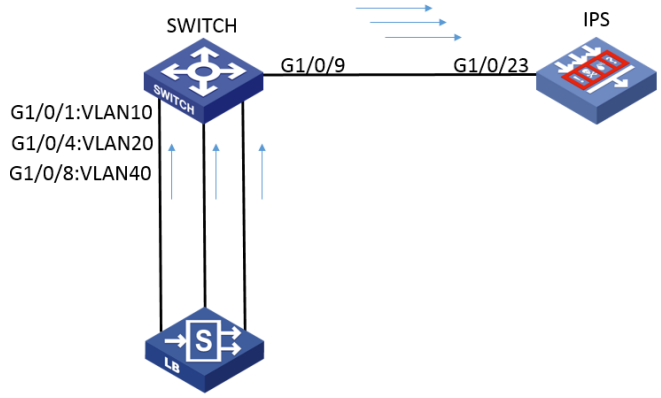
V7 IPS旁路部署inline黑洞转发配置案例（多VLAN）

郑标 2018-01-21 发表

如下图所示，不同业务VLAN的流量通过交换机进来，交换机将流量通过镜像上送IPS设备处理，IPS设备配置inline黑洞转发，对收到的报文处理完后直接丢弃。



1. Switch配置

```
[H3C]vlan 2
[H3C]vlan 10
[H3C]vlan 20
[H3C]vlan 40                    //创建vlan
[H3C]mirroring-group 1 local            //配置本地镜像组
[H3C]int GigabitEthernet 1/0/1
[H3C-GigabitEthernet1/0/1] port link-mode bridge     //配置接口模式为brige
[H3C-GigabitEthernet1/0/1] port access vlan 10       //允许vlan 10通过
[H3C-GigabitEthernet1/0/1] mirroring-group 1 mirroring-port both   //配置对接口g1/0/1收发的报文都进行镜像
[H3C-GigabitEthernet1/0/1]qu
[H3C]int GigabitEthernet 1/0/4
[H3C-GigabitEthernet1/0/4] port link-mode bridge     //配置接口模式为brige
[H3C-GigabitEthernet1/0/4] port access vlan 20       //允许vlan 10通过
[H3C-GigabitEthernet1/0/4] mirroring-group 1 mirroring-port both   //配置对接口g1/0/4收发的报文都进行镜像
[H3C-GigabitEthernet1/0/4]qu
[H3C]int GigabitEthernet 1/0/8
[H3C-GigabitEthernet1/0/8] port link-mode bridge     //配置接口模式为brige
[H3C-GigabitEthernet1/0/8] port access vlan 40       //允许vlan 10通过
[H3C-GigabitEthernet1/0/8] mirroring-group 1 mirroring-port both   //配置对接口g1/0/8收发的报文都进行镜像
[H3C-GigabitEthernet1/0/8]qu
[H3C]int GigabitEthernet 1/0/9
[H3C-GigabitEthernet1/0/9] port link-mode bridge       //配置接口模式为brige
[H3C-GigabitEthernet1/0/9] mirroring-group 1 monitor-port    //配置接口g1/0/9为镜像组的目的端口
[H3C-GigabitEthernet1/0/9] port access vlan 2
[H3C-GigabitEthernet1/0/9] qu
```

2. 配置IPS

```
[H3C]vlan 2                 //创建vlan
[H3C]int GigabitEthernet 1/0/23
[H3C-GigabitEthernet1/0/23] port link-mode bridge     //配置接口模式为brige
[H3C-GigabitEthernet1/0/23] port access vlan 2      //允许vlan 2通过
[H3C]bridge 2 blackhole       //创建黑洞模式Bridge转发实例
[H3C-bridge-2-blackhole] add interface GigabitEthernet1/0/23      //向Bridge转发实例中添加接口
[H3C]security-zone name  inline             //创建安全域inline
[H3C-security-zone-inline] import interface GigabitEthernet1/0/23  vlan 2    //向安全域中添加接口
[H3C]app-profile 103_103_37255_IPv4          //创建app-profile
[H3C-app-profile-103_103_37255_IPv4]  ips apply policy default mode protect   //在app-profile中引用IPS的default策略
[H3C-app-profile-103_103_37255_IPv4]  quit
```

[H3C]object-policy ip inline-inline　　//创建object-policy

[H3C-object-policy-ip-inline-inline] rule inspect 103_103_37255_IPv4　//引用app-pprofile

[H3C]zone-pair security source inline destination inline　　//配置源域和目的域均为inline的域间策略

[H3C-zone-pair-security-inline-inline] object-policy apply ip inline-inline //应用object-policy

一、注意报文的源目安全区域均为接口所在的安全区域。报表上无法区分上下行流量，只能通过发起地址来判断；

二、为了防止环路，交换机和IPS设备对接的接口需要单独划入一个非业务vlan，禁止两端接口类型配置为trunk且放通所有业务vlan。