F1000-X-G2/F100-X-G2系列限制迅雷、QQ等应用配置举例

应用审计 zhiliao_5ilsv 2019-09-03 发表

组网及说明

1 配置需求及说明

1.1 适用的产品系列

本案例适用于如F1000-A-G2、F1000-S-G2、F100-M-G2、F100-S-G2等F1000-X-G2、F100-X-G2系列的防火墙。

1.2 使用限制

防火墙应用控制功能需要安装License才能使用。License过期后，应用控制功能可以采用设备中已有的应用控制特征库正常工作，但无法升级特征库。

配置前请在防火墙界面“系统”>”License”>”授权信息”中确认应用（ACG）特性为激活状态。

License授权信息

刷新

位置	特性名称	是否授权	状态
Slot1	ACG	Y	In use
Slot1	AV	N	-
Slot1	IPS	N	-
Slot1	SLB	N	-
Slot1	SSLVPN	N	-
Slot1	UFLT	N	-

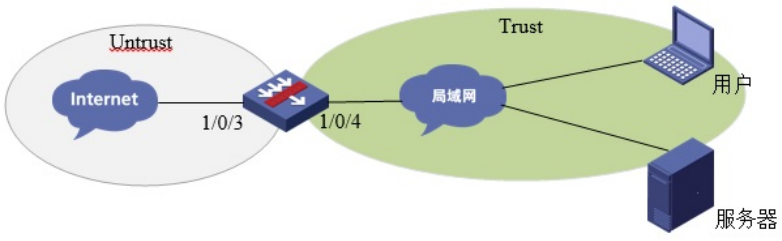
1.3 功能介绍及配置需求

应用审计与管理是在APR（Application Recognition，应用层协议识别）的基础上进一步识别出应用的具体行为（比如IM聊天软件的用户登录、发消息等）和行为对象（比如IM聊天软件登录的行为对象是账号信息等），据此对用户的上网行为进行审计和记录。

配置需求：

1）某公司为保证良好的工作氛围，需部署防火墙配置应用访问控制，达到公司员工在工作时间不能访问迅雷、QQ等与工作无关的软件。

2 组网图



配置步骤

3 配置步骤

3.1 基础组网配置

略

3.2 升级特征库至官网最新版本

在防火墙界面“系统”>”升级中心”>”特征库升级”中对特征库进行升级

升级中心列表

刷新 配置代理服务器

特征库	当前版本	版本发布日期	开启定时升级	定时升...	操作
入侵防御特征库	1.0.35	2017-05-17		-	立即升级 | 本地升级 | 版本回退
防病毒特征库	1.0.36	2017-05-13		-	立即升级 | 本地升级 | 版本回退
应用识别特征库	1.0.0	1999-12-31		-	立即升级 | 本地升级 | 版本回退
URL特征库	1.0.0	1999-12-31		-	立即升级 | 本地升级 | 版本回退

3.2.1 自动升级操作过程

1. 设备开启DNS代理并配置DNS服务器地址

在防火墙界面“网络”>”DNS”>”高级设置”开启防火墙DNS代理功能。

在防火墙界面“网络”>”DNS”>”DNS客户端”中添加DNS服务器地址。

2. 设备必须可以连接互联网

在防火墙界面“网络”>”探测工具”>”Ping”中测试域名是否可以正常解析?

3. 开启设备定时升级功能

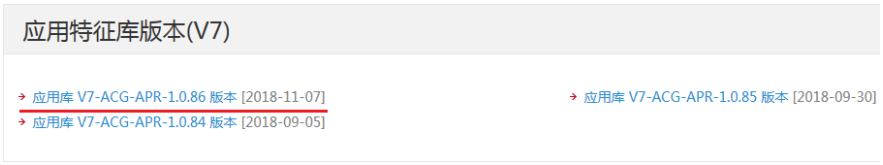
在防火墙界面“系统”>”升级中心”>”特征库升级”中 开启应用识别特征库定时升级功能。

3.2.2 手动升级操作过程

部分设备部署环境可能无法访问互联网，需要使用手动升级更新特征库。

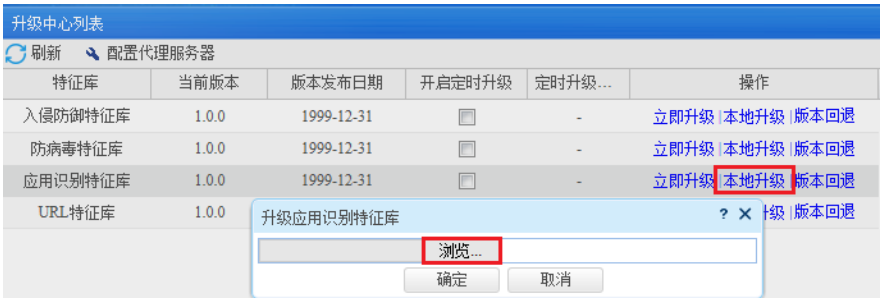
1. 在华三官网下载防火墙最新特征库文件

登录“www.h3c.com” 华三官网，在“产品技术”>“大安全”>”特征库服务专区”中下载应用识别特征库文件。



2. 升级特征库

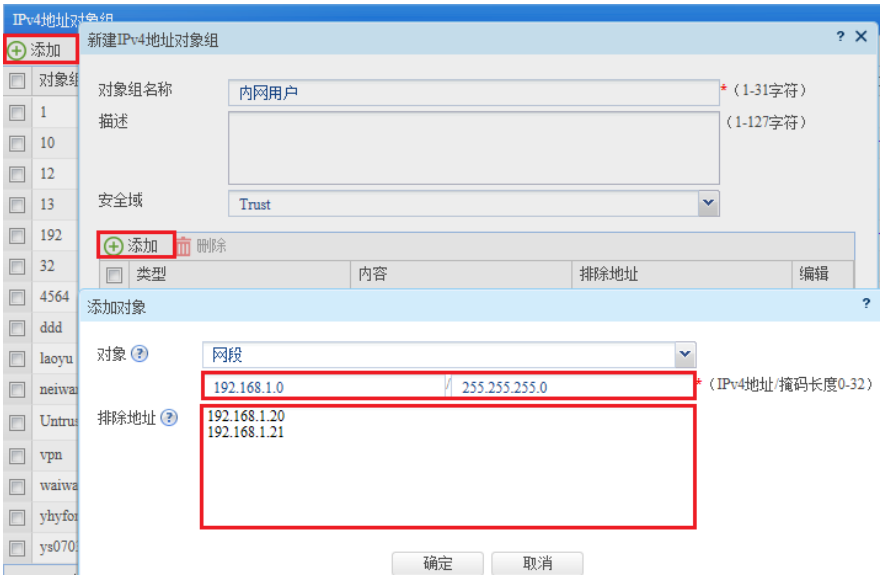
在“浏览”中选择下载好的特征库文件，点击“确定”后完成升级。



3.3 配置应用控制策略

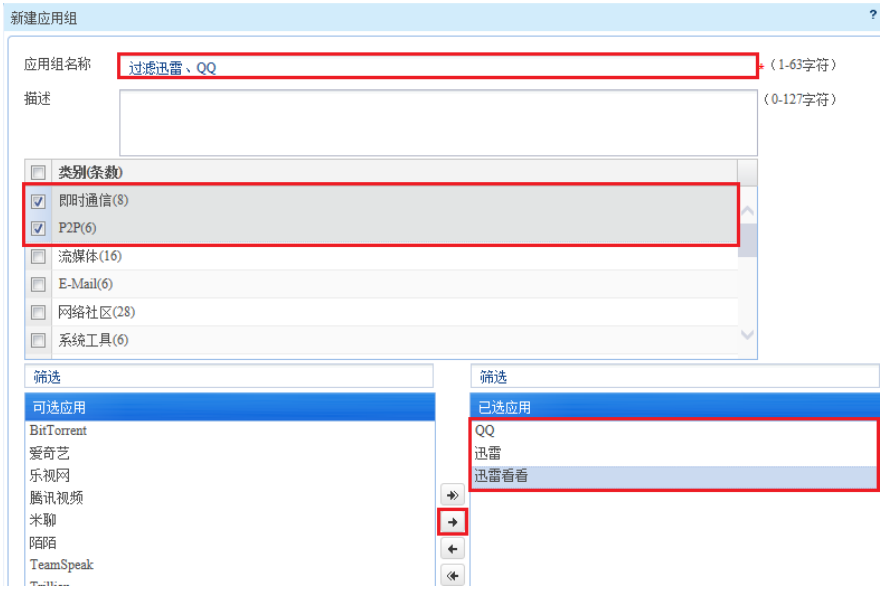
3.3.1 新建IPV4对象组

在防火墙界面“对象”>”对象组”>”IPV4地址对象组”中点击添加名称为“内网用户”的对象组，在网段中添加内网用户网段，因为内网192.168.1.20、192.168.1.21为经理电脑和手机的IP地址并不需要控制，所以将上述两个地址加入排除地址中。



3.3.2 新建应用组

选择“对象”>“应用安全”>“应用识别”>“应用组”>选择新建，应用组名称选择“过滤迅雷、QQ”



点击页面下方确定按钮后跳转到设置好的应用组界面。

3.3.3 在安全策略中调用应用组

选择“策略”>”安全策略”中点击新建，策略名称为“过滤迅雷、QQ”，源安全域选择“Trust”、目的安全域选择“Untrust”，动作选择拒绝，源IP地址选择“内网用户”，应用组将之前配置好的应用组调用。

确认后完成策略配置

配置关键点

3.4 配置注意事项

3.4.1 拒绝策略需要添加在放行策略之前

如果相同源、目的的策略存在两条，第一条为全放通策略，另外一条为拒绝策略则需要将拒绝策略上移至全放通策略之前才能生效。可以通过安全策略中的移动按钮进行移动策略。

3.4.2 只有安全策略中开启日志后才能在应用审计日志中看到对应日志。

如需设备应用审计日志中显示日志信息，需要将安全策略中的日志功能开启。

开启位置：“策略”>”安全策略”编辑策略，在策略内开启记录日志。