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192.16 8.3.1/24。

(1) 新建接口GE0/1.102

後口名称:	GigabitEthernet0/1 💙 102 • (1- 4094)
vio :	100 (1-4094)
мти:	
TCP MSS :	
P配置:	○无IP配置 ● 静态地址 ● DHCP ● BOOTP ● PPP协商 ● 借用地址
/P地址:	
网络捷码:	24 (255.255.255.0) 👻
其他接口:	GigabitEthemet0/0 ×

(2) 新建接口Vlan-interface100

接口名称:	Vlan-interface 100 *(1- 4094)
/ID :	
мти :	
TCP MSS :	
P配置:	○无IP配置 ●静态地址 ○DHCP ○BOOTP ○PPP协商 ○借用地址
/产地址:	192.168.2.1
网络掩码:	24 (255.255.255.0)
其他接口:	GlaabitEthemet0/0 ×

(3) 新建接口Vlan-interface103

行名称:	Vlan-interface 103 *(1- 4094)
/ID:	
MTU:	
TCP MSS :	
P配置:	○无IF配置 ●静态地址 ○DHCP ○BOOTP ○PPP协商 ○借用地址
/产地址:	192.168.3.1
网络掩码:	24 (255.255.255.0)
其他接口:	GloabitEthemet0/0 ×

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、GigabitEthern et0/1.102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

修改安全城		
ID:	2	
峨名:	Trust	
优先级:	85 (1- 100)
共享:	No 💌	
整想设备:	Root	
子网地址:	✓ 多选	
接口:	▶查询项: 接口 ¥关键字:	查询
	田田田	所麗VLAN
	GigabitEthernet0/0	
	GigabitEthernet0/4	
	NULLO	
	Vian-interface100	
	Vlan-interface 103	
	GigabitEthernet0/1	1-4094
	GigabitEthernet0/1.102	1-4094
	GigabitEthernet0/2	1000

(5) 编辑Untrust安全域

修改安全城										
ID:	4									
域名:	Untrost									
忧先愆:	5 (1-10))								
共享:	No									
虚拟设备:	Root									
子阿地址:	✓ 多选									
接口:	▶查询项: 接口 ¥ 关键字: 查询									
	1 接口	所屬VLAN								
	GigabitEthernet0/3									
	GigabitEthernet0/4									
	NULLO									
	Vian-interface60									
	Vlan-interface103									
	GigabitEthernet0/2	1-999, 1001-4094								

(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:

2992	目的城	規則の	VPN 实例	澄/P地址	目的/P地址	服务	时间段	过滤动作	描述	启用选项	日志功能	擾 MAC 地址	目的 MAC 地址		操作			
Untrust	Trust	0		any address	any address	any service		Permit		◎蓋	未开启			ø	1	¢	n v	6

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。