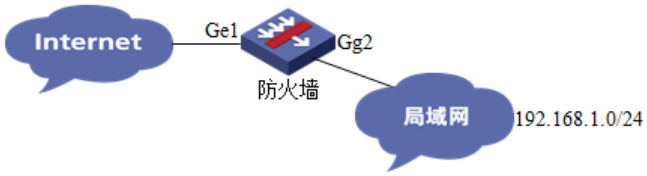
F100-X-G防火墙限制迅雷、QQ的配置案例

应用审计 刘嘉炜 2016-06-21 发表

客户购买F100-X-G的防火墙，内网用户为192.168.1.0网段。想要部分用户禁止访问迅雷和QQ等应用
。



1、分别设置外网接口和内网接口的IP地址（x.x.x.x为外网IP地址、192.168.1.1为内网网关）。

2、接口加入对应的安全区域

将0/1口加入到“untrust”区域，将0/2口加入到“trust”区域。

3、配置用于NAT的ACL

4、配置NAT

选择外网接口、ACL调用之前设置的ACL 2000、地址转换方式设置为Easy ip。

5、配置默认路由

x.x.x.x为外网网关

二、限制策略的使用

6、配置前需要注意

1）设备是否购买特征库licence，如果没有特征库相应的流量无法识别。

2）设备是否购买CF卡，需要设备携带CF卡运行深度检测模块应用。

3）防火墙需要运行在UTM模式，单独的防火墙模式下没有深度检测。

7、切换防火墙为“UTM”模式

设备当前运行模式必须选择为“UTM”模式。

8、注意在自动升级特征库前一定要设置设备的域名解析。

升级后的特征库版本

9、在“深度安全防御”中“带宽管理策略应用”中“新建”。

设置源域为“trust”目的域为“untrust”源IP地址为192.168.1.0网段。

10、设置过滤QQ

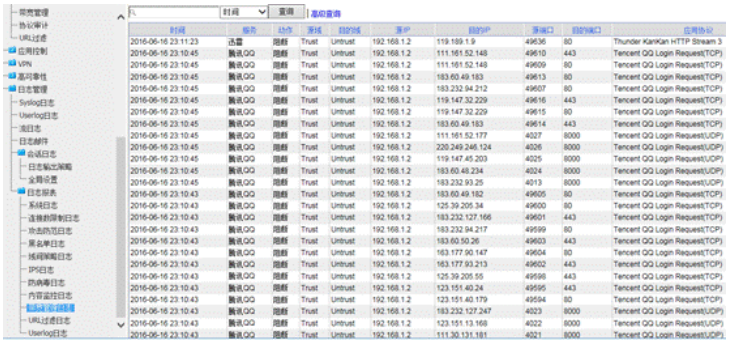
11、设置过滤迅雷

12、设置禁止动作并记录日志

实验结果：

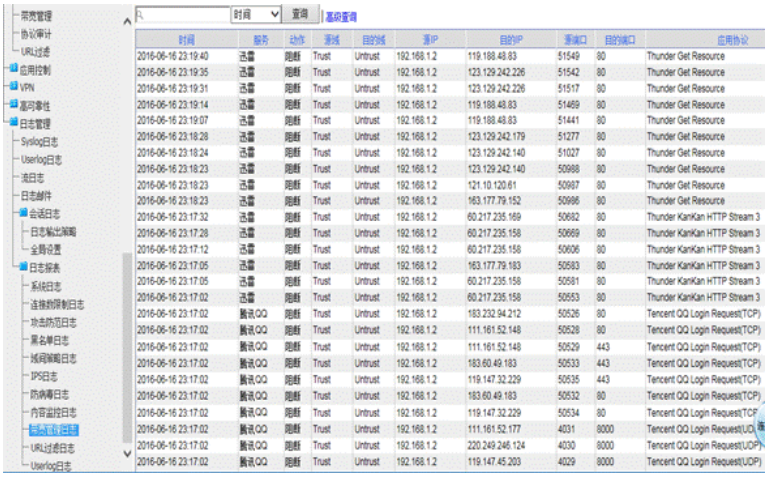
1、测试QQ无法登陆

2、在日志报表中带宽管理日志中查看阻断日志。



3、测试迅雷无法登陆

4、在日志报表中带宽管理日志中查看阻断日志。



1、策略在做上去后，对于已经登录的QQ、已经下载的是没有作用的。

2、防火墙在过滤迅雷、QQ等应用时，需要将防火墙设置在UTM模式。

3、如果发现无法过滤相关应用时请及时更新特征库。

4、使用自动升级的时候需要保证您的设备开启了DNS代理，并设置了DNS服务器地址。

5、特征库是需要维护的，我们会在定时更新特征库。如果发现自动更新请等待一段时间后再去更新。