H3C SecPath F100-A防火墙VLAN透传的典型配置

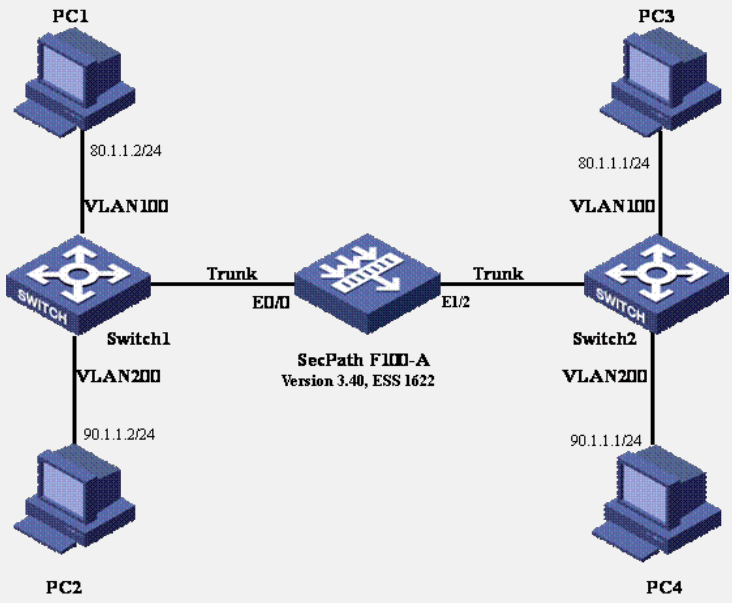
赵彪 2007-06-12 发表

H3C SecPath F100-A防火墙VLAN透传的典型配置

一、 组网需求：

客户端PC1和PC3属于VLAN100，客户端PC2和PC4属于VLAN200，用来模拟属于不同VLAN的用户，在Switch1和Switch2与防火墙相连接口上都要配置成Trunk模式，保证带Tag标记的报文能够透传。

二、 组网图：



支持混合模式的产品型号有：Secpath F1000-A/F1000-S/F100-E/F100-A；版本要求Comware software, Version 3.40, ESS 1622及以后。

三、 配置步骤：

当前视图	配置命令	注释
[H3C]	firewall packet-filter default permit	防火墙包过滤默认改为允许
[H3C]	undo insulate	取消以太网接口隔离
[H3C]	bridge enable	使能桥组功能
[H3C]	bridge 1 enable	创建桥组1
[H3C]	interface Ethernet 0/0	进入连接e0/0的接口视图
[H3C-Ethernet0/0]	bridge-set 1	将接口e0/0加入到桥组1
[H3C-Ethernet0/0]	bridge vlanid-transparent-transmit enable	使能接口VLAN透传
[H3C-Ethernet0/0]	interface Ethernet 1/2	进入连接e1/2的接口视图
[H3C-Ethernet1/2]	bridge-set 1	将接口e1/2加入到桥组1
[H3C-Ethernet1/2]	bridge vlanid-transparent-transmit enable	使能接口VLAN透传
[H3C-Ethernet1/2]	quit	退回系统视图
[H3C]	firewall zone trust	进入trust区域视图
[H3C-zone-trust]	add interface Ethernet0/0	将接口e0/0加入到trust区域
[H3C-zone-trust]	quit	退回系统视图
[H3C]	firewall zone untrust	进入untrust区域视图
[H3C-zone-untrust]	add interface Ethernet 1/2	将接口e1/2加入到untrust区域
[H3C-zone-untrust]	quit	退回系统视图

四、 配置关键点：

1、子接口不支持VLAN透传；

2、SecPath F100-A设备的四个LAN接口需要执行undo insulate命令聚合成一个接口

才能使用VLAN透传功能；
3、VLAN透传与交换机的Trunk功能并不相同，当与交换机互通时，如果希望SecPath防火墙与交换机的管理VLAN 互通，需要借助子接口来实现。即将配置了与交换机管理VLAN ID相同的子接口加入到桥组，并创建相应的桥组虚接口（BVI接口），配置同一网段地址，则防火墙的桥组虚接口就可以与交换机管理VLAN接口互通。