惠尔顿
WHOLETON
网络防泄密专家

上网行为管理更新总结

日期：2021.3.15

1 URL库自动升级

2 多种的认证方式

3 U盘可信与外拷审计

4 WEB加密审计改进

5 客户端加密审计更新

6 加密客户端邮件审计

7 更多……

1、URL/应用特征库自动更新

1.URL库/应用特征库**免费、自动**更新;

2.升级URL库/应用特征库;

2.1 批量添加修改组织结构

① 在添加用户名时，用“,”将多个用户分割开，可批量新增；修改时，同时选择多个用户，可批量编辑；

② 使用WEB认证时，如能获取到IP/MAC等信息时，则将获取到的结果自动写入到数据库中保存；

③ 多达10+种认证方式：WEB认证，客户端认证，LDAP,AD域，短信认证，IC卡认证，指纹认证，答题认证，UKEY认证，绑定认证（IP，MAC,计算机名）

2.2 实名制指纹身份认证

① 添加指纹认证用户

② 客户端插入指纹采集器

③ 第一次使用直接提示录入指纹

④ 高安全性的指纹认证

⑤ 满足一级保密单位的认证要求

2.3 实名制IC卡身份认证

① 下载硬件身份管理平台

② 管理员集中添加IC认证用户

③ 客户端使用IC登录,IC卡拿开终端锁屏

④ 高安全性的IC卡认证

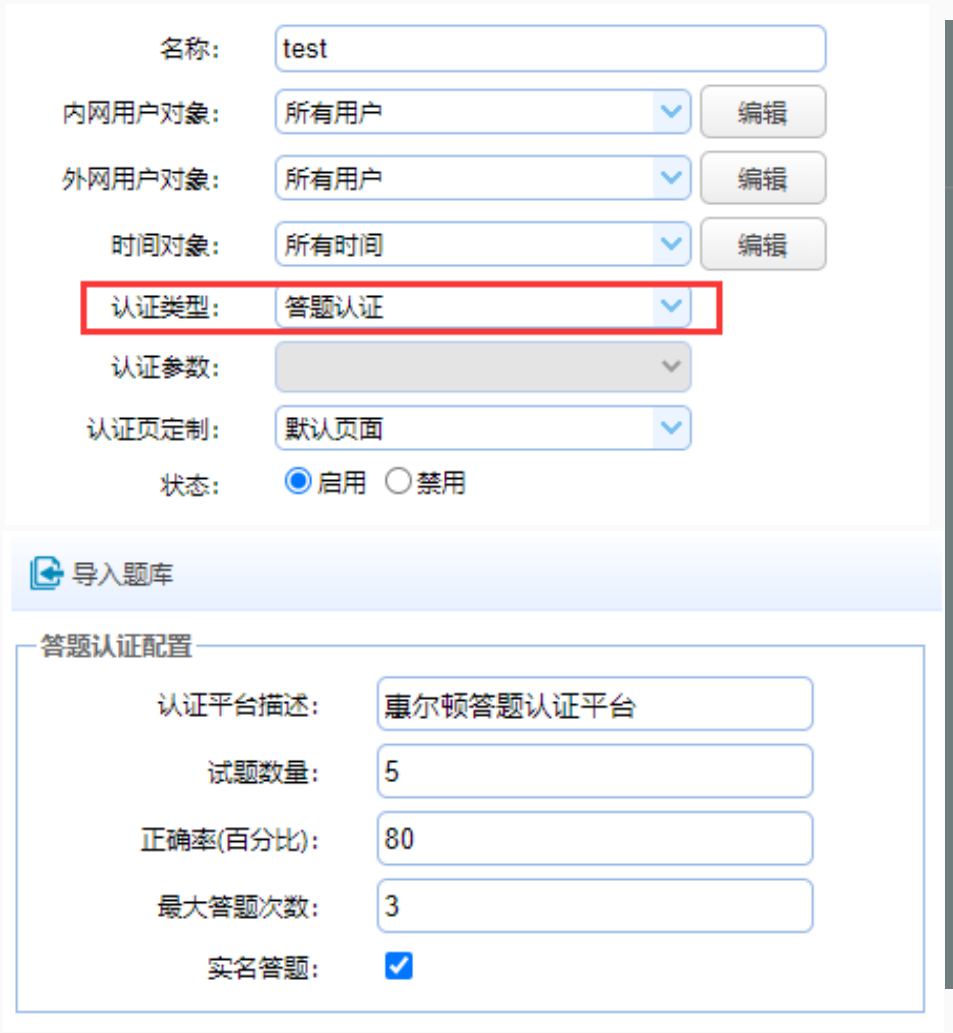
⑤ 满足一级保密单位的认证要求

2.4 答题认证支持实名制

① 内置50+道保密基础试题

② 如需实名制，请勾选“实名答题”

③ 满足用户实名台账要求



2.5 实名制U盘认证

① 客户端使用U盘登录,拔出U盘，客户端退出，禁止上网

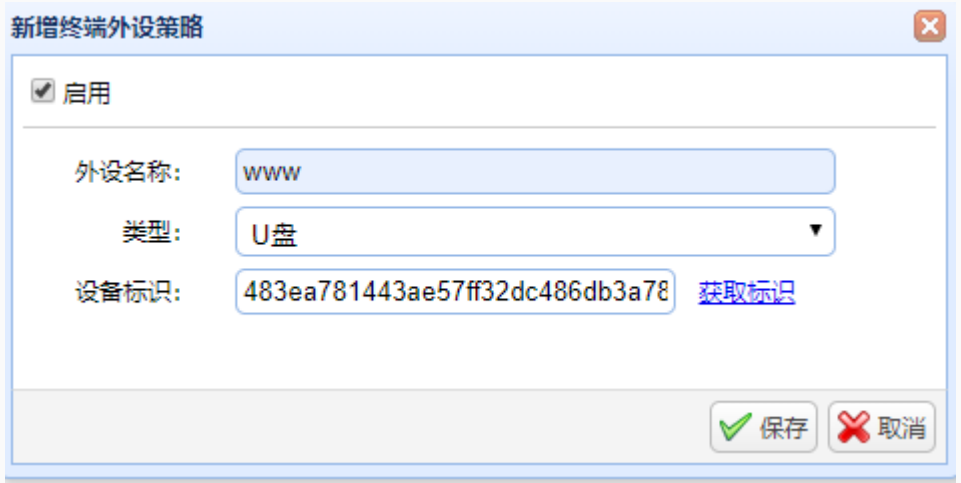
② 高安全性的双因素认证

③ 认证客户端随身携带，即插即用

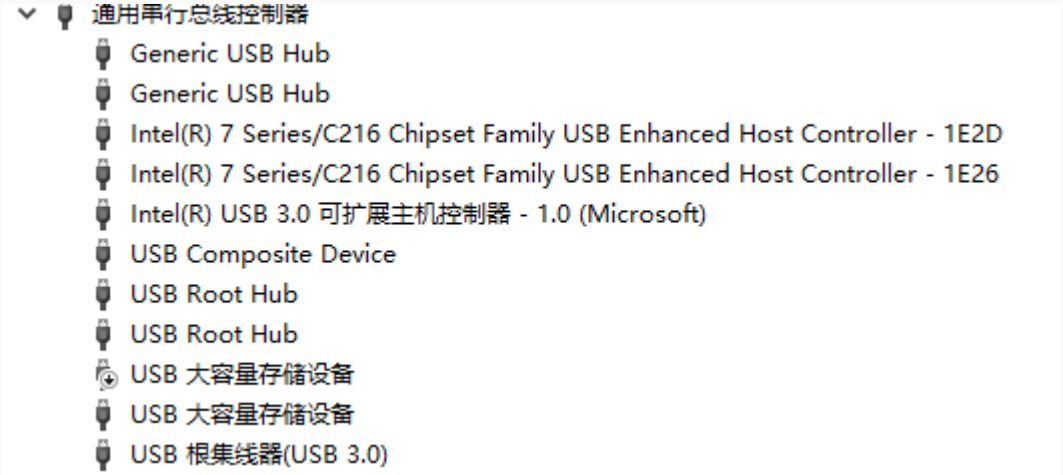
④ 满足一级保密单位的认证要求

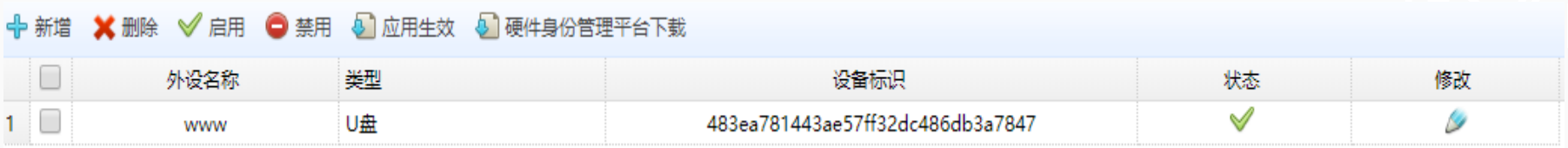
3.1 USB信任/外设白名单

1、添加U盘白名单：
策略管理-》外设管控-》外设白名单-》新增



2、使用认证客户端登录，客户端会调用设备管控功能模块，禁止非授权的U盘





注意：需要先下载硬件身份管理平台并安装，然后才能设置U盘白名单

3.2 信任U盘文件外拷审计

能审计到将本地文件COPY到U盘或者通过远程挂载到本地的网络盘：时间，文件名称，用户

id	datetime	filename	action	name	type	result
1	2020-07-20 15:48:29	I:\FileMonitor.py	Modify	cxz	1	(Null)
2	2020-07-20 15:48:30	I:\aaa.oxps	Modify	cxz	1	(Null)
3	2020-07-20 15:58:55	F:\Wholeton-TritonService	Modify	cxz	1	(Null)
4	2020-07-20 15:58:55	F:\Wholeton-TritonService\CapData.dll	Modify	cxz	1	(Null)
5	2020-07-20 15:58:55	F:\Wholeton-TritonService\del_db.bat	Modify	cxz	1	(Null)
6	2020-07-20 15:58:56	F:\Wholeton-TritonService\Detect.dll	Modify	cxz	1	(Null)
7	2020-07-20 15:58:56	F:\Wholeton-TritonService\devcon.exe	Modify	cxz	1	(Null)
8	2020-07-20 15:58:56	F:\Wholeton-TritonService\devcon_64.exe	Modify	cxz	1	(Null)
9	2020-07-20 15:58:56	F:\Wholeton-TritonService\FT_ND_API.dll	Modify	cxz	1	(Null)
10	2020-07-20 15:59:03	F:\Wholeton-TritonService\install_service.bat	Modify	cxz	1	(Null)
11	2020-07-20 15:59:03	F:\Wholeton-TritonService\mfc100.dll	Modify	cxz	1	(Null)
12	2020-07-20 15:59:11	F:\Wholeton-TritonService\mfc100u.dll	Modify	cxz	1	(Null)
13	2020-07-20 15:59:13	F:\Wholeton-TritonService\msvcp100.dll	Modify	cxz	1	(Null)
14	2020-07-20 15:59:13	F:\Wholeton-TritonService\msvcr100.dll	Modify	cxz	1	(Null)
15	2020-07-20 15:59:14	F:\Wholeton-TritonService\screen.exe	Modify	cxz	1	(Null)
16	2020-07-20 15:59:14	F:\Wholeton-TritonService\ShuttleCsp11_2001.dll	Modify	cxz	1	(Null)
17	2020-07-20 15:59:14	F:\Wholeton-TritonService\takeown.exe	Modify	cxz	1	(Null)
18	2020-07-20 15:59:15	F:\Wholeton-TritonService\Triton.exe	Modify	cxz	1	(Null)
19	2020-07-20 15:59:15	F:\Wholeton-TritonService\TritonConfig.exe	Modify	cxz	1	(Null)
20	2020-07-20 15:59:16	F:\Wholeton-TritonService\TritonService.exe	Modify	cxz	1	(Null)
21	2020-07-20 15:59:16	F:\Wholeton-TritonService\TritonServiced.exe	Modify	cxz	1	(Null)
22	2020-07-20 15:59:17	F:\Wholeton-TritonService\txmsg.dat	Modify	cxz	1	(Null)

注意：安装上网认证客户端 V2.0.0.39~

4.0 SSL管控—设置

开启SSL审计：勾选，保存，开启（默认开启）；

管控用户：此网段内的用户将审计加密的网络行为（IP/网段**不能是子网**）；

排除用户：免监控的用户与此处填写的用户将不受SSL审计程序的监控;

域名白名单：列表中的域名不审计其内容。

4.1 加密网页标题审计

	终端类型	用户名称	地址	URL	标题	语种	网站类型	风险	连接信息
1		192.168.4.66	120.52.183.15	/	Welcome to Kingsoft Web Server!	中文	HTTP		6 src=192.168.4.66 dst=120.52.183.150 sport=55487 dport=80
2		192.168.4.66	110.43.89.14	/	Welcome to Kingsoft Web Server!	中文	HTTP		6 src=192.168.4.66 dst=110.43.89.14 sport=55486 dport=80
3		192.168.4.66	pan.qun.qq.cc	/clt_filetab/groupSha	群文件	中文	聊天室或即时通讯		6 src=192.168.4.66 dst=183.57.48.94 sport=55389 dport=443
4		192.168.4.66	web.qun.qq.c	/announce/index.htm	群公告	中文	聊天室或即时通讯		6 src=192.168.4.66 dst=183.57.48.94 sport=55313 dport=443
5		192.168.4.66	pan.qun.qq.cc	/clt_filetab/groupSha	群文件	中文	聊天室或即时通讯		6 src=192.168.4.66 dst=183.57.48.94 sport=55257 dport=443
6		192.168.4.66	120.52.183.15	/	Welcome to Kingsoft Web Server!	中文	HTTP		6 src=192.168.4.66 dst=120.52.183.150 sport=55242 dport=80
7		192.168.4.66	110.43.89.14	/	Welcome to Kingsoft Web Server!	中文	HTTP		6 src=192.168.4.66 dst=110.43.89.14 sport=55241 dport=80
8		192.168.4.66	www.sogou.c	/web?query=%E7%BI	绝密 - 搜狗搜索	中文	搜索引擎		6 src=192.168.4.66 dst=183.36.114.45 sport=55169 dport=443
9		192.168.4.66	www.sogou.c	/	搜狗搜索引擎 - 上网从搜狗开始	中文	搜索引擎		6 src=192.168.4.66 dst=183.36.114.45 sport=55169 dport=443
10		192.168.4.66	www.baidu.cc	/	百度一下，你就知道	中文	搜索引擎		6 src=192.168.4.66 dst=14.215.177.38 sport=55152 dport=443

4.2 加密搜索引擎审计

	终端类型	用户名称	MAC地址	策略名称	访问动作	关键字	网址	连接信息
1		192.168.4.66		-	审计记录	中间人攻击的图片	www.baidu.com	6 src=192.168.4.66 dst=14.215.177.39 sport=55723 dport=443
2		192.168.4.66		-	审计记录	缁勬挱鏃板潪	www.sogou.com	6 src=192.168.4.66 dst=183.36.114.44 sport=55658 dport=443
3		192.168.4.66		all	放行 警戒级	绝密	www.sogou.com	6 src=192.168.4.66 dst=183.36.114.45 sport=55169 dport=443
4		192.168.4.66		-	审计记录	linux grep 正则表达式	www.baidu.com	6 src=192.168.4.66 dst=14.215.177.39 sport=57881 dport=443
5		192.168.4.66		-	审计记录	linux grep 正则表达式	www.baidu.com	6 src=192.168.4.66 dst=14.215.177.39 sport=57881 dport=443
6		192.168.4.66		-	审计记录	linuxgrepawk	www.baidu.com	6 src=192.168.4.66 dst=14.215.177.39 sport=57881 dport=443
7		192.168.4.66		-	审计记录	linuxgrep-d	www.baidu.com	6 src=192.168.4.66 dst=14.215.177.39 sport=57881 dport=443
8		192.168.4.66		-	审计记录	linux grep 正则表达式	www.baidu.com	6 src=192.168.4.66 dst=14.215.177.39 sport=57881 dport=443
9		192.168.4.66		-	审计记录	linuxgrep命令	www.baidu.com	6 src=192.168.4.66 dst=14.215.177.39 sport=57880 dport=443
10		192.168.4.66		-	审计记录	linux grep 不包含	www.baidu.com	6 src=192.168.4.66 dst=14.215.177.39 sport=57881 dport=443

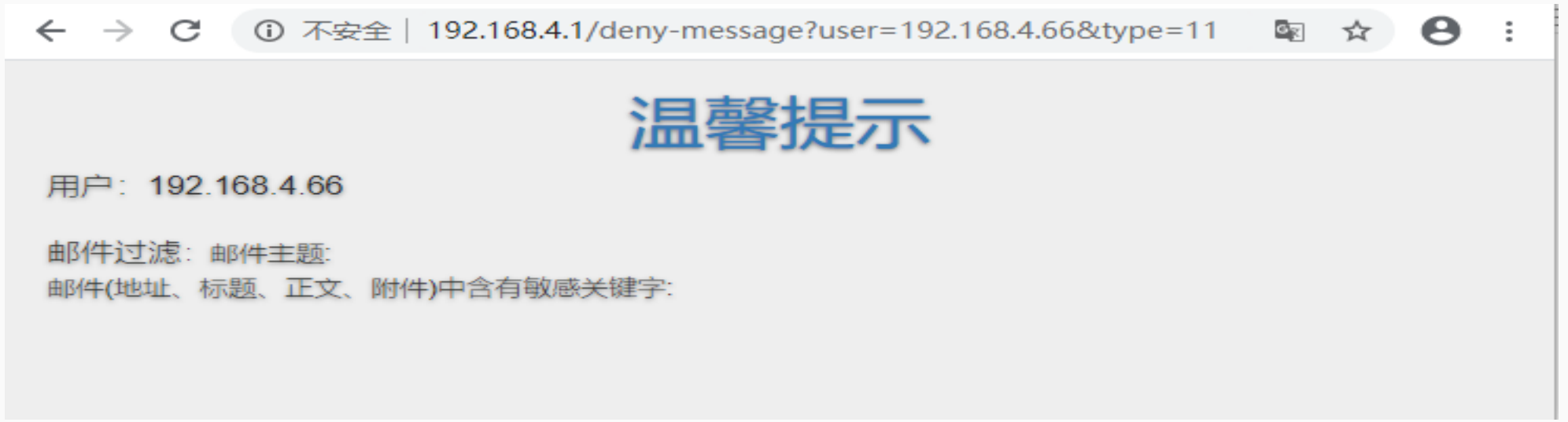
4.3 加密URL访问审计

	终端类	用户名称	MAC地址	策略名称	告警级别	域名	URL	语种	大小
121		192.168.4.66	00:E2:69:0B:0D:5F	-	审计记录	uq.file.cloud.duba.net	/upload_query?135336015	中文	720 B
122		192.168.4.66	00:E2:69:0B:0D:5F	-	审计记录	110.43.89.12	/	中文	441 B
123		192.168.4.66	00:E2:69:0B:0D:5F	-	审计记录	kns.duba.net	/kns-query?135335859	中文	524 B
124		192.168.4.66		-	审计记录	newvip.duba.net	/api/v2/user/userInfo	中文	1.76 KB
125		192.168.4.66		-	审计记录	newvip.duba.net	/api/v2/user/userInfo	中文	1.76 KB
126		192.168.4.66	00:E2:69:0B:0D:5F	-	审计记录	duba-defend.zhhainiao.com	/cloudscreenshot.dat	中文	457 B
127		192.168.4.66	00:E2:69:0B:0D:5F	-	审计记录	duba-defend.zhhainiao.com	/cloudscreenshot.dat	中文	457 B
128		192.168.4.66	00:E2:69:0B:0D:5F	-	审计记录	infoc2.duba.net	/c/	中文	637 B
129		192.168.4.66	00:E2:69:0B:0D:5F	-	审计记录	duba-defend.zhhainiao.com	/cloudpriority.dat	中文	455 B
130		192.168.4.66	00:E2:69:0B:0D:5F	-	审计记录	infoc2.duba.net	/c/	中文	664 B

4.4 加密WEB邮件审计

所有终端 | 2021-03-01 00:00:00 | 2021-03-18 23:59:59 | =192.168.4.66

	用户名称	策略名称	邮件类型	发送	主题	大小	风险级别	动作
1	192.168.4.66	all	WEB发件	315711885@qq.com	工作计划请查收	0 B	警戒级	放行
2	192.168.4.66	all	WEB发件	315711885@qq.com	工作计划请查收	0 B	警戒级	放行
3	192.168.4.66	all	WEB发件	315711885@qq.com	TEST for Wholeton	0 B	警戒级	放行
4	192.168.4.66	all	WEB发件	315711885@qq.com	TEST for Wholeton	0 B	警戒级	放行



4.5 加密社交发帖审计

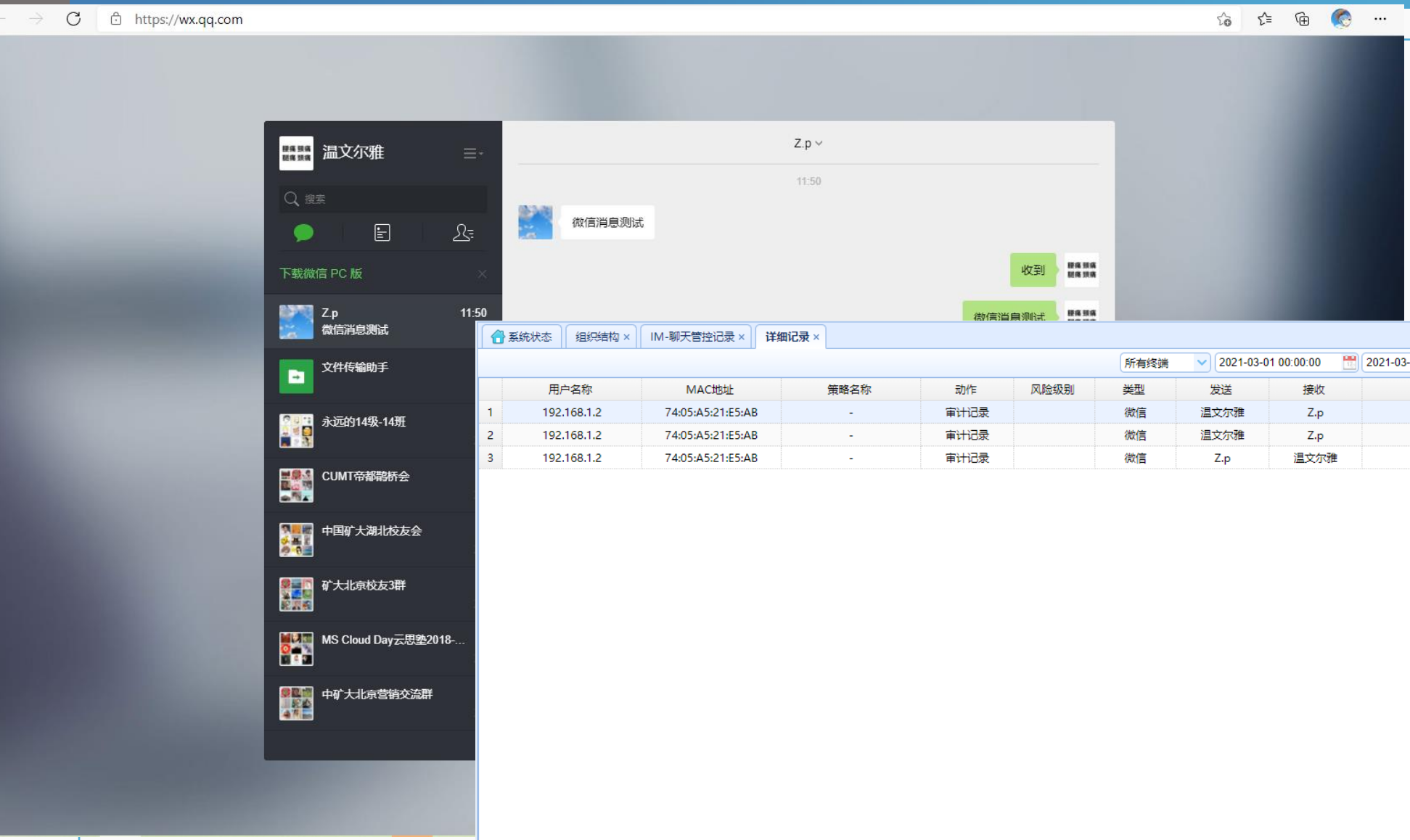
	终端类型	用户名称	用户账号	MAC地址	策略名称	服务	网址	类型	标题
1		192.168.4.66			-	百度贴吧		发贴	passat新能源车怎样

完整内容

查看社交发帖原始排版

用户组/用户名/IP地址	192.168.4.66 / 192.168.4.66
MAC地址	
连接信息	6 src=192.168.4.66 dst=14.215.177.221 sport=58139 dport=443
终端类型	电脑
服务	百度贴吧
网址	
类型	发贴
标题	passat新能源车怎样?
内容	有没有评价
时间	2021-03-18 09:31:41

4.6 微信web版聊天审计



系统状态 | 组织结构 × | IM-聊天管控记录 × | 详细记录 ×

所有终端 | 2021-03-01 00:00:00 | 2021-03-18 23:59:59 | =192.168.1.2 | 软件类型 | 关键字

	用户名称	MAC地址	策略名称	动作	风险级别	类型	发送	接收	内容	时间	操作
1	192.168.1.2	74:05:A5:21:E5:AB	-	审计记录		微信	温文尔雅	Z.p	微信消息测试	2021-03-18 11:33:46	更多
2	192.168.1.2	74:05:A5:21:E5:AB	-	审计记录		微信	温文尔雅	Z.p	收到	2021-03-18 11:33:41	更多
3	192.168.1.2	74:05:A5:21:E5:AB	-	审计记录		微信	Z.p	温文尔雅	微信消息测试	2021-03-18 11:33:33	更多

4.7 web加密审计内容总结

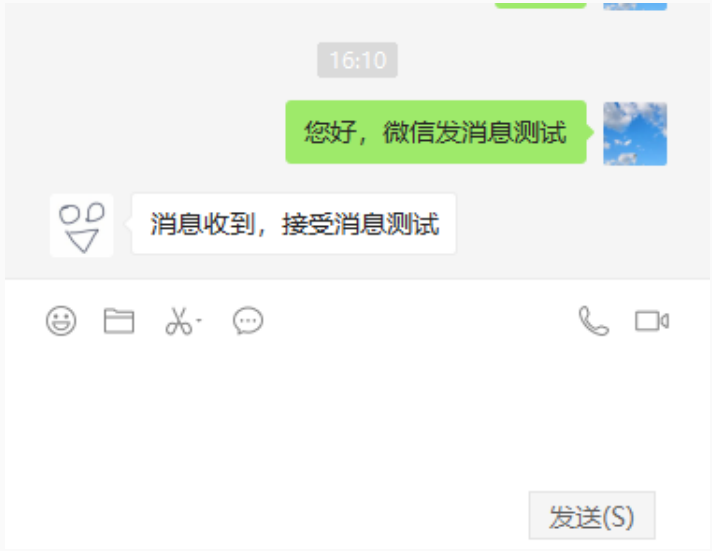
- 网页标题审计
- 搜索引擎审计
- URL访问审计
- 加密邮件审计
- 社交发帖审计
- 微信聊天审计

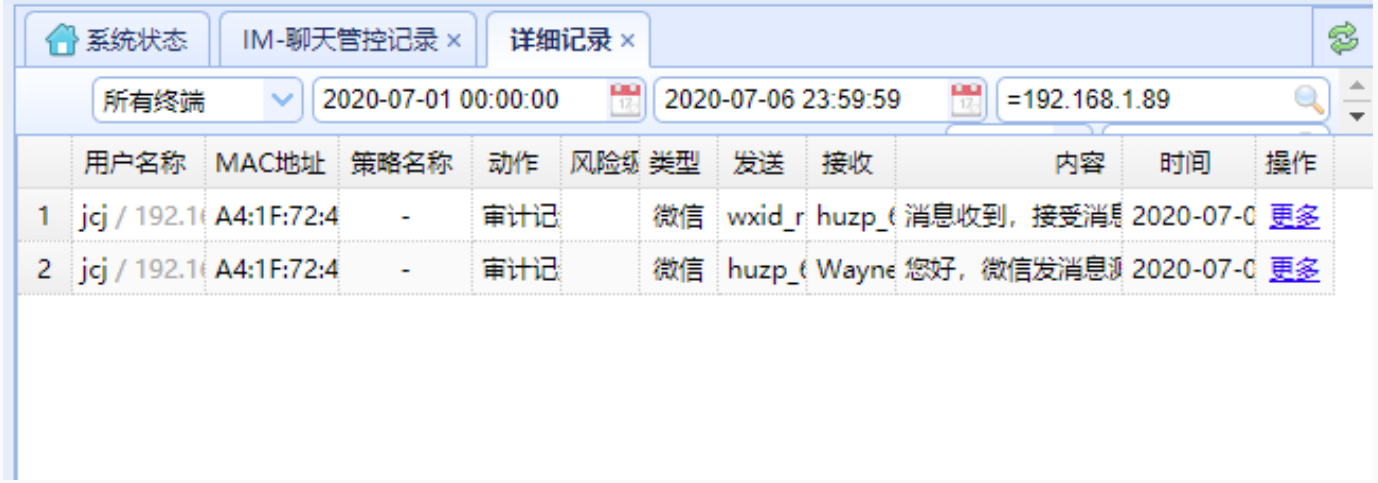
5.1 微信PC端聊天记录审计

① 登录微信PC客户端

② 发送消息，接收消息

③ 进入设备管理界面，查看记录





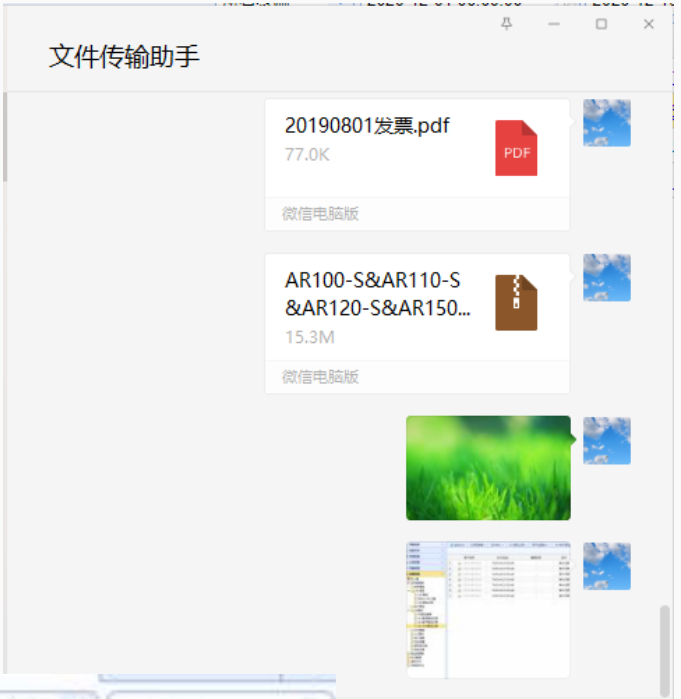
紧跟版本更新：

支持至目前最新PC端微信版本！

5.2 微信PC版文件图片发送审计

- ✓ 在微信PC版本上分别发送小于10M文件、大于10M文件、图片、截图，如右图所示
- ✓ 进入设备管理界面：

  策略管理/应用层策略/IM管控/IM文件管控记录
- ✓ 可看到刚才发送文件的四条记录



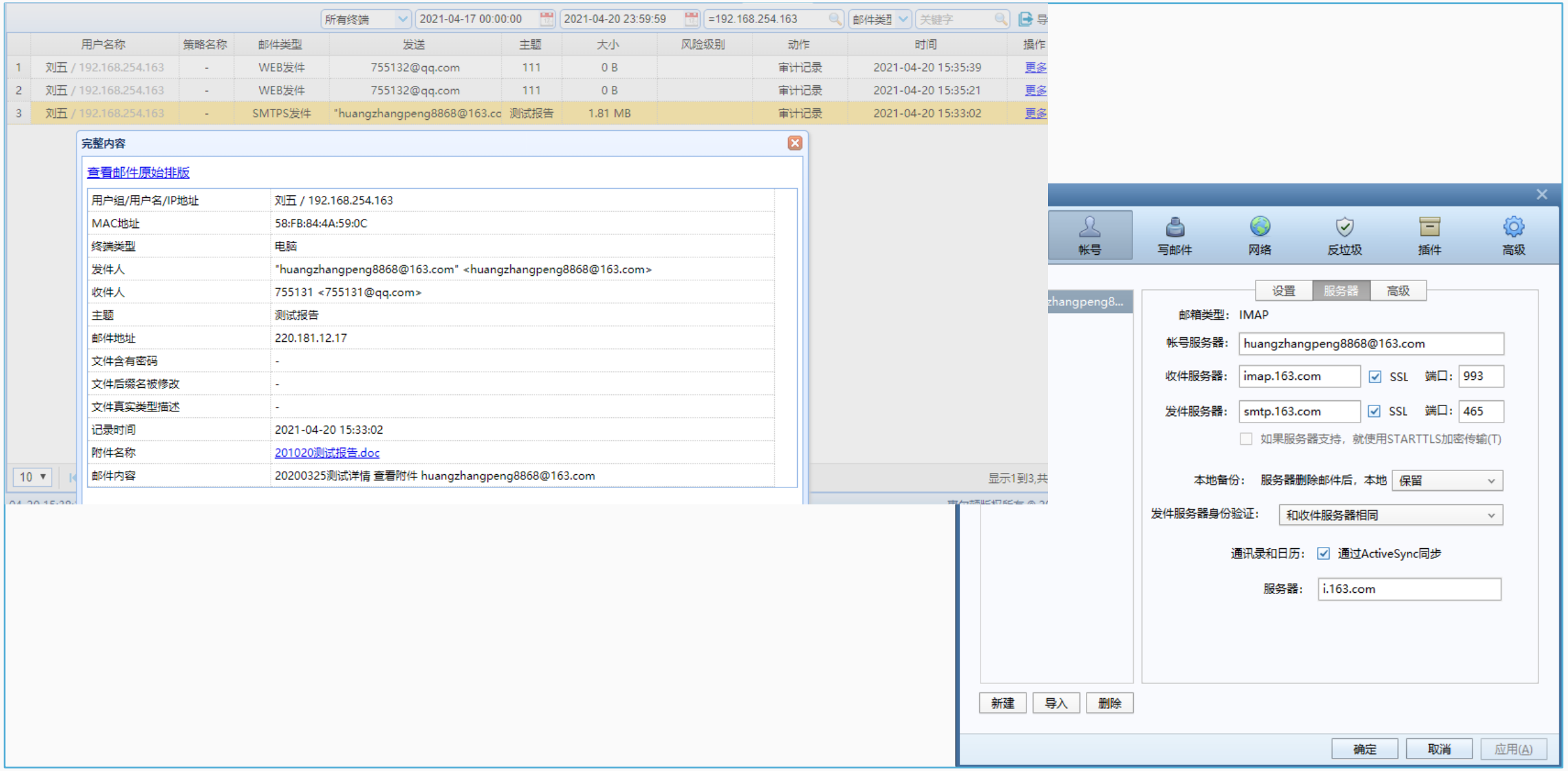
所有终端 | 2020-12-01 00:00:00 | 2020-12-16 23:59:59 | =192.168.0.254 | 软件类型 | 关键字

	用户名称	MAC地址	策略名称	动作	风险级别	类型	发送	接收	文件名	大小	开始时间	结束时间
1	cz / 192.168.(	74:05:A5:21:E	-	审计记录		微信	huzp_666	filehelper	1608103078(1).png	48.52 KB	2020-12-16 1	2020-12-1
2	cz / 192.168.(	74:05:A5:21:E	-	审计记录		微信	huzp_666	filehelper	1608103065.jpg	194.46 K	2020-12-16 1	2020-12-1
3	cz / 192.168.(	74:05:A5:21:E	-	审计记录		微信	huzp_666	filehelper	AR100-S&AR110-S&A	15.28 M	2020-12-16 1	2020-12-1
4	cz / 192.168.(	74:05:A5:21:E	-	审计记录		微信	huzp_666	filehelper	20190801发票.pdf	76.95 KB	2020-12-16 1	2020-12-1

5.3 QQ聊天记录审计

	用户名称	MAC地址	策略名称	动作	风险级别	类型	发送	接收	内容	时间	操作
1	刘五 / 192.168.254.163	58:FB:84:4A:59:0C	IM防泄密	审计记录		QQ	0	胡忠平	这个吗	2021-04-20 15:41:07	更多
2	刘五 / 192.168.254.163	58:FB:84:4A:59:0C	IM防泄密	审计记录		QQ	0	胡忠平	$2y$10$.TtR3um7KLlvm0YMez331O8wySiLzq8JLQO3WJvqdWZZYSYJRrz	2021-04-20 15:40:41	更多
3	刘五 / 192.168.254.163	58:FB:84:4A:59:0C	IM防泄密	审计记录		QQ	0	胡忠平	图片	2021-04-20 15:40:33	更多
4	刘五 / 192.168.254.163	58:FB:84:4A:59:0C	IM防泄密	审计记录		QQ	0	何永争	1.深圳鑫迪问题 2.山西运城浪潮问题 3.海洋学院升级问题	2021-04-20 15:40:25	更多
5	刘五 / 192.168.254.163	58:FB:84:4A:59:0C	IM防泄密	审计记录		QQ	0	何永争	成功接收离线文件“VPNServer.rar”	2021-04-20 15:40:15	更多

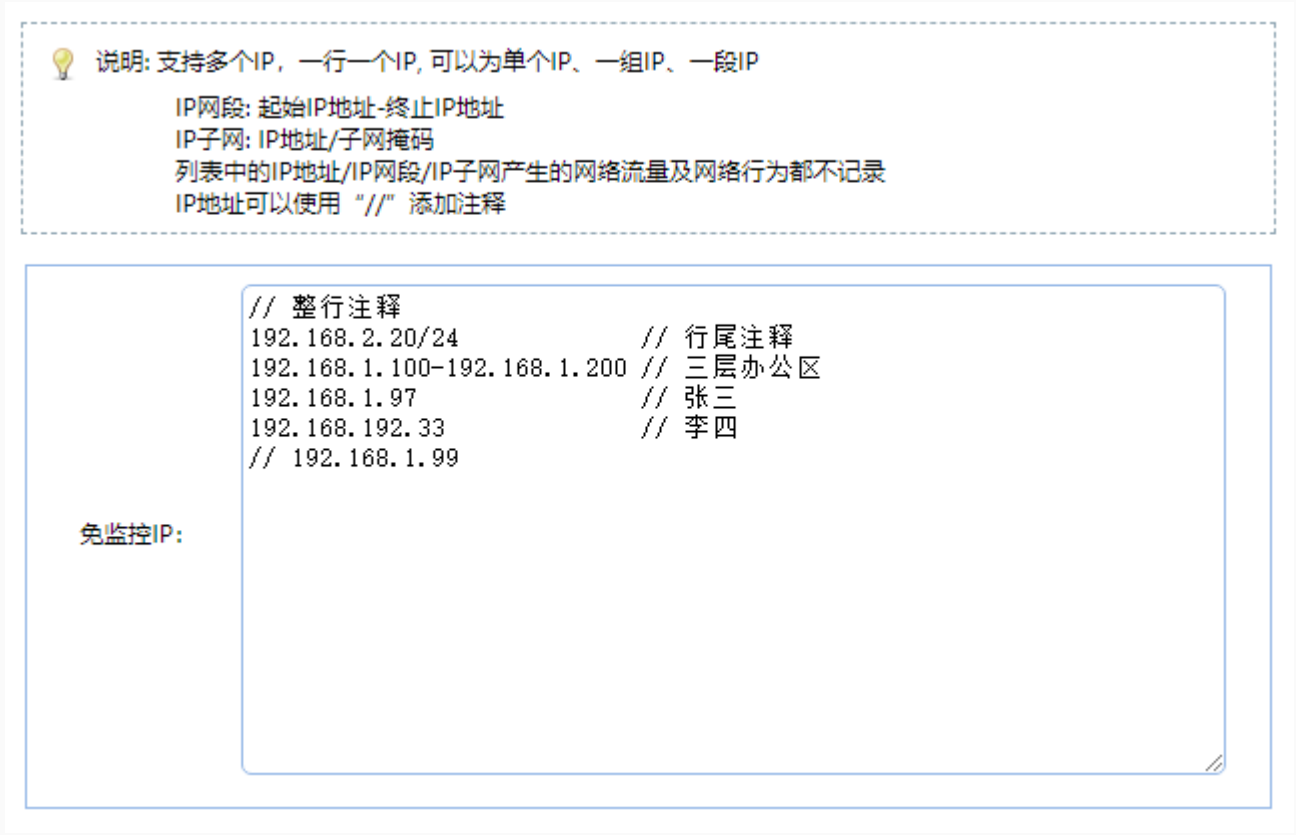
6 SMTPS邮件发送的审计



7.1 免监控[增加注释]

① 允许对免监控中的IP进行注释，如图，您可以整行注释，也可以行尾注释，甚至也可以注释IP，如此以来，虽然该IP还在，但却不受免监控影响了

② IP较多时，可以方便识别出某IP指向哪里



7.2 链路聚合桥模式

网络环境描述:

1、原网络S5700 23/24做链路聚合

2、W1000NM 5、6口做链路聚合上联

3、4口做链路聚合下联

3、W1000NM能正常审计并管控网络行为

在NAT/路由、桥/多桥、旁路模式的基础上，增加了链路聚合桥模式，适用于更大型复杂的组网。

7.3 每年四次升级

① 315版本

② 619版本

③ 国庆版

④ 元旦版

⑤ 现阶段的主版本为 V10.0

惠尔顿
WHOLETON
网络防泄密专家

欢迎指导