防火墙更改网络结构后网络不通

孟金宝 2008-12-10 发表

某公司防火墙结构调整后网络不通

问题描述：

某公司出口为两台防火墙，原先分别接网通和电信，全国有200多分支，分别通过IPSEC接到500F。
调整网络结构如下，两台500F对外作VRRP。所有分支连接到虚地址，实现防火墙的备份。
路由引入：
在主500f引入10.32/25网段的静态路由。
在备500f也引入10.32/25路由，但cost为100。以实现正常情况下内部网去往10.32走主防火墙。
调整后发现下面的分支有的pc可以访问服务器，有的就不可以。

解决方案：

经检查，在右下角的交换机上去往10.32网段时要去往主500F，但是去往主500F（ospf中的ASBR路由器）存在两台等价路由，一条走备防火墙，一条走左边交换机。
当选择走备防火墙时，报文走到备防火墙，发现还有一条preference为60的静态路由，高于从主防火墙过来的ASE路由（preference 150），所以不会发到主防火墙，但是由于没有ipsec隧道，所以也不可能发到分支。于是不通。
另有一些报文选择了走左边交换机，则正常。

需要将首包检查关闭，命令如下：
Firewall session aging-time 260 （260为特殊值，关闭首包检