SecPath系列防火墙开启IP欺骗防范导致正常报文被丢弃的解决方法

王思军 2006-09-18 发表

SecPath系列防火墙开启IP欺骗防范导致
正常报文被丢弃的解决方法

一、问题描述：

在如下四种组网环境中，SecPath防火墙开启firewall defend ip-spoofing，会导致防火墙丢弃正常报文：

1、SecPath启用某些VPN功能时，包括启用L2TP、DVPN，有些协议报文会被丢弃,VPN无法建立；

2、SecPath上配置策略路由时，匹配到策略路由的报文被丢弃；

3、SecPath上配置等值路由时，匹配到等值路由的报文被丢弃。

4、SecPath上，当报文出入防火墙的接口不一致时。

二、原因分析：

防火墙启用IP欺骗防范后通过反查路由表确定报文是否为攻击报文，在上述四种应用环境下，会导致SecPath防火墙IP欺骗防范功能误报，正常报文被丢弃。

三、处理措施：

本次受影响的产品涉及到Quidway SecPath全系列防火墙，包括SecPath10F、SecPath100F-S、SecPath100F、SecPath100F-E、SecPath500F、SecPath1000F；涉及的版本包括当前发布的所有版本：VRP3.4-R1210P01及以前版本。SecPath1800F上不存在此问题。

规避的措施：在上述四种组网环境下，不要配置firewall defend ip-spoofing 启用防火墙的IP欺骗防范功能；已经启用了该功能的局点，全局模式下用undo firewall defend ip-spoofing命令关闭该功能。