

行为管理-准入策略



版权所有：深圳市中科网威科技有限公司

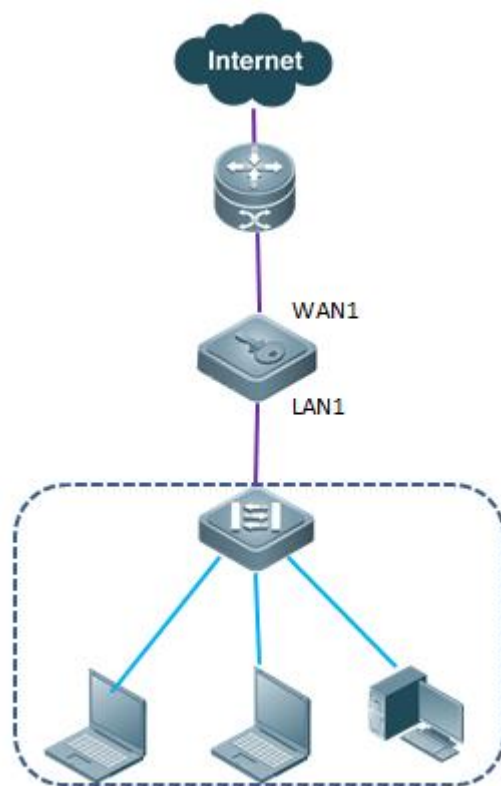
一、组网要求

公司有一台 上网行为 用于控制用户上网行为，对 QQ 做到如下监控：

- (1) 需要强制记录 Windows pc 端 QQ 聊天内容；
- (2) 强制记录 Windows pc 端 QQ 外发文件信息并支持原文件下载，记录接收文件文件名。
- (3) 允许不支持准入的终端（如 Windows xp sp1 及更早的版本、Vista、Linux、Mac、手机终端）直接上网

为了不影响现网拓扑，使用透明模式接入。

二、网络拓扑



三、操作步骤

步骤 1：配置网桥模式

- (1) 工作模式选择为“透明模式”；
- (2) 再根据需要勾选“网桥类型”，并配置网桥接口 IP 地址和网关 IP。注意：未配置为网桥的端口为独立网口，可用于网管和路由。

进入 **系统配置 > 工作模式**，配置网桥参数，如下图：



设备工作模式				确定
工作模式	<input checked="" type="radio"/> 网桥模式 <input type="radio"/> 路由模式 <input type="radio"/> 旁路模式 (改变工作模式，将会清除所有静态路由)			
>>网桥配置<<				
网桥类型	<input checked="" type="checkbox"/> 网桥1 (LAN1<-->WAN1) IP: 172.16.161.118	子网掩码: 255.255.0.0	格式范例: 16 或 255.255.0.0	
	<input type="checkbox"/> 网桥2 (LAN2<-->WAN2) IP:	子网掩码:	格式范例: 16 或 255.255.0.0	
说明: 未配置为网桥的端口为独立网口, 可用于网管和路由				
端口配置	LAN2 IP地址: 10.10.200.1	子网掩码: 255.255.255.0	格式范例: 16 或 255.255.0.0	
	WAN2 IP地址:	子网掩码:	格式范例: 16 或 255.255.0.0	
网关IP	172.16.161.2			

说明：根据实际需要设置网桥接口的 IP 地址和网关 IP，设置好网桥接口的 IP 地址和网关 IP 后，管理员可以连接 上网行为进行设备管理。

步骤 2：配置准入策略-IM 监控规则

上网行为管理策略按从上向下匹配的原则。状态为“启用”的上网策略才会生效。

进入 **行为管理 > 上网策略 > 准入策略**，点击页面右上角的 **新增** 按钮，添加策略。

首先，在“策略配置”选项卡，勾选策略树的“IM 监控规则”，如此才有配置权限，对于不支持运行准入的 PC 或者移动终端-允许上网；接着勾选 IM 聊天内容监控-QQ，以及 IM 发送文件内容监控-QQ，配置栏按下图红色框所示配置，

新增准入策略	
规则名称	准入测试
规则描述	
生效时间:	全天
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
不支持准入的终端策略配置	<input checked="" type="radio"/> 允许上网 <input type="radio"/> 视为检查失败, 禁止上网 (对于不支持运行准入/安全桌面系统的)
策略配置 适用用户组 高级设置	
准入策略	IM监控规则
ROOT <ul style="list-style-type: none"> <input checked="" type="checkbox"/> IM监控规则 <input type="checkbox"/> 操作系统规则 <input type="checkbox"/> 进程规则 <input type="checkbox"/> 文件规则 <input type="checkbox"/> 注册表规则 <input type="checkbox"/> 其他规则 	IM聊天内容监控: <input checked="" type="checkbox"/> QQ <input type="checkbox"/> MSN <input type="checkbox"/> Skype IM发送文件内容监控: <input checked="" type="checkbox"/> QQ <input type="checkbox"/> MSN <input type="checkbox"/> Skype 生效时间: 全天

然后, 在“适用用户组”选项卡配置该策略对应的用户或用户组或 IP 地址。如下图:

新增准入策略	
规则名称	准入
规则描述	
生效时间:	全天
状态	<input checked="" type="radio"/> 启用 <input type="radio"/> 禁用
不支持准入的终端策略配置	<input checked="" type="radio"/> 允许上网 <input type="radio"/> 视为检查失败, 禁止上网 (对于不支持运行准入/安全桌面系统的计算机及移动终端)
策略配置 适用用户组 高级设置	
<input checked="" type="radio"/> 用户及用户组 <input type="radio"/> IP <input type="radio"/> 地址簿	
用户组	选中的用户组
<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Root <input type="checkbox"/> aa <input type="checkbox"/> aaaaaa <input checked="" type="checkbox"/> 准入测试组 <ul style="list-style-type: none"> <input checked="" type="checkbox"/> win2003 <input checked="" type="checkbox"/> win7abc <input checked="" type="checkbox"/> win8 	Root\准入测试组

步骤 3: 安装准入客户端

打开浏览器访问网页如 www.baidu.com, 上网行为会返回准入安装提示:

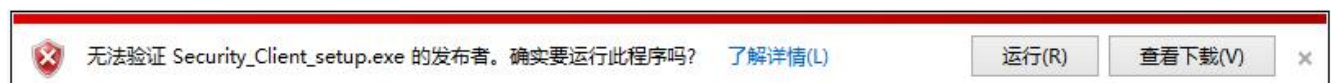


下载安装客户端请点击：确定。

可直接选择运行，或者另存为本地再安装



点击“运行”



下一步：



下一步:



下一步:



安装完成。
即可在在线用户查看客户端的安装情况

设备状态

- 实时监控
 - 设备资源
 - 物理接口
 - 服务监控
 - 用户监控
 - 上网行为
 - 在线用户
 - 防共享上网
 - 当前黑名单
 - 应用限额用户
 - 系统配置
 - 系统对象

在线用户 查询

用户名		所属组	选择
IP地址	172.16.111.186	MAC地址	
时间范围			

强制所有用户下线

总记录数:1 页码:1/1 当前页 1

定制显示项: 累计在线流量 最新速率 活跃会话数 安全客户端

	序号	用户名/用户组	IP地址/MAC地址	物理接口	上线时间	安全客户端	操作
<input type="checkbox"/>	1	172.16.111.186 Root/aa/aa	172.16.111.186 94:de:80:b8:9f:47	LAN1	2015-01-07 15:59:46	1.8.1	趋势图 活跃服务 黑名单 强制下线

总记录数:1 页码:1/1 当前页 1

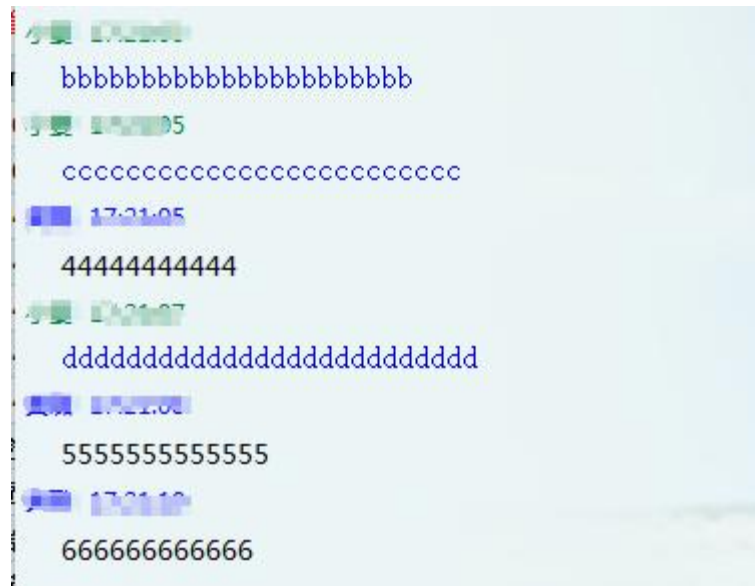
步骤 4：验证效果

验证 1：QQ 聊天，以及外发文件传输查看审计情况

 总机电话-- 0755-83658009
 <http://www.anysec.com>

 技术支持-- 0755-83658229
 深圳市龙华区观澜街道观光路 1301-80 号电子科技大学(深圳)高等研究院 3 号楼 1401

 24 小时技术值班热线----135-1069-3536



登录内置报表中心，查看对应聊天记录

已耗时: 1.041秒 | 主机IP地址: 172.16.111.186-172.16.111.186 | 排除组: 排除组包含子组: 是 | 日期范围: 2015-01-07 - 2015-01-07 | 时间范围: 00:00:00 - 23:59:59 | 动作: 拒绝, 记录 | 应用类型: 所有类型

上网行为查询结果

2 3 4 下一页 > 总记录数为49条!

点击列表 (按<键查看下一条记录, 按>键查看上一条记录, 按<-或->键 向前或后翻页) 自定义显示列

序号	发送帐号	接收帐号	聊天摘要	应用类型	用户名	主机IP	目的IP	所属组	日期与时间
1	小夏 172.16.111.1515...	小夏 172.16.111.529...	qqqqqqqqqqqqqqqqqqqq	QQ (私聊)	172.16.111.186	172.16.111.186	0.0.0.0	Root/aa/aa/	2015-01-07 17:24:03
2	小夏 172.16.111.1515...	小夏 172.16.111.529...	123456798	QQ (私聊)	172.16.111.186	172.16.111.186	0.0.0.0	Root/aa/aa/	2015-01-07 17:23:59
3	小夏 172.16.111.1515...	小夏 172.16.111.529...	777777777	QQ (私聊)	172.16.111.186	172.16.111.186	0.0.0.0	Root/aa/aa/	2015-01-07 17:23:57
4	小夏 172.16.111.1515...	小夏 172.16.111.529...	6666666666666	QQ (私聊)	172.16.111.186	172.16.111.186	0.0.0.0	Root/aa/aa/	2015-01-07 17:23:55
5	小夏 172.16.111.1515...	小夏 172.16.111.529...	5555555555555	QQ (私聊)	172.16.111.186	172.16.111.186	0.0.0.0	Root/aa/aa/	2015-01-07 17:23:53
6	小夏 172.16.111.529...	小夏 172.16.111.1515...	dddddddddddddddddd	QQ (私聊)	172.16.111.186	172.16.111.186	0.0.0.0	Root/aa/aa/	2015-01-07 17:23:52
7	小夏 172.16.111.515...	小夏 172.16.111.529...	44444444444	QQ (私聊)	172.16.111.186	172.16.111.186	0.0.0.0	Root/aa/aa/	2015-01-07 17:23:50
8	小夏 172.16.111.529...	小夏 172.16.111.1515...	cccccccccccccccccc	QQ (私聊)	172.16.111.186	172.16.111.186	0.0.0.0	Root/aa/aa/	2015-01-07 17:23:49
9	小夏 172.16.111.529...	小夏 172.16.111.1515...	bbbbbbbbbbbbbbbbbb	QQ (私聊)	172.16.111.186	172.16.111.186	0.0.0.0	Root/aa/aa/	2015-01-07 17:23:47
10	小夏 172.16.111.529...	小夏 172.16.111.1515...	aaaaaaaaaaaaaaaaaa	QQ (私聊)	172.16.111.186	172.16.111.186	0.0.0.0	Root/aa/aa/	2015-01-07 17:23:46

外发文件审计:





已耗时: 1.072秒 | 主机IP地址: 172.16.111.186-172.16.111.186 | 排除组: 排除组包含子组: 是 | 日期范围: 2015-01-07 - 2015-01-07 | 时间范围: 00:00:00 - 23:59:59 | 动作: 拒绝, 被记录 | 应用类型: IM传文件 | 自定义显示列

上网行为查询结果

点击列表 [快: 键查看下一条记录, 快: 键查看上一条记录], 快 <- 或 -> 键 向前或后翻页

序号	文件名	文件大小	文件发送方式	用户名	组名	日期	动作
1	F:\work\y86资料+手册\配置手册\AD和LDAP导入说明.docx	69.2KB	IM传文件-QQ	172.16.111.186	Root/aa/aa/	2015-01-07 17:39:16	允许
2	C:\Users\Administrator\Desktop\xxxx\IMS_1.8.1_150107.1...	4.3MB	IM传文件-QQ	172.16.111.186	Root/aa/aa/	2015-01-07 17:30:35	允许

详细信息

用户名:	172.16.111.186	时间:	2015-01-07 17:39:16
主机IP地址:	172.16.111.186	文件发送方式:	IM传文件-QQ
上传URL:			

LDAP/AD导入将LDAP/AD服务器上的用户组导入到设备的组织结构上时, 导入入口填上OU=组名 or CN=组名, DC=域名, 以下是二种形式: (a). 将LDAP/AD服务器中的所有组用用户全部导入到组织结构中去: 【dc=abc,dc=com】 (b). 前面两种是将组Users下的用户导入到组织结构中去: 【ou=users,dc=abc,dc=com】、【cn=users,dc=abc,dc=com】; 注: 导入格式按照从小到大的路径, 英文界面输入标点符号。用户查找可以是“匿名查询”(不需要输入用户名和密码)、“本地用户查询”(需要在相关组下用户的用户名和密码); 要查看ad服务器上的DN, 开始-运行, 输入命令 dsquery user即可; LDAP服务器上如果使用ad控制器的相关参数配置, 则需要用本地查询, 具体配置为 (DN:dc=aaa, dc=com; CN:cn:) 查找用户DN: cn=test,cn=users,dc=abc,dc=com; 查找用户密码: P@ssw0rd(单个例子而已)

附件个数(1)

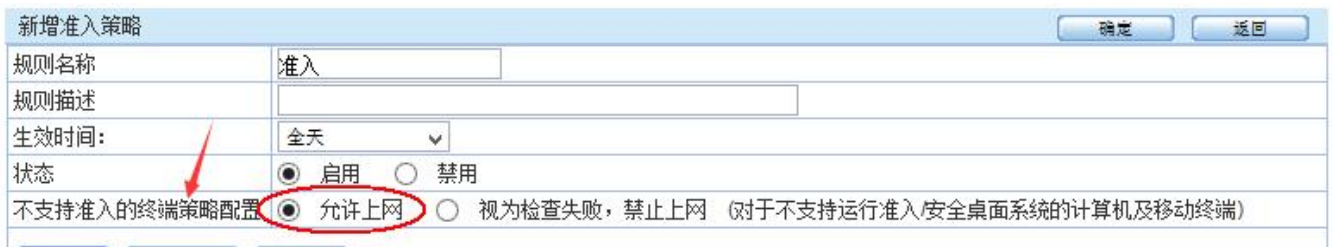
F:\work\y86资料+手册\配置手册\AD和LDAP导入说明.docx

word文档内容预览

该文件可下载到本地查看

验证 2: 对于不支持运行准入的 PC 或者移动终端-允许上网

对应配置:



新增准入策略

规则名称: 准入

规则描述:

生效时间: 全天

状态: 启用 禁用

不支持准入的终端策略配置: 允许上网 视为检查失败, 禁止上网 (对于不支持运行准入/安全桌面系统的计算机及移动终端)

移动一个手机上线的用户到准入组, 验证该手机能否正常上网

序号	名称	上网策略配置	绑定检查	所属组	摘要
1	172.16.166.168 (172.16.166.168)	无	172.16.166.168	Root准入测试组	普通用户 (在线)
2	win8 (win8)	无	172.16.111.186	Root准入测试组	普通用户 (在线)
3	win2003 (win2003)	无	172.16.0.221	Root准入测试组	普通用户 (离线)
4	win7abc (win7abc)	无	172.16.13.22	Root准入测试组	普通用户 (离线)

手机能正常上网:



步骤 5: 保存配置