创建策略映射来定义流量策略
policy-map COPP-POLICY
class ICMP-TRAFFIC
police 8000 1500 conform-action transmit exceed-action drop
class SNMP-TRAFFIC
police 5000 1000 conform-action transmit exceed-action drop
class ROUTING-TRAFFIC
class-default
police 100000 25000 conform-action transmit exceed-action transmit

! 第四步：将策略映射应用到控制平面
control-plane
service-policy input COPP-POLICY
``
```

在这个示例中：

- **ACLs** 定义了允许通过的 ICMP 类型和 SNMP 流量，以及允许的路由协议流量（如 BGP 和 OSPF）。
- **类映射** 通过匹配 ACL 来标识不同类型的流量。
- **策略映射** 包含具体的限速指令，控制各类流量的速率。在这个例子中，ICMP 流量限制为每秒 8000 字节，并且超出部分将被丢弃。SNMP 流量限制为每秒 5000 字节，并且超出部分也将被丢弃。路由协议流量则被允许，但也有一个较高的限速设置。
- 最后，将策略映射应用到控制平面，这样所有进入控制平面的流量都将受到 CoPP 策略的限制。

请注意，这只是一个示例配置，实际的 CoPP 配置将根据您的网络需求、流量模式和安全政策而有所不同。在将 CoPP 配置应用到生产网络之前，建议在测试环境中验证其影响，并确保了解每个命令的含义。