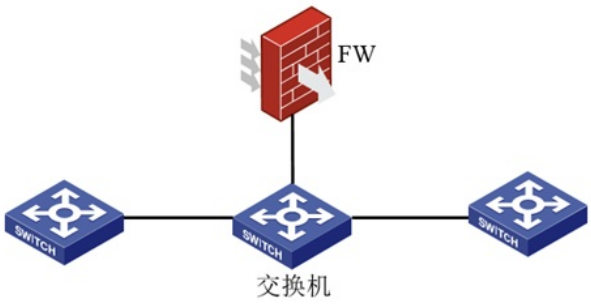
V7 IPS设备旁路做入侵检测设备（IDS）配置举例

IPS防攻击　丁珊　2019-07-26 发表

组网及说明

组网图如下：



配置步骤

设备做旁路IDS，从交换机上将流量镜像到设备上，设备仅做检测不做阻断。

交换机上的配置：

```
#
interface GigabitEthernet1/0/11
 port access vlan 2
 mirroring-group 1 mirroring-port both
#   //镜像端口
#
interface GigabitEthernet1/0/13
 port bridge enable
 mirroring-group 1 monitor-port
#  //镜像的目的端口
#
interface GigabitEthernet1/0/15
 port access vlan 2
 port bridge enable
#   //出接口配置
```

入侵检测上的配置

```
#
interface GigabitEthernet2/0/13
 port link-mode bridge
 port access vlan 2     //配置接收镜像流量的接口
```

在这里放通vlan 2 主要是因为交换机上镜像过来的流量不带vlan标签，如果交换机上镜像过来的流量带有vlan标签，可以选择trunk permit vlan all

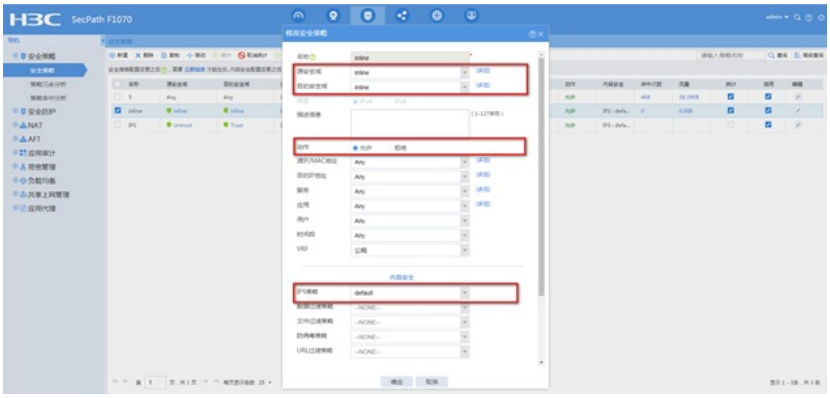
```
#
bridge 2 blackhole
 add interface GigabitEthernet2/0/13   //配置黑洞转发
#
security-zone name inline
 import interface GigabitEthernet2/0/13 vlan 2   将接口加入安全域
#
security-policy ip
 rule 5 name inline
  action pass
  profile 5_IPv4    //配置安全策略当中调用default的IPS策略
  source-zone inline
  destination-zone inline
#
```

配置关键点

web界面上的配置：

也可以在web界面上对策略进行配置，示例当中调用的是default策略，现场也可以根据现网需要自行创建新的策略，如果创建新的策略当中，设置特征筛选条件如果不进行勾选，那么所有的规则都是按照d

efault规则的内容执行。



策略当中并不是所有的规则都是启用的，可以在web界面的【对象】-【应用安全】-【入侵防御】-【特征】当中搜索现网攻击特征的关键字，排查这个规则是否启用，未启用的规则是不会产生IPS日志的

。