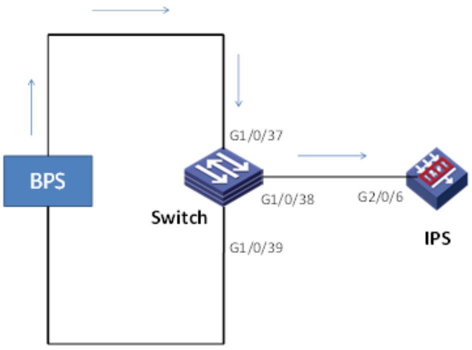
V7 IPS旁路部署inline黑洞转发配置案例

王晗 2016-03-17 发表

如图1所示，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             //创建vlan
[H3C-vlan2]qu
[H3C]mirroring-group 1 local             //配置本地镜像组
[H3C]int GigabitEthernet 1/0/37
[H3C-GigabitEthernet1/0/37] port link-mode bridge    //配置接口模式为brige
[H3C-GigabitEthernet1/0/37] port access vlan 2       //允许vlan 2通过
[H3C-GigabitEthernet1/0/37] mirroring-group 1 mirroring-port both   //配置对接口g1/0/37收发的报文都进行镜像
[H3C-GigabitEthernet1/0/37]qu
[H3C]int GigabitEthernet 1/0/38
[H3C-GigabitEthernet1/0/38] port link-mode bridge       //配置接口模式为brige
[H3C-GigabitEthernet1/0/38] mirroring-group 1 monitor-port   //配置接口g1/0/38为镜像组的目的端口
[H3C-GigabitEthernet1/0/38] qu
[H3C]int GigabitEthernet 1/0/39
[H3C-GigabitEthernet1/0/39] port link-mode bridge    //配置接口模式为brige
[H3C-GigabitEthernet1/0/39] port access vlan 2      //允许vlan 2通过
```

2. 配置IPS

```
[H3C]vlan 2               //创建vlan
[H3C]int GigabitEthernet 2/0/6
[H3C-GigabitEthernet2/0/6] port link-mode bridge    //配置接口模式为brige
[H3C-GigabitEthernet2/0/6] 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 GigabitEthernet2/0/6    //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 GigabitEthernet2/0/6 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
```

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