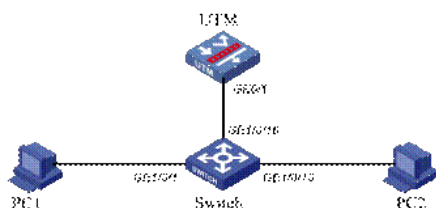


SecPath UTM 跨VLAN二层转发的典型配置

一. 用户需求

某公司内网用户PC1与PC2处于同一网段、但不相同的VLAN中，在此中间加入我司UTM设备作为二层模式使用，实现PC1与PC2之间跨VLAN的访问控制。

二. 组网图



三. 配置步骤

1. 交换机配置:

```
#
interface GigabitEthernet1/0/1 //将PC1划入VLAN 102
port access vlan 102
#
interface GigabitEthernet1/0/10 //将PC2划入VLAN 103
port access vlan 103
#
interface GigabitEthernet1/0/16 //配置与UTM互连接口
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 102 to 103
#
```

2. UTM命令行配置:

```
#
vlan 102 to 103
#
vlan 1000
#
interface GigabitEthernet0/1
port link-mode bridge
port link-type trunk
port trunk permit vlan 1 102 to 103
#
```

3. UTM WEB配置:

在导航栏中选择“设备管理 > 接口管理”界面，新建二层子接口GE0/1.102和GE0/1.103。

接口创建	
接口名称:	GigabitEthernet0/1 102 (1-4094)
VID:	(1-4094)
MTU:	
TCP MSS:	
IP配置:	☐ 无IP配置 ☐ 静态地址 ☐ DHCP ☐ BOOTP ☐ PPP协商 ☐ 借用地址
IP地址:	
网络掩码:	24 (255.255.255.0)
其他接口:	GigabitEthernet0/0
星号(*)为必填项	
确定 返回	

在导航栏中选择“网络管理 > VLAN > VLAN”,将接口GE0/1.102和GE0/1.103都加入VLAN 1000。

修改 VLAN

ID: 1000

描述: VLAN 1000 (1-32字符)

端口	Untagged 成员端口	Tagged 成员端口	非成员
GigabitEthernet0/1	☐	☐	☒
GigabitEthernet0/2	☐	☐	☒
GigabitEthernet0/1.102	☒	☐	☐
GigabitEthernet0/1.103	☒	☐	☐

在导航栏中选择“设备管理 > 安全域”，将GE0/1和GigabitEthernet0/1.102加入Trust安全域（所属vlan 应包含1000）；将GigabitEthernet0/1.103加入Untrust安全域（所属vlan 应包含1000）；

修改安全域

ID: 2

域名: Trust

优先级: 85 (1-100)

共享: No

虚拟设备: Root

子网地址: 多选

接口: 查询项: 接口 关键字: 查询

接口	所属 VLAN
☐ GigabitEthernet0/0	
☐ GigabitEthernet0/4	
☐ NULL0	
☒ Vlan-interface2	
☒ Vlan-interface1000	
☒ GigabitEthernet0/1	1-4094
☒ GigabitEthernet0/1.102	1-4094
☐ GigabitEthernet0/1.103	1-4094

4.PC1与PC2 IP配置:

PC1: 192.168.2.10/24

PC2: 192.168.2.11/24

- (1) 从PC1 Ping PC2地址: 192.168.2.10, 得到结果A;
- (2) 从PC2 Ping PC1地址: 192.168.2.11, 得到结果B;
- (3) 再将GigabitEthernet0/1加入Untrust域后, PC1 ping PC2, 得到结果C;
- (4) UTM 删除vlan 1000, 只有vlan 102 103, PC1 Ping PC2, 得到结果D;
- (5) UTM 删除vlan 102 103, 只有vlan 1000, PC1 Ping PC2, 得到结果E;

四. 验证结果

- A、PC1能够 Ping通PC2;
- B、PC2不能够Ping通PC1; (PC2处于untrust安全域, PC1处于trust安全域, trust域优先级高于untrust域优先级)
- C、PC1能够 Ping通PC2; (物理口工作在桥模式, 使用二层子接口实现跨vlan转发, 出入报文域由二层子接口所在安全域确定, 将GigabitEthernet0/1加入untrust域不影响互通)
- D、PC1能够 Ping通PC2; (删除vlan1000后, 子接口GE0/1.102, GE0/1.103默认属于vlan1, 所以流量能通过)
- E、PC1不能够Ping通PC2; (vlan不存在, 无法建立二层转发表)
- F、PC1 能够 ping通PC2。

五. 注意事项

- (1) 配置跨Vlan二层转发, 要保证存在与二层子接口ID相同的Vlan才能正常转发;
- (2) 物理口工作在桥模式, 使用二层子接口实现跨vlan转发, 出入报文域由二层子接口所在安全域确定, 不受物理口所在安全域的影响;
- (3) 跨Vlan二层转发, 加入安全域的子接口的Vlan范围要包含子接口的PVID, 才能通流量;
- (4) 子接口下若不配置vlan, 则PVID为1, 在设置加入域的Vlan范围时要包含vlan 1;
- (5) 跨Vlan二层转发, 不要将子接口PVID配置为和子接口ID相同, 否则可能下游交换机MAC学习会产生问题, 该问题已列为缺陷。

