

Breaking the ISP Service Blocking

Target Objective:

To break the denial of SIP service of some countries, Welltech have developed a proprietary encryption/decryption for SIP, RTP, RTCP and T.38. Thus the ISP monitor device will not be able to find any VOIP traffic but only UDP traffic. The system can support encryption and normal SIP device simultaneously to protect your existing investment.

Recommendations:

Enable WellSIP 6500 Encryption/Decryption Features

- 1) Add an additional WellSIP 6500 service port and click the encrypt as follows:
Listen UDP Port: 18080 (the port number more than 15000 is recommended)
Check **Encrypt**



The screenshot shows a 'System Configuration' window with the following fields and options:

Field	Value	Encrypt
SIP Domain :		
Listen UDP Port :	5060	<input type="checkbox"/>
Listen UDP Port2 :	8080	<input type="checkbox"/>
Listen UDP Port3 :	18080	<input checked="" type="checkbox"/>

- 2) Soft reset to take effective
- 3) Turn on the encryption feature for CPE device (e.g. WellGate 3504) as follows:
 - Login Wellgate 3504
 - Input "ifaddr -security 1" to enable Encryption feature
 - Input "sip -pxport 18088 -outpxport 18080" to set the encryption to correct WellSIP 6500 encryption port
 - Input "sip -port 18088" to change SIP local service port to non-standard port (5060).

```
login: root
password:
Welcome to Terminal Configuration Mode
Please enter your configuration item

usr/config$ sip -pxport 18088 -outpxport 18088

usr/config$ sip -port 18088

usr/config$ _
```

- Input "sip -print" to verify

```
login: root
password:
Welcome to Terminal Configuration Mode
Please enter your configuration item

usr/config$ sip -pxport 18088 -outpxport 18088

usr/config$ sip -port 18088

usr/config$ sip -print

Run Mode : PROXY MODE
Primary Proxy address : 192.168.19.69
Primary Proxy port : 18088
Secondary Proxy address : null
Secondary Proxy port : 5060
OutBound Proxy address : 192.168.19.69
OutBound Proxy port : 18088
Prefix string : null
Line1 : 1021
Line2 : 1022
Line3 : 1023
Line4 : 1024
pbook search : OFF
Local Ringback Tone : OFF
PRovisional ACKnowledgment : OFF
Late Media : OFF
SIP listen port : 18088
RTP receive port : 16384
Expire : 60
Session Expire : x
Minimum Session Expire : x
User agent : x
Retransmission T1 : 500
```

- Input "ifaddr -print" to verify

```

login: root
password:
Welcome to Terminal Configuration Mode
Please enter your configuration item

usr/config$ ifaddr -print

Internet address information
WAN IP address      : 192.168.19.33
Subnet mask         : 255.255.248.0
Default gateway     : 192.168.19.253
DHCP startup        : OFF
SNTP                : mode=1
                   : server 168.95.195.12
                   : time zone : GMT+8
                   : cycle=1024 mins

IPSharing           : no IPSharing device.

HTTP port           : 80
Primary DNS Server  : 168.95.192.1
Secondary DNS Server : 168.95.1.1
Security            : OFF
usr/config$ _

```

- Commit & reboot to take effect

```

login: root
password:
Welcome to Terminal Configuration Mode
Please enter your configuration item

usr/config$ ifaddr -print

Internet address information
WAN IP address      : 192.168.19.33
Subnet mask         : 255.255.248.0
Default gateway     : 192.168.19.253
DHCP startup        : OFF
SNTP                : mode=1
                   : server 168.95.195.12
                   : time zone : GMT+8
                   : cycle=1024 mins

IPSharing           : no IPSharing device.

HTTP port           : 80
Primary DNS Server  : 168.95.192.1
Secondary DNS Server : 168.95.1.1
Security            : OFF
usr/config$ reboot

```

After the installation, both CPE with encryption enabled will be able to talk directly. If one of the CPEs is encrypted and another one is unencrypted, the SIP, RTP/RTCP and T.38 will be routed back to WellSIP 6500 to make both parties talk. It will consume an RTP resource.

Although WellSIP 6500 can support both encrypted and non-encrypted devices simultaneously, it is recommended to have a separate server to use for all encrypted devices to make sure the Internet Service Provider has no findings on your VOIP traffic.