

Configuring gbox – a work in progress

Author: Anakin aka Psycho

Date: 7th august 2005

Version: 1.1

No rights whatsoever can be claimed from this document. It is purely meant for people to be able to read the logging and edit configuration-files for gbox. Errors and mal-functioning machines cannot be blamed upon this document. It's a proven concept.

Everything I have documented will be commented here. As I find out something new, it will be added. Text Marked **Anyone?** I don't know the answer to. Please fill in the blanks! 😊

Share-configuration

The template is:

Server

M: { <OWN_IP> { <KEY_A> } }

D: { <OTHER_IP> { port_from port_to { <KEY_B> { <X> <Y> } } } }

Client

M: { <OWN_IP> { <KEY_B> } }

D: { <OTHER_IP> { port_from port_to { <KEY_A> { <X> <Y> } } } }

- **<OWN_IP>** => IP-address of the box. If this is going over the internet, use the WAN-IP-address!!
- **<KEY_*>** => Encryption-key of the box
- **<OTHER_IP>** => The IP- or DNS-address of the person you want to connect to.
- **<PORT_FROM>** => Port you want to use on the box. If this is going over the internet, this needs to be forwarded if behind a router! **UDP!!**
- **<PORT_TO>** => Port that the other sided uses on the box.
- **<X>** => Share-level for the LOCAL cards.
- **<Y>** => Share-level for cards you receive from others.

Assuming the server has the IP-address 192.168.1.10 and the client 192.168.1.11:

Find the file /var/keys/cwshare.cfg and alter the following lines accordingly:

Server

M: { 192.168.1.10 { 1234ABCD } }

D: { 192.168.1.11 { 8019 8020 { DCBA4321 { 5 5 } } } } # Client

Client

M: { 192.168.1.11 { DCBA4321 } }

D: { 192.168.1.10 { 8020 8019 { 1234ABCD { 5 5 } } } } # Server

This will off-course work over the internet! Use the WAN-IP-address or Just use a DynDNS or no-

ip address... Looks cooler.. 😊

=====

Analyzing logging

So, you've got things sorted, and you want to take a look at what's what. Well, actually, there are 6 files to be viewed, of which 4 are permanent:

- **/var/tmp/share.info** => shows the cards you receive from others
To make things easy, I took myself as an example. I did this on my dreambox:

```
/tmp > cat share.info
CardID 0 at 192.168.2.102 Card 0100006A SI:3 Lev:0 dist:1 id:87F4
CardID 1 at 192.168.2.102 Card 0100006B SI:3 Lev:0 dist:1 id:87F4
CardID 2 at 192.168.2.102 Card 0100006C SI:3 Lev:0 dist:1 id:87F4
CardID 3 at 192.168.2.102 Card 0100006D SI:3 Lev:0 dist:1 id:87F4
CardID 4 at 192.168.2.102 Card 06260000 SI:11 Lev:0 dist:1 id:87F4
```

OK, to break things down I'll use the first line:

- **CardID 0** => ranking-number of the card the way they are sorted... Alphabetically on Card-number.
 - **at 192.168.2.102** => IP-address of where they are coming from
 - **Card 0100006A** => Card-number. This is how the card is identified
 - **SI:3** => Displays the slot the card is in at the provider, when run on a Linux-PC up to 18 has been seen.
 - **Lev:0** => Amount of hops I'm allowed to reshare. Zero. 😊
 - **dist:1** => Amount of hops the card is at. In this case: 1.
 - **id:87F4** => Identification-number for gbox that is providing the card.
-
- **/var/tmp/share.log** => Same as share.stat, only that this displays the real-time data.
 - **/var/tmp/share.onl** => shows who's on-line
Again, I'll use myself as an example:

```
/tmp > cat share.onl
1 192.168.2.102 192.168.002.102 87F4 2.01
```

 - **1** => 1 is on-line, 0 is offline.
 - **192.168.2.102** => The entry you use in cwshare.cfg.
 - **192.168.002.102** => The way gbox translated cwshare.cfg to an actual IP-address. See the 002 ? 😊
 - **87F4** => Identification-number for gbox on the other end.
 - **2.01** => Version-number of gbox on the other end.
 - **/var/tmp/share.stat** => Same as share.log, only that this displays the stats over the entire running-time, and of the last 5 minutes.

- **Hello_I/O** => Number of hello's or "handshakes" between 2 peers.
 - **ECM_I/O/F** => ECM received (In), sent (Out) and Forwarded by gbox.
 - **CW_I/O/F** => Control Words received (In), sent (Out) and Forwarded by gbox. Control Word is the reply to an ECM request.
 - **GSMS_I/O** => Messages received (In) and sent (Out) and by gbox.
 - **loc_up and loc_down** => LOCAL Network traffic. (Probably filters defined by the internet standard, 10.x.x.x / 127.x.x.x / 192.268.x.x / 169.254.x.x)
 - **inet_up and inet_down** => Network traffic in and out of internet. (Probably every other IP-address different from what I mentioned 1 point before?)
- **attack.txt** => Shows a misconfiguration or someone that is trying to connect to you without being authorized to do so.

An example. On my server I mutilated the key for the client (that means the line starting with D:). On the client the attack.txt is created and filled with a number of messages:

- **ATAK ALERT: from IP 192.168.002.102 port 3101 PASSWORD IS WRONG EDB2097E (32) Sun Aug 7 16:32:09 2005**

This means that someone is trying to connect using a wrong password.

I then remove the server completely out of the config:

- **INTRUDER ALERT: IP 192.168.002.102 Port 3101 (PASS 2346A4B2 ID 87F4 unknown) Sun Aug 7 16:40:50 2005**

You see the difference?

- **goneOFFLINE: BAD IP|PORT (DynDNS Peer1) Actual IP Peer1/Localport (IP-address from local DNS Resolve/Localport) Tue Aug 23 12:55:02 2005**

This message says that the actual IP-address of the Peer doesn't match with what gbox thinks it should be.

- **Debug.txt** => Can take all message generated by gbox. Depends on what you put after Z: in the file gbox_cfg
 - **->HelloL to** => Initial request to every "D:-line" in cwshare.cfg
 - **->Hello1 to** => Second request if first not answered to (quickly enough)
 - **->Hello2 to** => Third request if first not answered to (quickly enough)
 - **->HelloR to** => I think this means Reconnect to peer if timed out? **Anyone?**
 - **->HelloW to** => Don't know. **Anyone?**
 - **->HelloS1 to** => Don't know. **Anyone?**
 - **->Here? to** => Repetitive request every x seconds to see if peer has come on-line.
 - **<-Hello from** => Reply to Hello L/1/2/R from Peer, Or first request after Peer reboot? **Anyone?**
 - **<=Hello from** => Don't know. Reply is received in the same millisecond as "<-Hello from". **Anyone?**
 - **->Hello to** => Reply to "<- Hello from".

- **||CW (->1) blocked from Peer1 to Peer2/GboxID Peer2 =>** Don't know actually. **Anyone?**
 - **<>ECM (1->1) from Peer1 forwarded to Peer2 (GboxID Peer2)**
<>CW (->1) from Peer2 forwarded to Peer1 => Here you see a request being relayed to someone else, and the answer to that request. In (1->1), the first "1" stands for the slot the card is in at the supplier, "->1" stands for the amount of hops the message has to travel to that supplier. In (->1) "1" stands for for the slot the card is in at the supplier.
 - **<-ECM (1<-) received from Peer1**
->CW (->1) send to Peer1 (527 ms) => This is a request from Peer1 to a local card, the reply and the time it took to read the card and supply the key.
 - **dbox2 Peer1 is not responding 6 times =>** Well, that says enough I think?
 - **goneOFFLINE: Removing Peer1 from list, seems offline =>** Sets Peer1 from 1 to 0 in share.onl, after not responding 6 times.
- **online.log =>** Shows the coming and going of peers. Creation of this file depends on the line N: in cwshare.cfg
 - **comeONLINE : Welcome PEER1 IP xxx.xxx.xxx.xxx/<Port PEER1> Sun Sep 4 16:22:45 2005 =>** PEER1 comes online
 - **goneOFFLINE: Removing PEER1 from list, seems offline Sun Sep 4 17:45:39 2005 =>** PEER1 doesn't respond anymore
 - **IP update : PEER1 was xxx.xxx.xxx.xxx now xxx.xxx.xxx.xxx Sun Sep 4 17:45:53 2005 =>** PEER1 has a new IP-address
 - **comeONLINE : Welcome PEER1 IP xxx.xxx.xxx.xxx/<Port PEER1> Sun Sep 4 18:01:05 2005 =>** PEER1 is back on-line again!

URL's for more information:

<http://www.db-sat.com/>
<http://www.digital-4-all.com>

© Anakin '05