关于S8016交换机和天融信防火墙三层不通的案例

王雪梅 2006-02-16 发表

关于S8016交换机和天融信防火墙三层不通的案例

组网:

问题描述:
某政府部门采用我司S8016交换机作为核心网络交换机组网，下面连接华为3026二层以太网交换机，用户的网关都在S8016上。
S8016上行连接天融信防火墙，采用三层互联方式。所有上公网的报文全部送到防火墙上，由防火墙做NAT转换后访问互联网络资源。
原来网络采用S3526E作为核心设备和防火墙互联，S3526E做缺省路由将报文送到防火墙上公网，业务正常。
现在将S3526E交换机改为S8016交换机，防火墙的配置没有更改。将原有的S3626E交换机的配置移到S8016上。但是用户无法上网。

原因分析:
原有的组网用S3526E交换机只是简单的三层互通，用户的报文送到防火墙做NAT转换上公网，表明防火墙的回程路由生效没有问题。
将S8016替换S3526E交换机，S8016的三层功能不存在问题，而且S8016和防火墙之间互联网段能够PING通。但是在S8016上带着用户网段的IP地址无法PING通防火墙上和S8016互联的那个IP地址。这个表明防火墙上的回程路由没有生效。
问题集中在防火墙的回程路由是否对S8016生效：如果不生效，为什么只对S3526E生效，而对S8016不生效。

测试的具体操作:
测试一：确认并证明防火墙回程路由没有生效，或者说对S8016没有生效
在S8016上以用户网段的地址为源地址去PING防火墙的三层地址，不通。查看S8016和防火墙互联的接口，该接口上收发数据都有。无法判断多方是否真的把这个PING包报文送回来。
采用端口镜像方式，将S8016和防火墙互联接口镜像到其他接口上，在监测端口用SNIFFER进行抓包。用超级终端在S8016上以用户网段的地址为源地址去PING防火墙的三层地址。在SNIFFER上能够看到端口出去的报文，始终没有回来的报文，证明了防火墙并没有将回程的报文送回到S8016上。
测试二：明确防火墙为何能够和S3526E配合良好，难道回程路由和设备有关系?
用户表明原来在使用S3526E和防火墙互通，路由没有问题。但是有个前提，就是将两个设备同时重新启动一下。如果重启后还是上不了网，那就还要同时在重启两边设备。直到能够上网为止。
从用户的描述来看，初步估计了防火墙在二层ARP上可能存在一些问题。多次的重启才能建立一个ARP表项。但是由于防火墙和交换机直连路由没有问题，否决了ARP学习能力的问题。那么问题出在回程路由的配置或者回程路由和下一跳转发配合那里。
查看防火墙的路由如下:

```
[sadm@xxxx3000]# route
Current IP Routing Table:
------------------------------------------------------------
Destination     Genmask       Gateway         Interface
192.1.1.3       255.255.255.255  0.0.0.0         eth2
192.0.0.0       255.0.0.0       0.0.0.0         eth2
0.0.0.0         0.0.0.0         218.x.x.x       eth0
[sadm@xxxx3000]#
```

从路由上能够看到整个192网段的路由确实送到了eth2接口。也就是说送到了S8016上。并且还针对S8016的三层地址做了一条主机路由。
主机路由：192.1.1.3   255.255.255.255 0.0.0.0   eth2
查看防火墙的ARP表项:

```
[sadm@NGFW3000]# arp
Current Firewall Arp Table:
------------------------------------------------------------------------------
Address           HWtype       HWaddress          Flags Mask        Iface
```

192.1.1.3 ether 00:E0:FC:1B:A6:00 C eth2
从以上信息来看防火墙上基本的数据都有了。

解决方法：
经确认，他们这么做路由没有什么问题的。后来建议在他们的路由的下一跳改成IP地址的方式试一试
。
路由表改成如下：
192.0.0.0 255.0.0.0 192.1.1.3 eth2
问题解决。