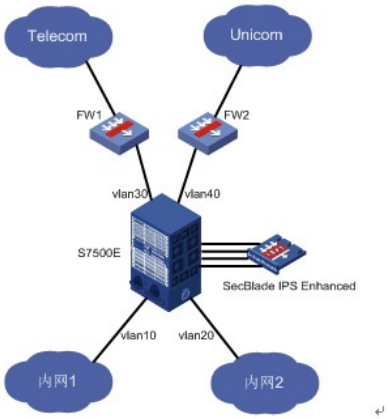
H3C S7500E&S10500 IPS Enhanced插卡开局指导

部署方式 张泷文 2015-10-30 发表

用户S7500E&S10500与防火墙通过以太网线相连。交换机内划分多个VLAN区分内外网段。使用两个C类地址连接外网，其余网段作为内网业务VLAN。

如图3-1所示，VLAN30、VLAN40连接外网，VLAN10、VLAN20连接内网用户。按需求配置进入S7500E&S10500的流量重定向到SecBlade IPS Enhanced的4个内联接口，经匹配的安全防护及流量管理策略处理后在S7500E&S10500上进行三层转发，转发到相应出接口。



1.1 S7500E&S10500主控板相关配置

```
# MQC基本配置
acl number 3000
 rule 0 permit ip
#
acl number 4000                          //过滤掉二层报文，只允许目的MAC为虚接口MAC的IP报文通过
 rule 0 permit type 0800 ffff dest-mac 000f-e22e-94b3 ffff-ffff-ffff
 rule 5 deny
#
traffic classifier IPS operator and
 if-match acl 3000
 if-match destination-mac 000f-e22e-94b3          //匹配vlan虚接口的MAC地址
#
traffic behavior IPS2
 redirect interface Ten-GigabitEthernet3/0/2
traffic behavior IPS3
 redirect interface Ten-GigabitEthernet3/0/3
traffic behavior IPS4
 redirect interface Ten-GigabitEthernet3/0/4
traffic behavior IPS1
 redirect interface Ten-GigabitEthernet3/0/1
#
qos policy up1                     //上行策略up1，将vlan10的流量引到内联口1
 classifier IPS behavior IPS1
qos policy up2                     //上行策略up2，将vlan20的流量引到内联口3
 classifier IPS behavior IPS3
qos policy down1                    //下行策略down1，将vlan30的流量引到内联口2
 classifier IPS behavior IPS2
qos policy down2                    //下行策略down2，将vlan40的流量引到内联口4
 classifier IPS behavior IPS4
# S7500E&S10500交换机其他配置
```

```
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
interface Vlan-interface10                    //内网vlan10
 ip address 10.0.1.1 255.255.255.0
#
interface Vlan-interface20                    //内网vlan20
 ip address 10.0.2.1 255.255.255.0
#
interface Vlan-interface30                    //外网vlan30
 ip address 30.0.3.1 255.255.255.0
#
interface Vlan-interface40                    //外网vlan40
 ip address 30.0.4.1 255.255.255.0
#
interface GigabitEthernet1/0/8                  //连接内网接口1，应用qos策略up1
 port link-mode bridge
 port access vlan 10
 qos apply policy up1 inbound
#
interface GigabitEthernet1/0/9                  //连接内网接口2，应用qos策略up2
 port link-mode bridge
 port access vlan 20
 qos apply policy up2 inbound
#
interface GigabitEthernet1/0/10                  //连接外网接口，应用qos策略down1
 port link-mode bridge
 port access vlan 30
 qos apply policy down1 inbound
#
interface GigabitEthernet1/0/11                  //连接外网接口，应用qos策略down2
 port link-mode bridge
 port access vlan 40
 qos apply policy down2 inbound
#
interface Ten-GigabitEthernet3/0/1                  //内联接口1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 30 40
 packet-filter 4000 outbound                  //过滤掉二层报文
 mac-address mac-learning disable                  //禁止MAC地址学习
#
interface Ten-GigabitEthernet3/0/2                  //内联接口2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 30 40
 packet-filter 4000 outbound
 mac-address mac-learning disable
#
interface Ten-GigabitEthernet3/0/3                  //内联接口3
 port link-mode bridge
 port link-type trunk
```

```
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 30 40
 packet-filter 4000 outbound
 mac-address mac-learning disable
#
interface Ten-GigabitEthernet3/0/4                    //内联接口4
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10 20 30 40
 packet-filter 4000 outbound
 mac-address mac-learning disable
```

IPS Enhanced插卡配置

在IPS插卡上去使能ACFP Client。

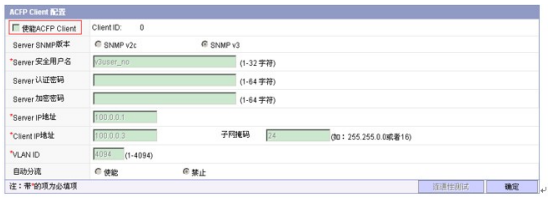


图1-1 去使能ACFP Client

配置安全域、段。

创建安全区域时，注意将内联接口1、3加入内部域，vlan配置10、20；内联接口2、4加入外部域，vlan配置30、40。

由于是单块IPS Enhanced插卡，域应用模式选择“常规”。

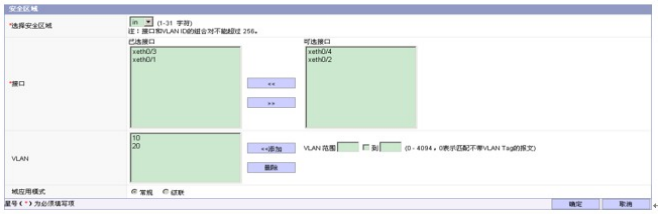


图1-2 配置安全域

	名称	接口列表	VLAN	所属段	操作
	in	xeth0/3 xeth0/1	10, 20	0	
	out	xeth0/4 xeth0/2	30, 40	0	

激活　新建安全区域　删除

图1-3 配置安全域和段

（1）IPS内联接口1、2是一对物理交换表（流量1口进2口发，固定写死）；3、4是一对物理交换表（流量3口进4口发，固定写死）。因此不能把接口1、2配置到同一安全域。接口3、4同理。

（2）流量出IPS内联接口后按照路由转发，不需要在IPS内联接口配置引流策略。

（3）由注意事项2可知，内联接口1的回程流量有可能从内联接口4发回，为了避免来回路径不一致，不能配置两个段（接口1、2一个段；接口3、4一个段）。必须一个段。

（4）S7500E IPS Enhanced插卡支持ACFP自动分流。S7500E开启ACFP自动分流后，整机二三层转发功能失效，请慎重使用。配置方法参见《H3C 万兆IPS开局指导书》。

（5）目前S7500E&S10500 IPS Enhanced插卡不支持ACFP方式引流。