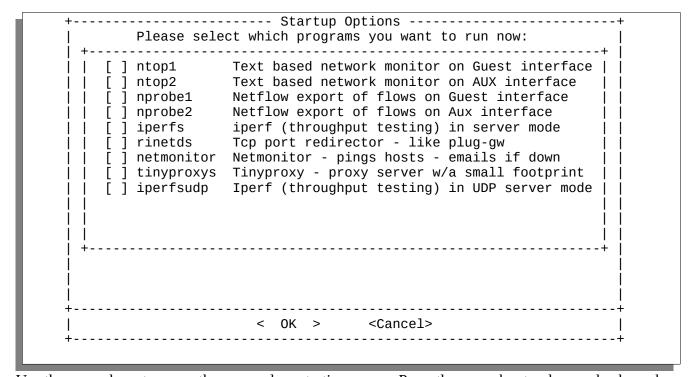
NUK Documentation – Proxy Server Introduction

The NUK comes with a proxy server known as tinyproxy. It is meant to be a low footprint (meaning doesn't require lots of memory or disk space) proxy server. It can be accessed via port 8888 or via Stunnel on port 48228. If you are going to connect your NUK to the public Internet, we recommend using Stunnel, or only allowing access to port 8888 (or unlimited access if you wish) to certain specific addresses. This is because people search for "open" proxy servers (especially people in countries that don't have unlimited Internet access) and will use up your bandwidth.

Setting up Stunnel is covered in the document titled "NUK Documentation – VNC Menu"

Starting the Proxy server

The proxy server can be started in three ways. It can be started from the Nettools2 choice on the VNC Menu, or it can be started via the Start Services or Startup-opts. The first two (Nettools2, and Start Services) are to launch the proxy server only when needed. Startup-opts starts the proxy server whenever the NUK boots. We will cover the second two options (Start Services and Startup-opts). After choosing Start Services, you'll see this menu:



Use the arrow keys to move the cursor down to tinyproxys. Press the space bar to place a check mark

(an "X" in this case) and press enter. This will case tinyproxy to start:

```
tinyproxy is running. If you want more information on how to configure tinyproxy, please see ...
```

Now you can access tinyproxy via port 8888 or via stunnel. The Startup-opts menu looks identical except for the first two lines:

To have tinyproxy start whenever the NUK starts, move down with the arrow keys, press spacebar to add a check (or "X") and press enter. You might want to have iperfs start as well.

Firewalling

Including in the NUK is a sample firewall file called ipfsample.conf. For a firewall file to be used, it must be named ipf.conf. You can test a firewall file by going to the **VNC Menu, Main menu, Choice D, subchoice F.** This brings up the following window:

Entering this will test the default firewall file. It will block all traffic (except from 172.16.0.0/16) on ports except 48226 (SSH), 48227 (stunnel-vnc), 48228 (stunnel-proxy).

```
block in quick all with short
block in quick all with opt lsrr
block in quick all with opt ssrr
block in quick all with ipopts

pass in quick on re1 proto tcp from 172.16.0.0/16 to any port = 21
pass in quick on re1 proto tcp from 172.16.0.0/16 to any port = 23
pass in quick on re1 proto tcp from 172.16.0.0/16 to any port = 5900
pass in quick on re1 proto tcp from 172.16.0.0/16 to any port = 6001
pass in quick on re1 proto tcp from 172.16.0.0/16 to any port = 8888
```

The first four lines block traffic with suspicious IP packet settings (setting usually used by hackers). The bolded lines are the ones we're interested in. They allow access to five ports from any address in the 172.16.0.0/255.255.0.0 range to the management interface. Those ports are:

Port	Service
21	FTP
23	Telnet
5900	VNC
6001	X-Windows (experimental)
8888	Tinyproxy

So if you want to allow other addresses access to the proxy or VNC (or FTP or Telnet), just copy the lines and change 172.16.0.0/16 to the address range you want to allow. If you want to allow access on other interfaces (the default firewall rule denies this), then the following table will show you what interface name(s) to use:

"Human" interface name	"Computer" interface name
Monitor1	re2
Mgmt.	re1
Monitor2	re0

The best way to edit ipfsample.conf is to use psftp (on windows) or sftp on Mac or Unix (or standard FTP if you've allowed that) to download the file to your computer. Once you're done, you can upload the file back to the NUK for testing (via the menu choice above) and then once it's working satisfactorily, rename it to ipf.conf

Table of Proxy Servers

Here's a table you can fill in.

NUK Location	NUK Mgmt IP	NUK Mgmt range	NUK Monitor1 IP	NUK Monitor 2 IP