

The accredited security level of this system is: TOP SECRET//SI-GAMMA/TALENT
KEYHOLE//ORCON/PROPIN/RELIDO/REL TO USA, FVEY *
TOP SECRET//SI//REL TO USA, FVEY

(U) QUANTUM Shooter SBZ Notes

From Wikilinfo

Contents

- 1 (U) Overview
- 2 (U) Infrastructure Components
 - 2.1 FREEFLOW
 - 2.2 (TS//SI,OC//REL) CHIMNEYPOOL and Comms
 - 2.3 (U) Diodes
 - 2.4 (U) NCC
 - 2.5 (S//SI//REL) Gateway ("ROC_LOW")
 - 2.6 (S//SI//REL) TURBINE
- 3 (U) How To
 - 3.1 (TS//SI//REL) Connecting to the QUANTUM NCC
 - 3.2 (TS//SI//REL) Getting a DND from the NCC
 - 3.3 (TS//SI//REL) Getting a DND from /targets for an upgrade
 - 3.4 (TS//SI//REL) Updating a DND from the NCC for FELONYCROWBAR
 - 3.5 (S//SI//REL) Getting Link Info and Modifying Links
 - 3.5.1 (S//SI//REL) I have a FRZ address. How do I get a linkEndId?
 - 3.5.2 (S//SI//REL) How do I get/change the link state?
 - 3.5.3 (S//SI//REL) How do I modify the IP address or port of the link?
- 4 (U) Other notes
 - 4.1 (U) MHS
- 5 References

(U) Overview

(TS//SI//REL) For an overview of QUANTUM and how shooters fit into the greater QUANTUM infrastructure, see QUANTUM Operational Design Implementation ([REDACTED]) on the ROC Wiki.

(TS//SI//REL) A QUANTUM shooter is a host computer on the internet that has been implanted with a STRAITBIZARRE (SBZ) configured to receive commands from TURBINE, via SURPLUSHANGAR/HANGARSURPLUS diodes, and the

KEYHOLE//ORCON/PROPIN/RELIDO/REL TO USA, FVEY *

Once a box has been identified for use as a QUANTUM shooter, an SBZ is configured using FELONYCROWBAR along with a Deployed Node Document (DND), an XML config file. The FELONYCROWBAR GUI and build scripts handle some aspects of configuration, such as which SBZ modules to include, but it also needs the DND to configure most aspects of the communications links. For an upgrade, an old DND can be modified by hand, but for a new build, a new DND will need to be generated in the NCC (with some changes by hand). Once the core and "bin" customization SBZ files are generated (usually a zip file output from FELONYCROWBAR), an interactive operator can deploy these to the shooter box.

(U) Infrastructure Components

FREEFLOW (




(TS//SI//REL) There are four operational FREEFLOW threads (plus one for PASSAGEHILL testing):

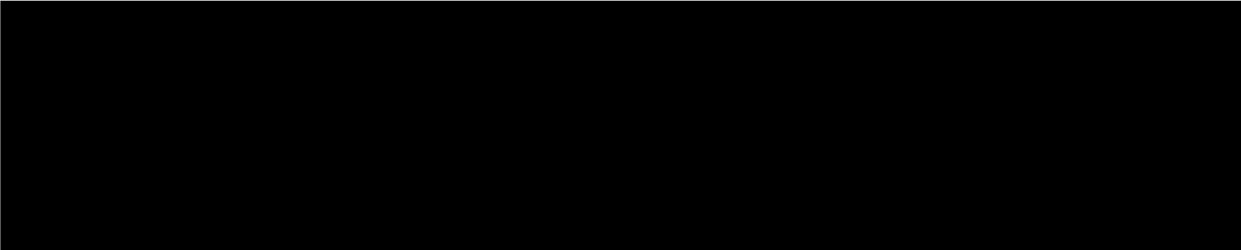
- Thread A, the original FREEFLOW thread (early 2008), associated with the old ROC/MIT covert infrastructure (FORESTPLACE/FUSSYKEEL).
- Thread B, the QUANTUM thread
- Thread C, FINGERGNOME high-to-low transfer
- Thread D, the new FREEFLOW 2.0 thread, associated with new covert infrastructure (FROZENEARTH).

The FREEFLOW Confluence page (<https://confluence-nf.tao.nsa/display/ROC/FREEFLOW>) has a good overview picture, especially showing the differences between the old FREEFLOW (1.0, the purplish-gray area) and the new FREEFLOW (2.0, the yellow area). The QUANTUM thread is 1.0 for now, but will eventually be upgraded and this whole process will change.

FREEFLOW components important for understanding QUANTUM shooters are described below **as they apply to the shooter build process**, and a good overview of the QUANTUM infrastructure can be found here



(TS//SI,OC//REL) CHIMNEYPOOL



(TS//SI,OC//REL) CHIMNEYPOOL uses its own version of RPC (CHM RPC) for communications, which ride on the FRIEZERAMP Network Stack [REDACTED]. CHIMNEYPOOL-compliant nodes are referred to by their four-byte FRIEZERAMP (FRZ) addresses, which are usually represented in hex.

(TS//SI//REL) **Links** are half-duplex comms paths that need to be configured for two CHM nodes to be able to talk. These can be encrypted or unencrypted and are usually spit out correctly by the NCC DND, along with the Security Associations that allow them to communicate with the NCC (keys are generated by the NCC). To communicate with TURBINE, the SBZ also needs to have two additional Security Associations configured -- one to communicate with SURPLUSHANGAR and one for HANGARSURPLUS. [REDACTED] MIT) usually configures the HS/SH side, which generates the keys. You'll need to configure SAs to match [REDACTED] keys, which can be done either by modifying the DND, or post-deployment via commands directly to the SBZ via NCC (see Dave).

(TS//SI,OC//REL) More details on the CHIMNEYPOOL/FRIEZERAMP comms can be found here [REDACTED]

(U) Diodes [REDACTED]

SURPLUSHANGAR [REDACTED] (Low-to-High), and HANGARSURPLUS [REDACTED] (Low-to-High), which each have three parts:

- High Proxy: connects to ISLANDTRANSPORT [REDACTED] and converts to CHIMNEYPOOL messages.
- Packager (high-to-low only)
- Low Proxy: talks CHM/FRZ.

(U) NCC

(TS//SI//REL) The GENIE Network Configuration Center (NCC) manages CHIMNEYPOOL comms links for all STRAITBIZARRE implants, via MIDDLEMAN. Information on the NCC is often out of date (the "new" NCC will be on the high side and will hopefully be easier to update), so only use the NCC to generate a DND if you can't modify an old config, either from [REDACTED] or from /targets/zombiearmy to find the one the operator put on the box. You'll also need the NCC to manage the links.

(S//SI//REL) Gateway ("ROC_LOW")

(TS//SI//REL) Web Sniper Gateways (WSGs) sit between MIDDLEMAN and the

QUANTUM shooters. Information about these is NOFORN and is found in a spreadsheet updated by [REDACTED]. You'll need to configure the shooter to send comms via the nearest gateway -- choose the gateway that has the lowest latency to the shooter, based on the results of latency tests (which are not expected to change frequently).

(S//SI//REL) TURBINE

The Confluence TURBINE [REDACTED] page describes what happens when an SBZ calls back.

(U) How To

(TS//SI//REL) Connecting to the QUANTUM NCC

- Your WAITAUTO box needs to be able to talk to the QUANTUM NCC [REDACTED]. You may need an MITHelp ticket to get the firewall to allow this connection.
- Use Putty to SSH to the NCC box (username: ncc_user; email [REDACTED], [REDACTED] for password) with the following options:
 - Connection -> SSH -> check box to "Enable X11 forwarding"
 - Connection -> SSH -> X display location: set this to **<Your WAITAUTO IP address>:0**
- cd /opt/ncc/ and run ./start_gui.sh. User name (either user1 or user2) depends on who else is using the box -- check with the POCs above.

(TS//SI//REL) Getting a DND from the NCC

- Follow instructions in the document in References, or confirm that the settings are correct.
- Once your changes have been saved, in the terminal window, run the following:

```
cd /opt/ncc/util
./build_sbz_bin.sh WebSnipe <your node cover term> localhost (where "WebSnipe" is the target cover te
```

- The resulting DND will be in /tmp (WebSnipe_<node cover term>_DeployedNode#.xml). Copy this to a thumb drive and upload to RSS.

(TS//SI//REL) Getting a DND from /targets for an upgrade

- Check either FELONYCROWBAR or /targets/ZOMBIEARMY/<node>/ops/<date>/techdata if they have it there from a previous op. This doesn't contain the DND, but it contains an XML which can be used to back out

the DND.

- Send zip file to ██████████ to be run through the Fiptrix tool to generate a DND XML file.

(TS//SI//REL) Updating a DND from the NCC for FELONYCROWBAR

- (TS//SI//REL) Add "implantId" element as the first child node, and "implantUuid" as the last
- (TS//SI//REL) Add "<sbzXfilConfig><defaultDestAddr>00100005</defaultDestAddr></sbzXfilConfig>"
- (TS//SI//REL) Add Security Associations for HANGARSURPLUS (00 for send) and SURPLUSHANGAR (02 for receive)
- You are now ready to upload to FELONYCROWBAR for your SBZ build.

(S//SI//REL) Getting Link Info and Modifying Links

(TS//SI//REL) This is mostly done using the Wrench/Screwdriver tab ("Rudy") in the NCC.

(S//SI//REL) I have a FRZ address. How do I get a linkEndId?

Choose the appropriate send and receive nodes for your link, "Interface Provider":Cidr, "Procedures":

(S//SI//REL) How do I get/change the link state?

getLinkState to check state. (1,2) indicate the link is off; (3,4) indicate the link is on. Use link0

(S//SI//REL) How do I modify the IP address or port of the link?

To change an IP address or port, choose "Interface Provider":LinkMgr and "Procedures":getLinkParameter
getLinkState to check state. If it's on, turn it off (linkOff, stopLink).
setLinkParameter: enter linkEndId and parameterId, same as above (should return success)
startLink, linkOn to bring link back up (should return success).
getLinkState to check state (should be on)

(U) Other notes


(U) MHS

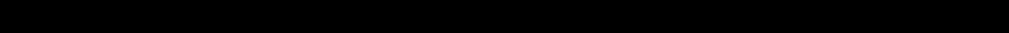
(S//REL) There is no HANGARSURPLUS in the MHS case. GCHQ basically does not want it to call back. They have their own method of determining shooter health.

- Disable the CCFP since it requires the node to ack back through the HANGARSURPLUS (which doesn't exist in the MHS configuration).
- For good measure, configure only the receive Security Associations and UDP link (Low Proxy to SBZ), and none of the send SAs/links.
- Configure BonjourMod to not send heartbeats.
- Configure SbzLogMod to not exfil logs.
- Do not include SbzXfilMod if possible, or set Min Priority To Exfil to 16.
- Do not include any of the default modules (SiphonCauseway, ShinyObject, etc.).

(U) Look into testing using CHIMNEYPOOL Python script ("chim.py") to issue commands.

References

Configuring SBZ from scratch using the NCC 

Retrieved from 

Derived From: SI Classification Guide, 02-01, Dated: 20060711
and NSA/CSSM 1-52, Dated: 20070108
Declassify On: 20320108

TOP SECRET//SI//REL TO USA, FVEY