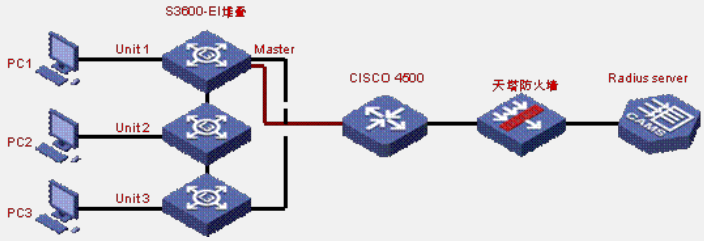
S3600堆叠后通过友商设备到达cams做认证的案例

董亮 2007-07-27 发表

S3600堆叠后通过友商设备到达cams做认证的案例

一、 组网：



三台S3600交换机作堆叠，在Master上连接cisco 4500,然后连接到天塔防火墙，最终连接到cams做认证.

二、 问题描述：

只有连接到Unit 1上的pc可以认证成功，如上图所示，只有pc 1可以认证成功。

三、 过程分析：

（1）在cams侧抓包，确认cams处理流程是否正确，最终确认是正确的。

（2）在设备侧，连接cisco设备的端口处抓包，对于堆叠的设备，发送request报文的源端口分别是5001（表示unit1设备，）5002表示unit2设备，5003表示unit3设备。在这种情况下，unit1发送的报文都正常到达cams服务器，并且cams回应的报文也正常到达了堆叠设备，但是unit2和unit3发送的radius报文到达cams后，cams给堆叠设备的的回应报文却没有送达堆叠设备。

（3）根据以上分析，确定cams回应的带有端口号5002，5003的报文被防火墙或cisco设备丢弃了，最终检查防火墙的配置，防火墙上只允许5001的UDP端口号通过，而拒绝了5002/5003等端口号的UDP报文通过。因此问题原因为防火墙丢弃认证回应报文所致

四、 解决方法：

在天塔防火墙上开放端口号5002和5003.允许端口号为5002，5003的UDP报文通过。