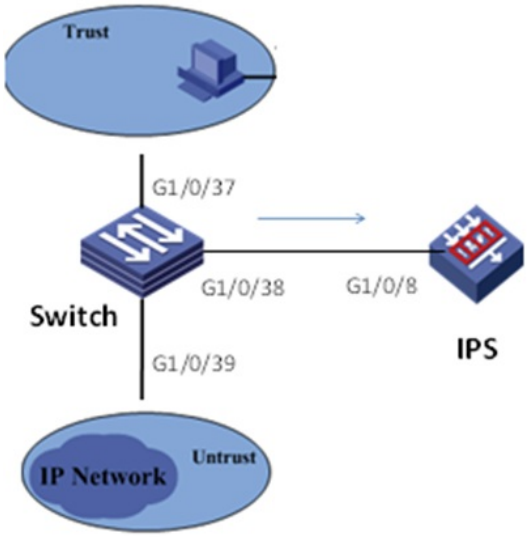
V7 IPS设备旁路做入侵检测设备（IDS）配置举例

IPS防攻击 ZL_qiufeng 2024-06-19 发表

组网及说明

IPS设备旁挂在交换机上，交换机通过端口镜像，将内外网访问流量镜像到设备上。设备在接收到镜像流量后做安全策略及IPS等业务处理，只进行攻击检测并生成告警日志。

图1-1 旁路模式组网图



配置步骤

1.1 配置思路

- 配置交换机镜像组和镜像源目的接口。
- 配置设备inline黑洞模式的Bridge实例并添加接口。
- 配置安全域并添加接口。
- 在安全策略中引用IPS策略。

1.2 配置步骤

1. 配置交换机镜像组和镜像源目的接口

创建vlan

[H3C]vlan 2

[H3C-vlan2]qu

配置本地镜像组

[H3C]mirroring-group 1 local

[H3C]int GigabitEthernet 1/0/37

配置接口模式为brige

[H3C-GigabitEthernet1/0/37] port link-mode bridge

允许vlan 2通过

[H3C-GigabitEthernet1/0/37] port access vlan 2

配置对接口g1/0/37收发的报文都进行镜像

[H3C-GigabitEthernet1/0/37] mirroring-group 1 mirroring-port both

[H3C-GigabitEthernet1/0/37]qu

[H3C]int GigabitEthernet 1/0/38

#配置接口模式为brige

[H3C-GigabitEthernet1/0/38] port link-mode bridge

配置接口g1/0/38为镜像组的目的端口

[H3C-GigabitEthernet1/0/38] mirroring-group 1 monitor-port

[H3C-GigabitEthernet1/0/38] qu

[H3C]int GigabitEthernet 1/0/39

配置接口模式为brige

[H3C-GigabitEthernet1/0/39] port link-mode bridge

允许vlan 2通过

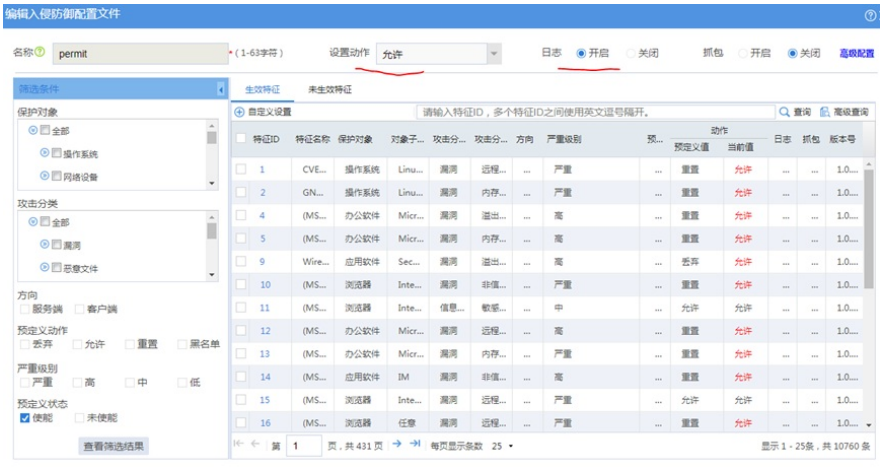
[H3C-GigabitEthernet1/0/39] port access vlan 2

2. 配置设备inline黑洞模式的Bridge实例并添加接口

3. 配置安全域并添加接口

4. 创建安全策略，并引用IPS策略

新建ips策略，配置防护动作为允许，开启日志：



安全策略绑定ips策略

5.执行安全策略“立即加速“和规则下发“提交”