Freedom Fone and SIP

The default policy of Freedom Fone is to only allow authenticated SIP calls. However, in order to allow unauthorized users to call into Freedom Fone via SIP (which is free of charge and only requires an Internet connection), we have implemented a solution which enables this.

Furthermore, to block VoIP scanners and other unsolicited traffic to hit the platform, we have implemented a firewall that blocks unwanted traffic.

Non authenticated SIP calls

SIP authentication can be set (true|false) in the configuration file core.php

```
/opt/freedomfone/gui/app/Config/core.php

define ('NO_SIP_AUTH',false);
```

true: No SIP authentication will take place. This will allow you do make unauthenticated SIP calls to Freedom Fone to reach its voice services.

false: SIP authentication is required.

The NO_SIP_AUTH setting is reflected in the dialplan.

```
/opt/freedomfone/xml_curl/dialplan.xml
```

Firewall to block unwanted traffic

If you set the NO_SIP_AUTH to ***true***, you allow any IP address to make a non-authenticated call to your platform. This is frequently misused by so called VoIP scanners, robots that aim to establish free phone calls though poorly configured VoIP gateways. VoIP scanners perform password brute force attacks, which generate large numbers of CS_DESTROY records. The CS_DESTROY records are shown in the Freedom Fone GUI as incomplete calls, and gives a misleading image of incoming calls.

To deal with the problem of unwanted traffic, a firewall has been implemented that blocks all SIP registration traffic that comes from any network that is not included in the whitelist.

The firewall is managed by a bash script (/opt/freedomfone/firewall/run.sh) which allows the following options:

```
/opt/freedomfone/firewall/run.sh {config|show|start|stop}

config: setup the whitelist file (/opt/freedomfone/firewall/whitelist.txt)
show:   shows status of firewall (whitelist and iptables rules)
start:  add rules from the iptables firewall
stop:   remove rules from the iptables firewall
```

Example setup

This example will set up a firewall that only allows SIP calls from the networks 192.168.1.0/24 and 192.168.2.0/24.

Step 1) Configuration wizard

When running the firewall script with the config option, the user will be guided through a configuration wizard which will create a whitelist.

```
root@sharicus:/opt/freedomfone/firewall# bash run.sh config

What is the public interface of your freedomfone installation? eth0
Do you want  to be able to place calls in your freedomfone installation (y/n)? y
Do you want 192.168.1.0/24 to able to place calls in your freedomfone installation
(y/n)? y
Do you want to allow more networks to place calls in your freedomfone installation
(y/n)? y
Enter network in CIDR format e.g. 192.168.0.0/16: 192.168.2.0/24
Do you want to allow more networks to place calls in your freedomfone installation
(y/n)? n
The following networks will be whitelisted in the firewall

192.168.1.0/24
192.168.2.0/24
```

Step 2) Add rules to firewall

This step creates the iptables rules, and must be run after creating the whitelist.

```
root@sharicus:/opt/freedomfone/firewall# bash run.sh start
```

Step 3) Show firewall status

The final step shows what settings that have been made. Please note that this option takes some time to display the result.

```
root@sharicus:/opt/freedomfone/firewall# bash run.sh show

Networks whitelisted

192.168.1.0/24
192.168.2.0/24

Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  192.168.0.0/16       anywhere            udp dpt:sip
ACCEPT     udp  --  192.168.0.0/16       anywhere            udp dpt:5080
LOG        udp  -- !192.168.0.0/16       anywhere            udp dpt:sip LOG level
warning prefix "Freedom Fone SIP registration"
LOG        udp  -- !192.168.0.0/16       anywhere            udp dpt:5080 LOG
level warning prefix "Freedom Fone SIP registration"
ACCEPT     udp  --  192.168.1.0/24       anywhere            udp dpt:sip
ACCEPT     udp  --  192.168.1.0/24       anywhere            udp dpt:5080
LOG        udp  -- !192.168.1.0/24       anywhere            udp dpt:sip LOG level
warning prefix "Freedom Fone SIP registration"
LOG        udp  -- !192.168.1.0/24       anywhere            udp dpt:5080 LOG
level warning prefix "Freedom Fone SIP registration"
```

```
DROP       udp  --  anywhere             anywhere             udp dpt:sip
DROP       udp  --  anywhere             anywhere             udp dpt:5080
ACCEPT     udp  --  192.168.1.0/24       anywhere             udp dpt:sip
ACCEPT     udp  --  192.168.1.0/24       anywhere             udp dpt:5080
LOG        udp  -- !192.168.1.0/24       anywhere             udp dpt:sip LOG level
warning prefix "Freedom Fone SIP registration"
LOG        udp  -- !192.168.1.0/24       anywhere             udp dpt:5080 LOG
level warning prefix "Freedom Fone SIP registration"
ACCEPT     udp  --  192.168.2.0/24       anywhere             udp dpt:sip
ACCEPT     udp  --  192.168.2.0/24       anywhere             udp dpt:5080
LOG        udp  -- !192.168.2.0/24       anywhere             udp dpt:sip LOG level
warning prefix "Freedom Fone SIP registration"
LOG        udp  -- !192.168.2.0/24       anywhere             udp dpt:5080 LOG
level warning prefix "Freedom Fone SIP registration"
DROP       udp  --  anywhere             anywhere             udp dpt:sip
DROP       udp  --  anywhere             anywhere             udp dpt:5080

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Logs

All SIP registrations are logged in:

```
/var/log/syslog
```