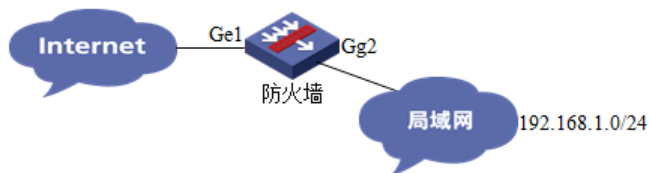


知 F100-X-G防火墙限制迅雷、QQ的配置案例

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。

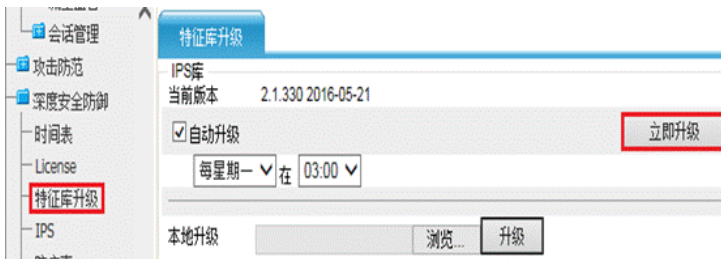
7. 切换防火墙为“UTM”模式



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“深度安全防护”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无法登录



2、在日志报表中带宽管理日志中查看阻断日志。

时间	源IP	目的IP	源端口	目的端口	应用协议	
2016-06-16 23:11:23	192.168.1.2	119.188.48.83	49536	80	Thunder Kankan HTTP Stream 3	
2016-06-16 23:10:45	腾讯QQ	192.168.1.2	111.161.52.148	49610	443	Tencent QQ Login Request(TCP)
2016-06-16 23:10:45	腾讯QQ	192.168.1.2	111.161.52.148	49609	80	Tencent QQ Login Request(TCP)
2016-06-16 23:10:45	腾讯QQ	192.168.1.2	183.80.49.183	49613	80	Tencent QQ Login Request(TCP)
2016-06-16 23:10:45	腾讯QQ	192.168.1.2	183.232.94.212	49607	80	Tencent QQ Login Request(TCP)
2016-06-16 23:10:45	腾讯QQ	192.168.1.2	119.147.32.229	49616	443	Tencent QQ Login Request(TCP)
2016-06-16 23:10:45	腾讯QQ	192.168.1.2	119.147.32.229	49615	80	Tencent QQ Login Request(TCP)
2016-06-16 23:10:45	腾讯QQ	192.168.1.2	183.80.49.183	49614	443	Tencent QQ Login Request(TCP)
2016-06-16 23:10:45	腾讯QQ	192.168.1.2	111.161.52.177	4027	8000	Tencent QQ Login Request(UOP)
2016-06-16 23:10:45	腾讯QQ	192.168.1.2	200.249.246.124	4026	8000	Tencent QQ Login Request(TCP)
2016-06-16 23:10:45	腾讯QQ	192.168.1.2	119.147.45.203	4025	8000	Tencent QQ Login Request(TCP)
2016-06-16 23:10:45	腾讯QQ	192.168.1.2	183.80.49.234	4024	8000	Tencent QQ Login Request(UOP)
2016-06-16 23:10:45	腾讯QQ	192.168.1.2	183.232.93.25	4013	8000	Tencent QQ Login Request(UOP)
2016-06-16 23:10:43	腾讯QQ	192.168.1.2	183.80.49.182	49605	80	Tencent QQ Login Request(TCP)
2016-06-16 23:10:43	腾讯QQ	192.168.1.2	129.39.205.84	49600	80	Tencent QQ Login Request(TCP)
2016-06-16 23:10:43	腾讯QQ	192.168.1.2	183.232.127.166	49601	443	Tencent QQ Login Request(TCP)
2016-06-16 23:10:43	腾讯QQ	192.168.1.2	183.232.94.217	49599	80	Tencent QQ Login Request(TCP)
2016-06-16 23:10:43	腾讯QQ	192.168.1.2	183.80.30.26	49603	443	Tencent QQ Login Request(TCP)
2016-06-16 23:10:43	腾讯QQ	192.168.1.2	183.177.90.147	49604	80	Tencent QQ Login Request(TCP)
2016-06-16 23:10:43	腾讯QQ	192.168.1.2	183.177.93.213	49602	443	Tencent QQ Login Request(TCP)
2016-06-16 23:10:43	腾讯QQ	192.168.1.2	129.39.205.55	49598	443	Tencent QQ Login Request(TCP)
2016-06-16 23:10:43	腾讯QQ	192.168.1.2	123.155.40.24	49595	443	Tencent QQ Login Request(TCP)
2016-06-16 23:10:43	腾讯QQ	192.168.1.2	123.155.40.179	49584	80	Tencent QQ Login Request(TCP)
2016-06-16 23:10:43	腾讯QQ	192.168.1.2	183.232.127.247	4023	8000	Tencent QQ Login Request(UOP)
2016-06-16 23:10:43	腾讯QQ	192.168.1.2	123.151.13.168	4022	8000	Tencent QQ Login Request(UOP)
2016-06-16 23:10:43	腾讯QQ	192.168.1.2	111.30.131.181	4021	8000	Tencent QQ Login Request(UOP)

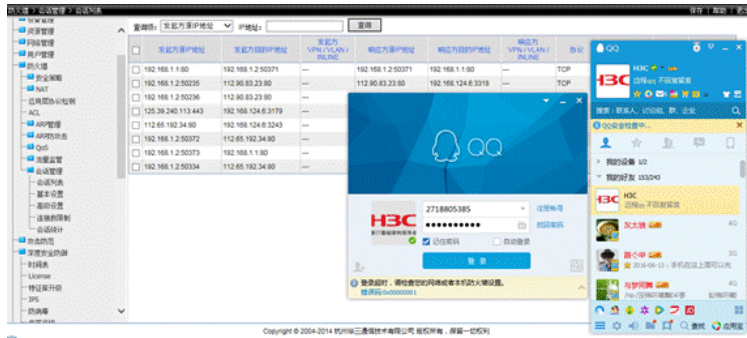
3、测试迅雷无法登录



4、在日志报表中带宽管理日志中查看阻断日志。

时间	源IP	目的IP	源端口	目的端口	应用协议	
2016-06-16 23:19:40	迅雷	192.168.1.2	119.188.48.83	51549	80	Thunder Get Resource
2016-06-16 23:19:35	迅雷	192.168.1.2	123.129.242.226	51542	80	Thunder Get Resource
2016-06-16 23:19:31	迅雷	192.168.1.2	123.129.242.226	51517	80	Thunder Get Resource
2016-06-16 23:19:14	迅雷	192.168.1.2	119.188.48.83	51489	80	Thunder Get Resource
2016-06-16 23:19:07	迅雷	192.168.1.2	119.188.48.83	51441	80	Thunder Get Resource
2016-06-16 23:18:28	迅雷	192.168.1.2	123.129.242.179	51277	80	Thunder Get Resource
2016-06-16 23:18:24	迅雷	192.168.1.2	123.129.242.140	51027	80	Thunder Get Resource
2016-06-16 23:18:23	迅雷	192.168.1.2	123.129.242.140	50988	80	Thunder Get Resource
2016-06-16 23:18:23	迅雷	192.168.1.2	121.10.120.61	50967	80	Thunder Get Resource
2016-06-16 23:18:23	迅雷	192.168.1.2	183.177.79.152	50966	80	Thunder Get Resource
2016-06-16 23:18:23	迅雷	192.168.1.2	80.217.235.169	50882	80	Thunder Kankan HTTP Stream 3
2016-06-16 23:18:23	迅雷	192.168.1.2	80.217.235.158	50669	80	Thunder Kankan HTTP Stream 3
2016-06-16 23:18:23	迅雷	192.168.1.2	80.217.235.158	50606	80	Thunder Kankan HTTP Stream 3
2016-06-16 23:18:23	迅雷	192.168.1.2	183.177.79.183	50583	80	Thunder Kankan HTTP Stream 3
2016-06-16 23:18:23	迅雷	192.168.1.2	80.217.235.158	50581	80	Thunder Kankan HTTP Stream 3
2016-06-16 23:18:23	迅雷	192.168.1.2	80.217.235.158	50583	80	Thunder Kankan HTTP Stream 3
2016-06-16 23:18:23	迅雷	192.168.1.2	183.232.94.212	50526	80	Tencent QQ Login Request(TCP)
2016-06-16 23:18:23	迅雷	192.168.1.2	111.161.52.148	50528	80	Tencent QQ Login Request(TCP)
2016-06-16 23:18:23	迅雷	192.168.1.2	111.161.52.148	50529	443	Tencent QQ Login Request(TCP)
2016-06-16 23:18:23	迅雷	192.168.1.2	183.80.49.183	50533	443	Tencent QQ Login Request(TCP)
2016-06-16 23:18:23	迅雷	192.168.1.2	119.147.32.229	50535	443	Tencent QQ Login Request(TCP)
2016-06-16 23:18:23	迅雷	192.168.1.2	183.80.49.183	50532	80	Tencent QQ Login Request(TCP)
2016-06-16 23:18:23	迅雷	192.168.1.2	119.147.32.229	50534	80	Tencent QQ Login Request(TCP)
2016-06-16 23:18:23	迅雷	192.168.1.2	111.161.52.177	4031	8000	Tencent QQ Login Request(UOP)
2016-06-16 23:18:23	迅雷	192.168.1.2	200.249.246.124	4030	8000	Tencent QQ Login Request(UOP)
2016-06-16 23:18:23	迅雷	192.168.1.2	119.147.45.203	4029	8000	Tencent QQ Login Request(UOP)

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。