

(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:

```
+----- Startup Options -----+
|           Please select which programs should run on startup:           |
| +-----+ |
| | [ ] ntop1      Text based network monitor on Guest interface |
| | [ ] ntop2      Text based network monitor on AUX interface  |
| | [ ] nprobe1   Netflow export of flows on Guest interface   |
| | [ ] nprobe2   Netflow export of flows on Aux interface     |
| | [ ] iperfs    Iperf (throughput testing) in server mode    |
| | [ ] rinetds   Tcp port redirector - like plug-gw           |
| | [ ] netmonitor Netmonitor - pings hosts - emails if down   |
| | [ ] tinyproxys Tinyproxy - proxy server w/a small footprint |
| | [ ] iperfsudp Iperf (throughput testing) in UDP server mode |
| | +-----+ |
| | +-----+ |
| | < OK >      <Cancel> |
| +-----+ |
+-----+
```

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:

```

+----- Test ipf configuraton -----+
|           What is the name of the new ipf configuration file?           |
| +-----+ |
| -|/config/ipfsample.conf |
| +-----< OK >-----<Cancel>-----+ |
+-----+

```

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:

