



中新金盾抗拒绝服务系统 攻击监控软件

版本号：201102A

中新金盾抗拒绝服务系统攻击监控软件使用说明

版本 V1.1.0.1

为便于客户管理多台以及集群防火墙，我们为您提供金盾抗拒绝服务系统管理器。可针对金盾抗拒绝服务系统进行实时监控，根据流量和连接设置报警参数。

一、软件下载：

下载地址：<http://setup.zxfirewall.com:8022/jdfwmon.rar>

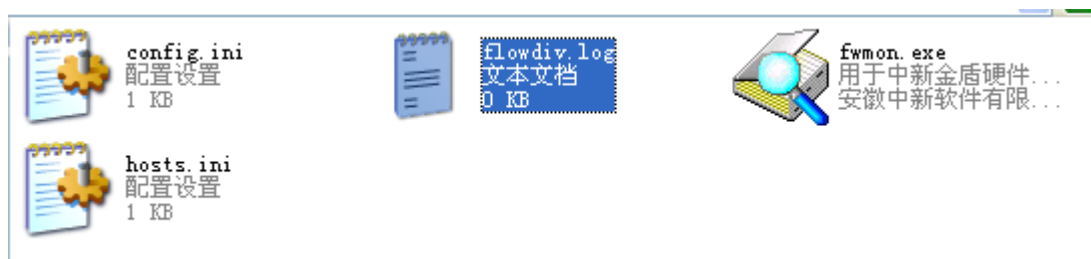
文件名称：中新金盾抗拒绝服务系统管理器

下载 jdfwmon.rar 后解压缩到 jdfwmon. 目录，可看到 config.ini fwmon.exe hosts.ini 四个文件 config.ini 为配置文件（请不要修改） fwmon.exe 为控制器主文件 hosts.ini 为单一 IP 监控报警配置文件



jdfwmon 文件

注：在使用过软件的流量牵引功能后，会自动在目录下生成一个日志文件 flowdiv.log



二、使用说明：

运行 fwmon.exe 文件，界面如图一：



(图一)

1、攻击监控界面：



(图二)

1.1 设备管理

设备地址:

通过此项设置防火墙管理地址，设置格式为：*. *.*.*.*: 28099 (*. *.*.*.*表示外网管理 IP 地址)

用户名:

输入防火墙管理用户名

密码:

输入防火墙管理控制密码

设置:

输入防火墙管理地址、用户名和密码后，点击“设置”即可添加受监控防火墙

删除:

选中受监控防火墙后点击“删除”可取消该台防火墙的监控

1.2 流量记录

设备信息:

显示管理地址、用户、状态

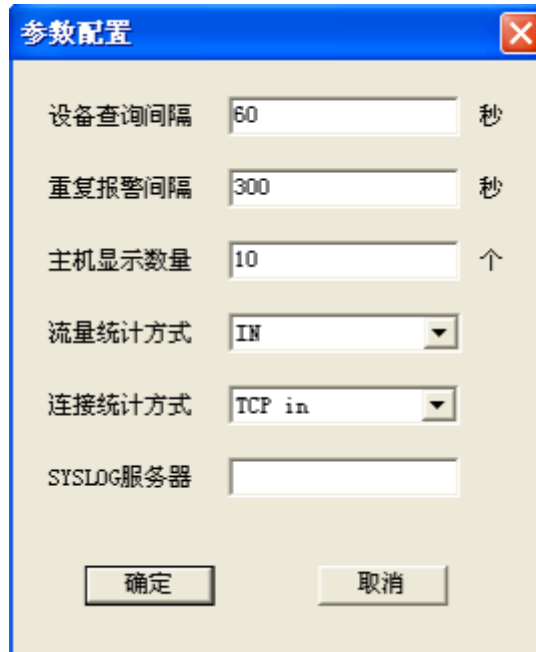
当前状态:

显示流量、连接

详细统计:

显示攻击频率

2、 参数设置：



(图三)

设备查询间隔：

默认值 60 秒，即监控器对于设备进行查询的间隔时间为 60 秒查询一次，可根据客户需要调整数值

重复报警间隔：

默认值 300 秒，即当首次报警后如仍符合报警条件会在 300 秒后进行二次报警，可根据客户需要调整数值

主机显示数量：

默认值 10 个，即在主机列表中显示最大流量的前 10 台主机状态，可根据客户需要调整数值

流量统计方式：

表示进行流量报警设置时可选择 IN、OUT 或 IN+OUT 形式进行流量计算

连接统计方式：

表示进行连接报警设置时可选择 TCP in、TCP out、TCP（TCP 总连接）、UDP（总连接）、及 TCP+UDP 形式进行连接计算

SYSLOG 服务器：

设置 SYSLOG 服务器报警方式，通过添加 SYSLOG 服务器地址，便于客户对日志信息进行管理

3、 告警设置：

告警方式设置
✕

报警条件

总流量报警	<input type="text"/>	Mbps	忽略 ▼
总连接报警	<input type="text"/>	个	忽略 ▼
单墙流量报警	<input type="text"/>	Mbps	忽略 ▼
单墙连接报警	<input type="text"/>	个	忽略 ▼
主机流量报警	<input type="text"/>	Mbps	忽略 ▼
主机连接报警	<input type="text"/>	个	忽略 ▼

攻击频率

SYN频率报警	<input type="text"/>	PPS	忽略 ▼
ACK频率报警	<input type="text"/>	PPS	忽略 ▼
UDP频率报警	<input type="text"/>	PPS	忽略 ▼
ICMP频率报警	<input type="text"/>	PPS	忽略 ▼
Frag频率报警	<input type="text"/>	PPS	忽略 ▼
New-TCP频率报警	<input type="text"/>	个	忽略 ▼
New-UDP频率报警	<input type="text"/>	个	忽略 ▼

铃声设定

邮件设定

短信设定

确定

取消

(图四)

3.1 报警条件

总流量报警:

指受监控防火墙的流量和，即所有受监控防火墙的流量（in 流量和 out 流量和）达到此设置数值时，开始报警，单位为 MBPS。该项如果不进行设置，则关闭此项，即视为不进行总流量监控。

总连接报警:

指受监控防火墙的连接和，即所有受监控防火墙的连接（in 连接和 out 连接和）达到此设置数值时，开始报警，单位为个。该项如果不进行设置，则关闭此项，即视为不进行总连接监控。

单墙流量报警:

指单台防火墙的流量，即受监控防火墙中有一台流量（in 流量和 out 流量和）达到此设置数值时，开始报警，单位为 MBPS。该项如果不进行设置，则关闭此项，即视为不进行单墙流量监控报警，但会记录到日志。

单墙连接报警:

指单台防火墙的连接，即受监控防火墙中有一台连接（in 连接和 out 连接和）达到此设置数值时，开始报警，单位为个。该项如果不进行设置，则关闭此项，即视为不进行单墙连接监控。

主机流量报警：

指单一主机单墙流量，即受监控防火墙某一主机单墙流量（in 流量和 out 流量和）达到此设置数值时，开始报警，单位为 MBPS。该项如果不进行设置，则关闭此项，即视为不进行单一主机单墙流量监控。

主机连接报警：

指单一主机的连接，即受监控防火墙某一主机连接数（in 连接和 out 连接和）达到此设置数值时，开始报警，单位为个。该项如果不进行设置，则关闭此项，即视为不进行单一主机连接监控。

3.2 攻击频率

SYN 频率报警：

指当受监控防火墙上，每秒的 SYN 攻击包总数达到设定阈值时开始报警，单位为 pps（包每秒）。该项如果不进行设置，则关闭此项，即视为不进行 SYN 攻击频率监控报警

ACK 频率报警：

指当受监控防火墙上，每秒的 ACK 攻击包总数达到设定阈值时开始报警，单位为 pps（包每秒）。该项如果不进行设置，则关闭此项，即视为不进行 ACK 攻击频率监控报警

UDP 频率报警：

指当受监控防火墙上，每秒的 UDP 攻击包总数达到设定阈值时开始报警，单位为 pps（包每秒）。该项如果不进行设置，则关闭此项，即视为不进行 UDP 攻击频率监控报警

ICMP 频率报警：

指当受监控防火墙上，每秒的 ICMP 攻击包总数达到设定阈值时开始报警，单位为 pps（包每秒）。该项如果不进行设置，则关闭此项，即视为不进行 ICMP 攻击频率监控报警

Frag 频率报警：

指当受监控防火墙上，每秒的 Frag 分片攻击包总数达到设定阈值时开始报警，单位为 pps（包每秒）。该项如果不进行设置，则关闭此项，即视为不进行 Frag 分片攻击频率监控报警

New-TCP 频率报警：

指当受监控防火墙上，每秒新建立的 TCP 连接总数达到设定阈值时开始报警，单位为个。该项如果不进行设置，则关闭此项，即视为不进行 TCP 新连接频率监控报警

New-UDP 频率报警：

指当受监控防火墙上，每秒新建立的 UDP 连接总数达到设定阈值时开始报警，单位为个。该项如果不进行设置，则关闭此项，即视为不进行 UDP 新连接频率监控报警

注：Udp 是无连接的，此处的 UDP 连接是指，有一次交互传输的过程

3.3 报警方式



(图五)

忽略:

表示不进行告警条件设置，但会记录到日志

窗口闪动:

设定后会进行窗口闪动提示

铃声告警:

设定后会进行铃声报警提示（设定铃声必须为：wav 格式）

邮件通知:

设定后会发送邮件进行提示

短信提醒:

设定后可进行短信报警提示

3.4 报警方式详细参数配置

铃声设定:

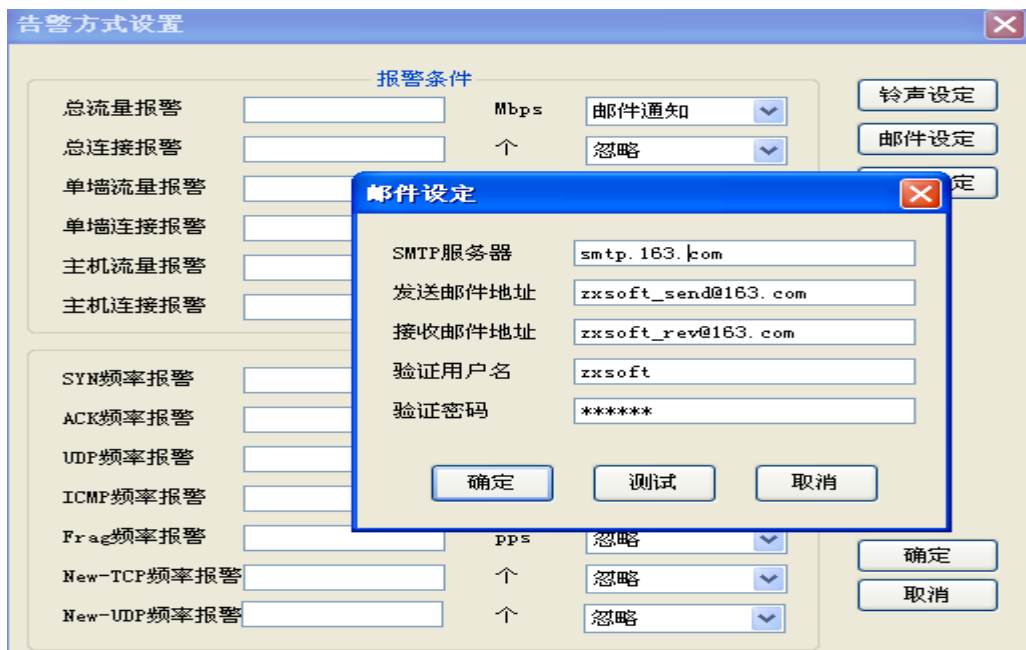
通过浏览已存 wav 文件路径，进行设定，如图六:



(图六)

邮件设定:

通过设置 SMTP 服务器、发送邮件地址、接收邮件地址、验证用户名、验证密码进行确定，实现邮件告警功能，如图七：



(图七)

注：不支持安全套接字的邮件

短信设定：

邮箱如果设置短信提醒，则 mail 报警即可实现短信报警功能

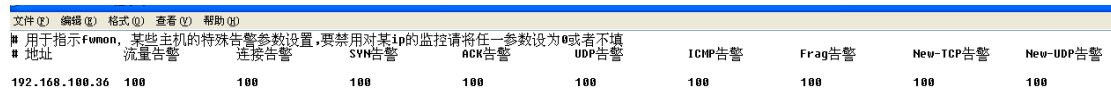
3.5 设定单一主机的监控报警

前面所介绍的报警方式都是以墙上信息为监控单位，没有针对单一主机的监控设置。如需要针对具体的单一主机进行设置，则进行如下操作

1) 找到软件根目录下的 hosts.ini 文件



2) 打开 hosts.ini 文件



(图八)

3) 依据图八中所示格式增加需要监控的单一主机

4、流量牵引

4.1 作用

本软件的流量牵引功能通过从金盾防火墙所收集到的流量信息进行判断，当流量超过牵引触发值时，软件会自行发起一个 telnet 到事先指定的网络设备中（该设备是要有决定流量走向能力的），并将预先定义的一个命令集中的所有操作命令在设备中执行。以改变特定主机的流量。（如写入一条静态路由之类的方式）。

4.2 使用说明

点击流量牵引弹出如下对话框



(图九)

4.2.1 触发参数:

索引流量触发:

设置该值后，当某主机流量超过该值

持续次数:

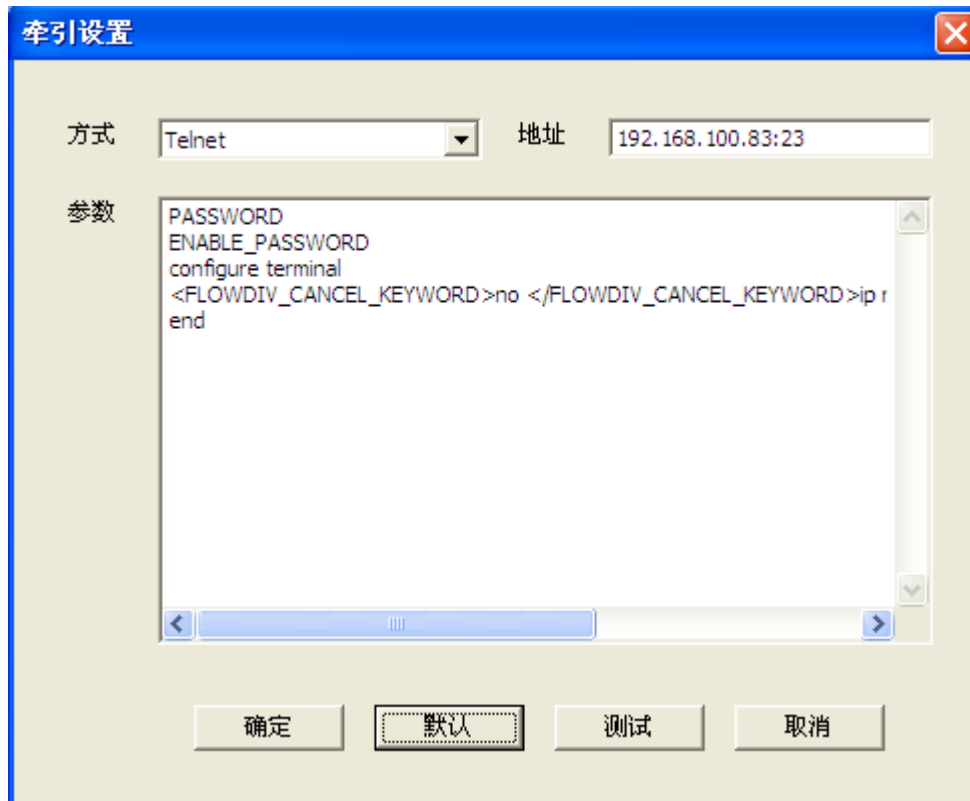
超过流量触发值指定次数就会启用牵引

4.2.2 已牵引列表:

显示已牵引的地址和时间。

4.2.3 牵引配置

点击牵引配置弹出如下对话框



(图十)

方式:

HTTP 为其它功能使用，流量牵引仅使用 Telnet 模式

地址:

需要执行命令集的网络设备的 IP 地址和登录端口，格式如图

(华为、csico 等厂商的设备都可以，但对应的命令参考相应厂商的命令)

参数:

此处就是建立命令集

以 Cisco 设备为例

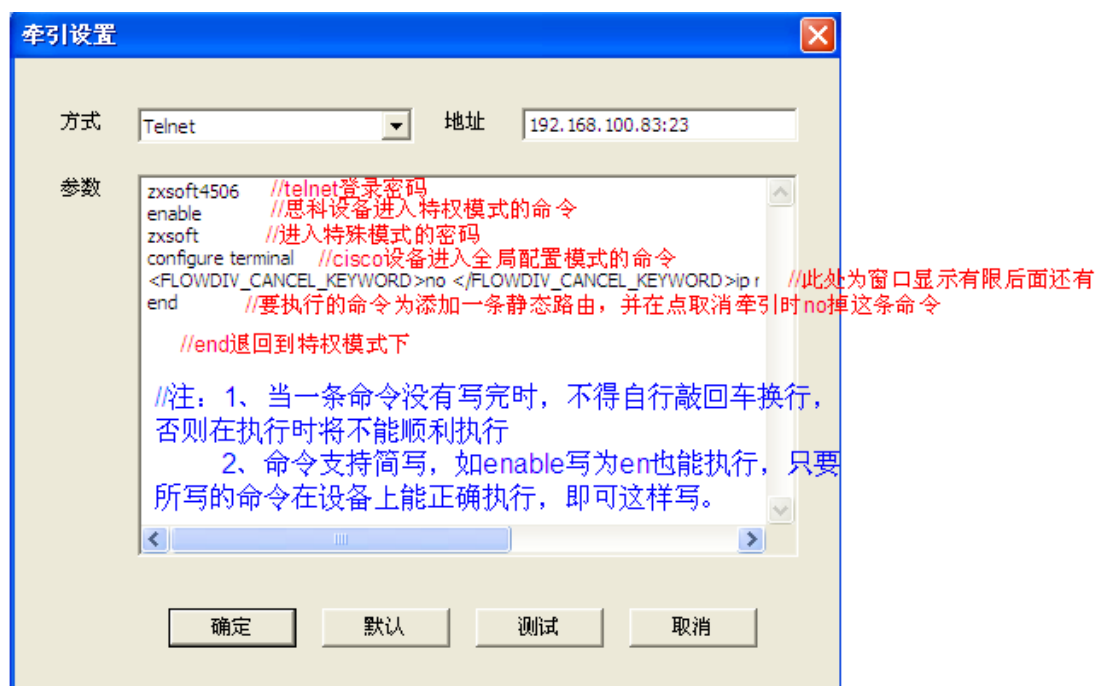
PASSWORD //telnet 登录密码

注: 有时可能采取本地用户名+密码方式，此时就要先写用户名，再换行写密码了

ENABLE_PASSWORD //进入特权 enable 模式的密码

注: 在此命令前应该加上进入特权模式的命令，具体命令跟据不同厂商而定，如 cisco 的为 enable, 华为的为 system 。总之一切都按照实际中登录设备的步骤进行就好

如图：此处以 cisco 设备为例



(图十一)

Configure terminal

//cisco 设备进入配置模式的命令

```
<FLOWDIV_CANCEL_KEYWORD>no </FLOWDIV_CANCEL_KEYWORD>ip route <HOST_ADDRESS>
255.255.255.255 null0
```

//此处为 cisco 设备添加/取消一条静态路由的命令

该命令分为两部分：

1) 牵引设置

```
ip route <HOST_ADDRESS> 255.255.255.255 null0
```

为添加一条静态的主机路由，下一跳为 null0。此处<HOST_ADDRESS>为一个变量，fwmon 会自动将触发了牵引设置的 IP 替换此变量。也可以不用此变量，直接写成一个 ip。

2) 取消牵引设置

```
<FLOWDIV_CANCEL_KEYWORD>no </FLOWDIV_CANCEL_KEYWORD>
```

此部分，在执行命令集时时候不会被执行。只有当用户在流量牵引界面中选择了已牵引的地址并点取消牵引按钮的时候才会被执行，即 no 掉先前的操作。

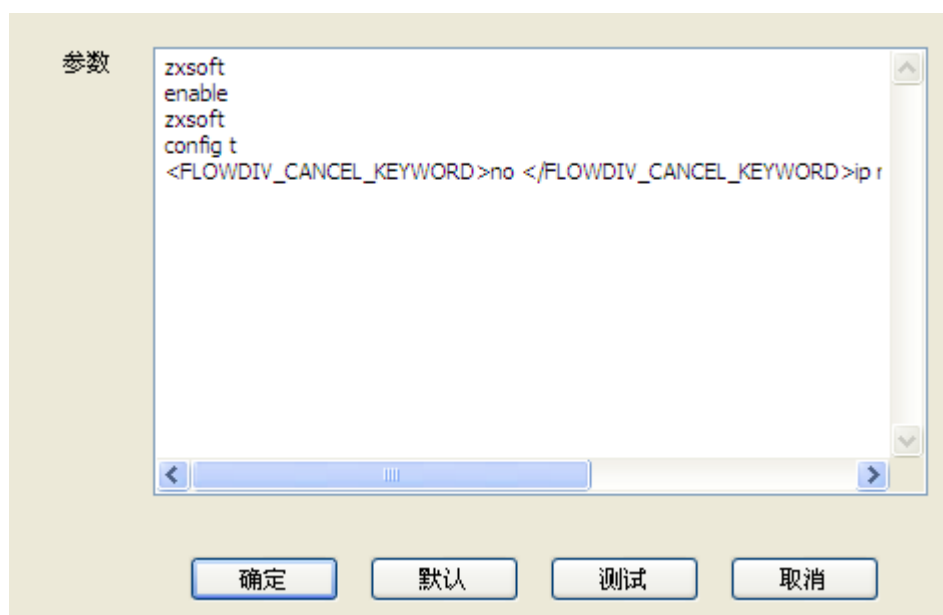


(图十二)

注：在编写命令集的时候也支持跟实际设备上一样的命令简写方式，如：enable 命令可以写成 en，Configure terminal 命令写成 conf t 都可以，只要写出的命令在设备上能正确执行

4.2.4 牵引配置中密码的密文显示

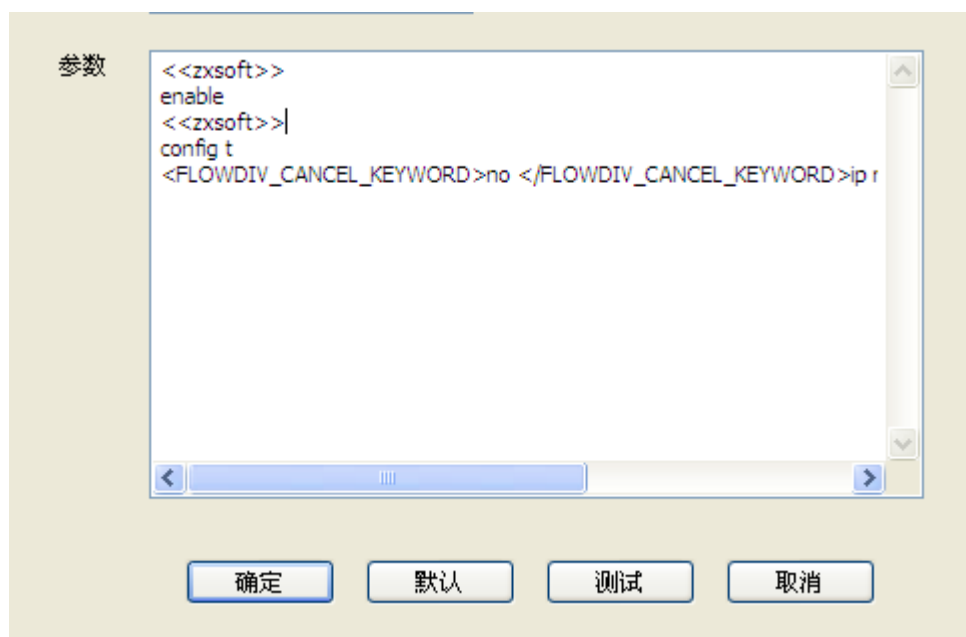
在点击牵引配置查看先前配置的参数，发现其中的密码都是以明文显示，这种方式显然容易造成设备权限泄露的事情，不符合当前网络管理的要求如图 12 所示



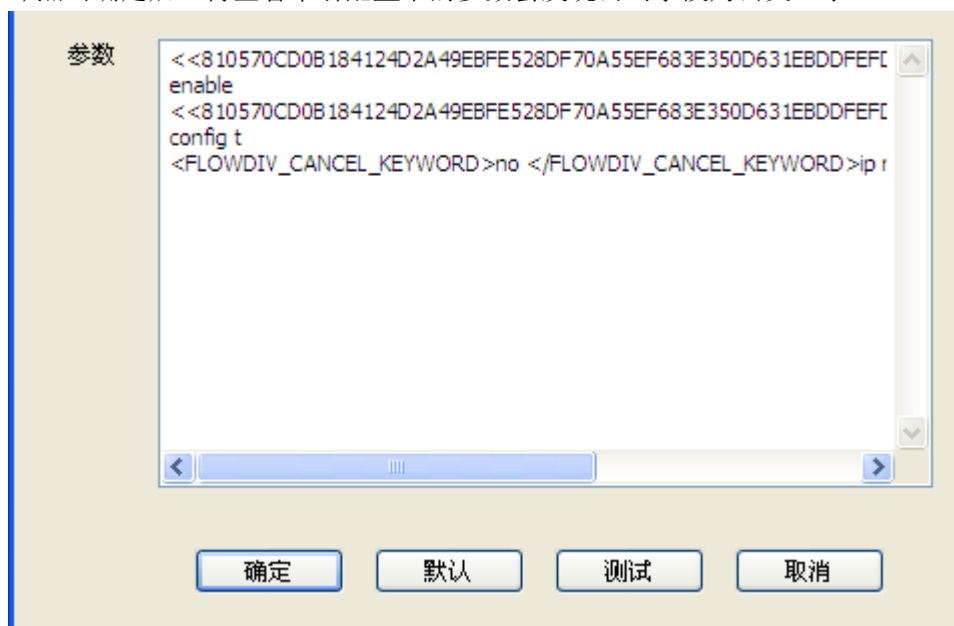
(图十三)

因而此处密码必需以密文方式显示操作如下：

- 1) 点击索引配置
- 2) 修改参数中的密码输写方式:以两层“<>”将密码写在其中



- 3) 点击确定后，再查看牵引配置中的参数会发现密码字段为密文显示



5、主机列表：



(图八)

主机：

根据主机列表数显示流量最大的 N 台主机地址

带宽：

显示该主机当时带宽占用情况，以 MBPS 为单位，包括 in 流量、out 流量

攻击频率：

显示该主机当时的攻击频率

连接：

显示该主机的连接数，包括 in 连接、out 连接、udp 连接

注：如设置多台集群管理地址，可通过选择其中一台管理查看单台防火墙的主机列表显示，未选择某台防火墙管理而直接点击“主机列表”，可查看到 TOPN 主机的总流量、总攻击频率及总连接情况。

6、 日志查看



(图九)

6.1 日志列表

时间:

记录事件详细时间

事件:

记录报警条件、设备地址和细节

6.2 主机列表:

详细记录报警设备中的 TOPN 主机地址、带宽、攻击频率连接和状态信息。

6.3 保存:

可将当时日志以.txt 文件格式保存至设定路径。

6.4 清除:

清除当时日志。

6.5 退出:

退出日志列表返回主界面

7、 退出:

即退出此监控器，便不再进行监控

三、获取技术支持方式

a) **咨询电话：**

24 小时技术支持热线：800-868-7722

售后服务直线：86-0551-5321158、5321558

点击在线“金盾技术客服” 金盾 24 小时竭诚为您服务

b) **OICQ：**

727339 798691 716897 937282 175282

182522 762736 103972 786909