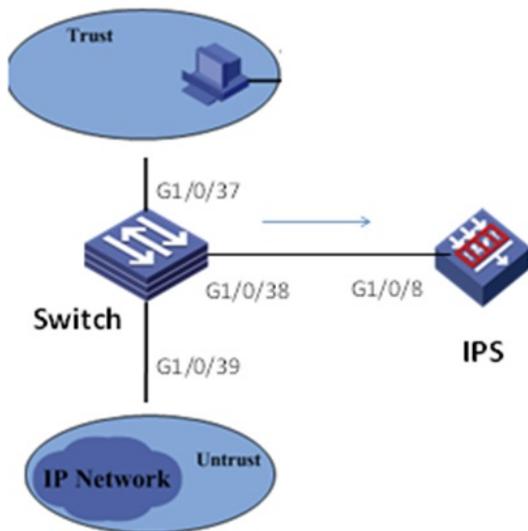


### 组网及说明

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

## 新建接口对

工作模式 ?

反射

黑洞

转发

Bypass功能

开启

关闭

成员

接口一

GE1/0/8

确定

取消

### 3. 配置安全域并添加接口

## 新建安全域

安全域名称

bridge

(1-31字符)

VLAN成员列表 ?

(1-4094)

二层成员列表

Q 筛选

接口列表

GE1/0/1  
GE1/0/2  
GE1/0/6  
GE1/0/7  
GE1/0/12  
XGE1/0/14  
XGE1/0/15  
XGE1/0/17  
XGE1/0/18  
XGE1/0/19

Q 筛选

成员列表(0)

三层成员列表

Q 筛选

接口列表

GE1/0/1  
GE1/0/3  
GE1/0/4  
GE1/0/5  
GE1/0/9  
GE1/0/10  
GE1/0/11  
GE1/0/13  
XGE1/0/16  
XGE1/0/17

Q 筛选

成员列表(1)

GE1/0/8

### 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：

## 编辑入侵防护配置文件

名称 permit (1-63字符) 设置动作 允许 日志 开启 关闭 抓包 开启 关闭 高级配置

生效特征 未生效特征

自定义设置 请输入特征ID，多个特征ID之间使用英文逗号隔开。

特征ID	特征名称	保护对象	对象子...	攻击分...	攻击分...	方向	严重级别	预...	动作	日志	抓包	版本号
1	CVE...	操作系统	Linu...	漏洞	远程...	...	严重	...	重置 允许	...	...	1.0...
2	GN...	操作系统	Linu...	漏洞	内存...	...	严重	...	重置 允许	...	...	1.0...
4	(MS...	办公软件	Micr...	漏洞	溢出...	...	高	...	重置 允许	...	...	1.0...
5	(MS...	办公软件	Micr...	漏洞	内存...	...	高	...	重置 允许	...	...	1.0...
9	Wire...	应用软件	Sec...	漏洞	溢出...	...	高	...	丢弃 允许	...	...	1.0...
10	(MS...	浏览器	Inte...	漏洞	非值...	...	严重	...	重置 允许	...	...	1.0...
11	(MS...	浏览器	Inte...	信息...	敏感...	...	中	...	允许 允许	...	...	1.0...
12	(MS...	办公软件	Micr...	漏洞	远程...	...	高	...	重置 允许	...	...	1.0...
13	(MS...	办公软件	Micr...	漏洞	内存...	...	严重	...	重置 允许	...	...	1.0...
14	(MS...	应用软件	IM	漏洞	非值...	...	高	...	重置 允许	...	...	1.0...
15	(MS...	浏览器	Inte...	漏洞	远程...	...	严重	...	允许 允许	...	...	1.0...
16	(MS...	浏览器	任意	漏洞	远程...	...	严重	...	重置 允许	...	...	1.0...

1 / 431 页 每页显示条数 25 显示 1 - 25 条, 共 10760 条

**新建安全策略**

常规配置

源 VRF 请选择时间段  
公网

目的

操作

动作  允许  拒绝

Web应用防护配置文件 --NONE--

入侵防御配置文件 permit [配置]

数据过滤配置文件 --NONE--

文件过滤配置文件 --NONE--

防病毒配置文件 --NONE--

URL过滤配置文件 --NONE--

APT防御策略 --NONE--

记录日志  开启  关闭

开启策略匹配统计  启用

会话老化时间  启用

长连接老化时间  启用

启用策略  开启  关闭

策略冗余分析

5.执行安全策略“立即加速”和规则下发“提交”

安全策略配置变更之后，如需立即生效，请点击 **立即加速** 按钮。内容安全配置变更之后，如需立即生效，请点击 **提交** 按钮。时

允许配置的最大策略总数为：100000，且每种类型策略数不允许大于50000。

名称	源安全域	目的安全域	类型	ID	描述	源地址	目的地址	服务	转换	用户
<input type="checkbox"/> security	Any	Any	IPv4	5		Any	Any	Any	Any	Any