SecPath UTM 二三层混合转发的典型配置

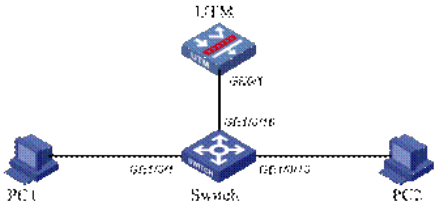
万欣 2009-06-06 发表

SecPath UTM 二、三层转发混合转发的典型配置

一．用户需求

某公司内网用户PC1与PC2处于不同网段，在此中间加入我司UTM设备作为混合模式使用，实现PC1与PC2之间访问控制。

二．组网图



三．配置步骤

1.交换机配置

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

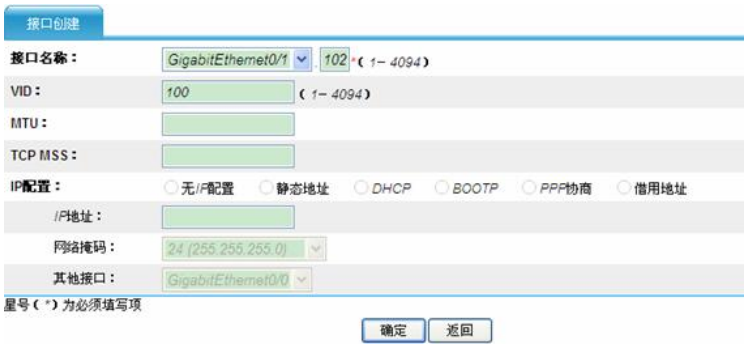
2.UTM命令行配置

```
#
vlan 100 to 103
#
interface GigabitEthernet0/1
   port link-mode bridge
   port link-type trunk
   port trunk permit vlan 1 102 to 103
#
```

3.UTM的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，加入VLAN100；新建Vlan-interface100，配置IP地址为192.168.2.1/24；新建Vlan-interface103， 配置IP地址为192.168.3.1/24。

（1）新建接口GE0/1.102

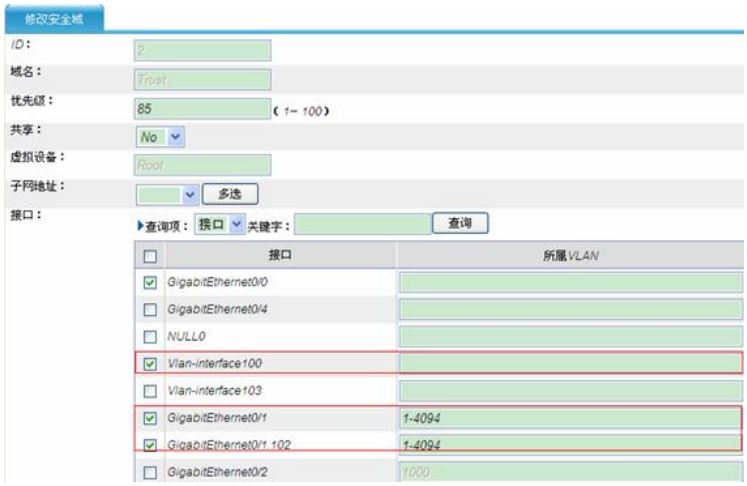


（2）新建接口Vlan-interface100

（3）新建接口Vlan-interface103

在导航栏中选择“设备管理 > 安全域”，编辑Trust安全域，将GE0/1、Vlan-interface100、GigabitEthernet0/1.102子接口加入该安全域；编辑Untrust安全域，将vlan-interface103加入Untrust安全域。

（4）编辑Trust安全域



（5）编辑Untrust安全域

（6）PC机IP地址配置：

PC1：192.168.2.10/24 缺省网关：192.168.2.1
PC2：192.168.3.11/24 缺省网关：192.168.3.1
PC1 Ping PC2 地址：192.168.3.11，查看结果A；

（7）编辑域间策略

在导航栏中选择“防火墙 > 安全策略 > 域间策略”界面，建立从Untrust到Trust域的permit all 策略：

然后从PC2 Ping PC1地址：192.168.2.1，查看结果B。

四．验证结果

A、能够ping通；
B、能够ping通；

五．配置注意事项

二层子接口的PVID不能与接口ID相同，也不能与三层vlan虚接口所在Vlan相同；本例中，二层子接口ID 102，PVID为100，三层虚接口vlan ID为103。