

Zeroshell as filtering bridge with connection tracking log and HAVP proxy

I have already used and administrated several Firewall distributions, like IP-Cop, PFSense, Monowall, RouterOS, OpenWRT, DD-WRT, but none of them was easily customizable to do what this project was about.

So I decided, to give Zeroshell a try.

Since the documentation to this Distro is, well, amendable, I ran into a few dead ends, before I got the setup as desired.

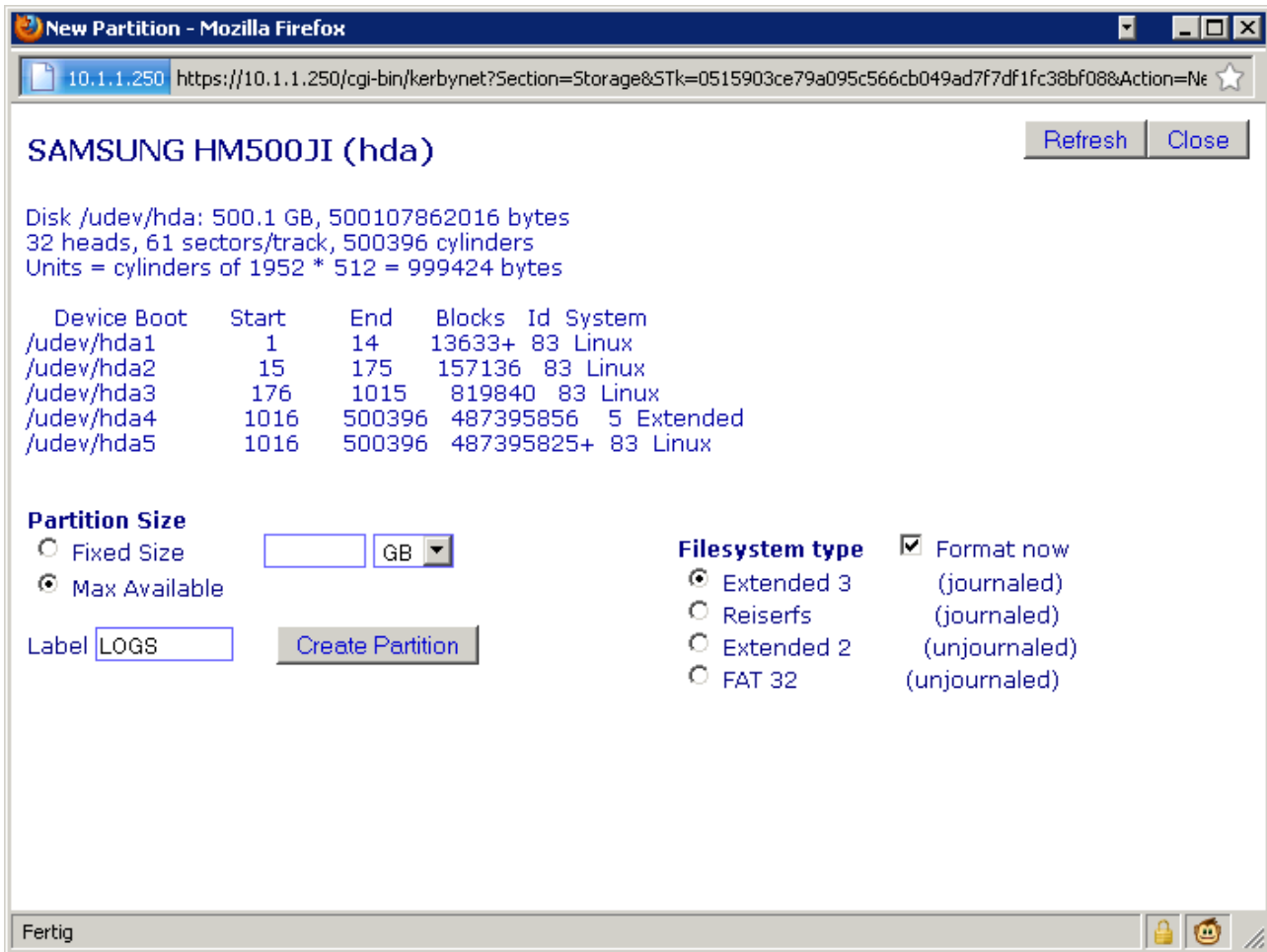
Therefore (and for the activation keys, of course) I decided to write some instructions on how to do this.

There was a 500 GB SATA hdd laying around, so it was used to store the image for CF and later the data partition for profile and logs. I used physdiskwrite to write the image to the disk (make sure you start physdiskwrite with admin rights), with a Windows 7 Computer, took only a few minutes. Then the hdd was built into my firewall „server“, a Celeron 1200 Mhz, 512 MB SD-RAM, a 4-Port Gigabit Lan adapter (Realtek 8169).

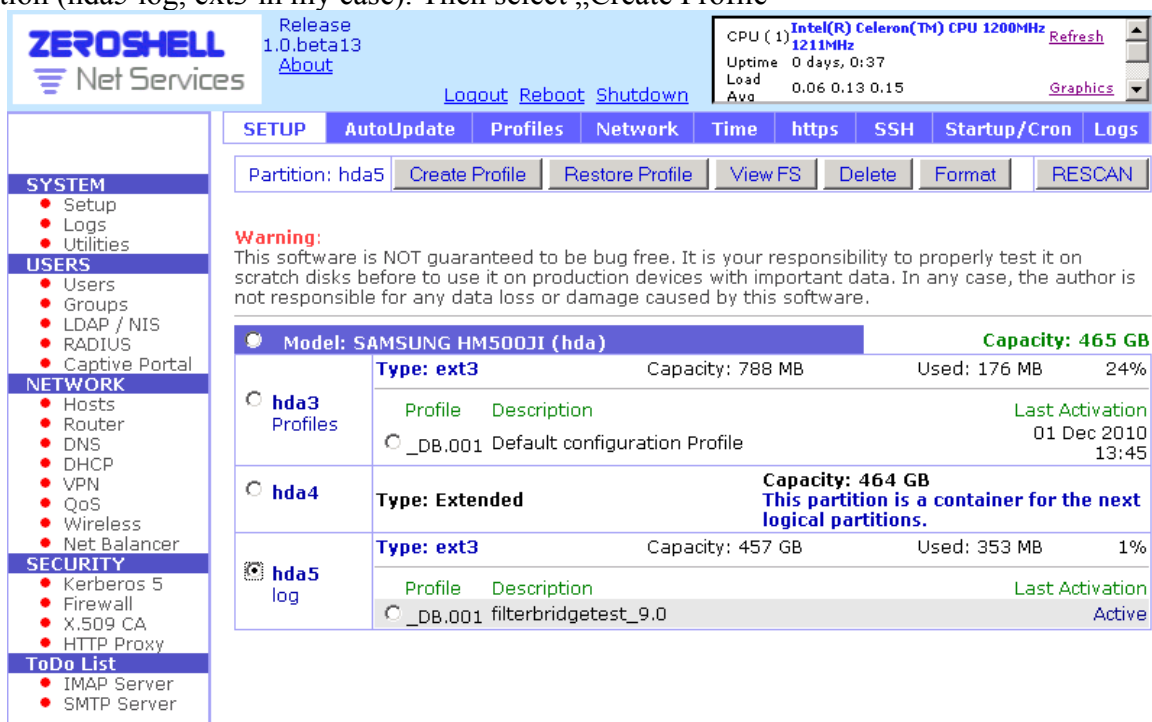
After booting Zeroshell the first time, you can reach the web-interface at 192.168.0.75. Set your PC's IP accordingly. You can ignore any Browser messages about „certificate invalid“. Login with admin / zeroshell. Then click on System/Setup(1), then Profiles(2). Your disk(s) will be shown, I chose the only one,(3) then click on „New Partition“(4)

The screenshot shows the Zeroshell web interface. At the top left is the logo for Zeroshell Net Services. The top right shows system information: Release 1.0.beta13, About, CPU (1) Intel(R) Celeron(TM) CPU 1200MHz 1211MHz, Uptime 0 days, 0:37, Load Avg 0.06 0.13 0.15, Refresh, and Graphics. Below this is a navigation bar with tabs: SETUP, AutoUpdate, Profiles, Network, Time, https, SSH, Startup/Cron, and Logs. The SETUP tab is active. Below the navigation bar, there is a section for Storage Device: hda, with buttons for Raw view, New partition, and RESCAN. A red '2' is placed over the Profiles tab and a red '4' is placed over the New partition button. On the left side, there is a sidebar menu with categories: SYSTEM (Setup, Logs, Utilities), USERS (Users, Groups, LDAP / NIS, RADIUS, Captive Portal), NETWORK (Hosts, Router, DNS, DHCP, VPN, QoS, Wireless, Net Balancer), SECURITY (Kerberos 5, Firewall, X.509 CA, HTTP Proxy), and ToDo List (IMAP Server, SMTP Server). A red '1' is placed over the Setup option in the SYSTEM category. The main content area shows a warning message: "Warning: This software is NOT guaranteed to be bug free. It is your responsibility to properly test it on scratch disks before to use it on production devices with important data. In any case, the author is not responsible for any data loss or damage caused by this software." Below the warning, there is a table of storage devices. A red '3' is placed over the first device, hda. The table has columns for Model, Capacity, Type, and Used space. The first device is hda, Model: SAMSUNG HM500JI (hda), Capacity: 465 GB, Type: ext3, Used: 176 MB (24%). Below this, there is a table of profiles for hda3. The first profile is _DB.001 Default configuration Profile, Last Activation: 01 Dec 2010 13:45. Below this, there is a table of partitions for hda4. The first partition is hda4, Type: Extended, Capacity: 464 GB, and a note: "This partition is a container for the next logical partitions." Below this, there is a table of logs for hda5. The first log is _DB.001 filterbridgetest_9.0, Last Activation: Active.

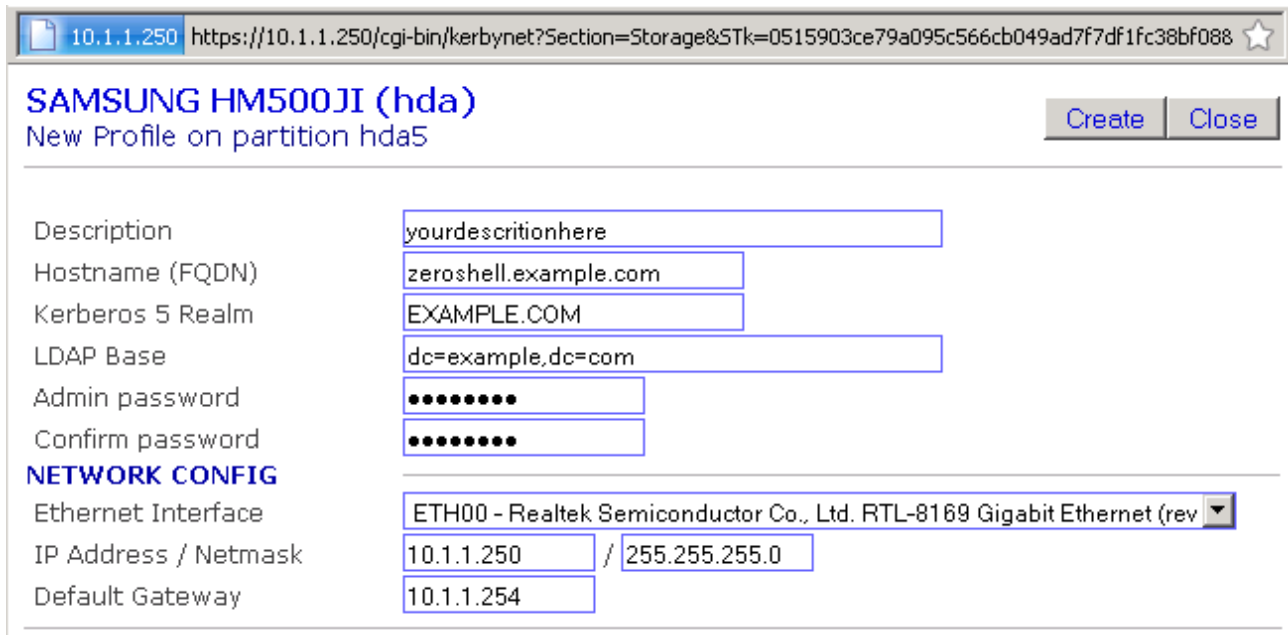
You will see something like the following:



I just gave a Label name, left all other settings to default. Then click on „Create Partition“, and be patient (depending on your harddisk size, this could take a while). After the creation of the partition and the formatting is done, you can go back to the „Profiles“ menu. Select the newly created partition (hda5 log, ext3 in my case). Then select „Create Profile“

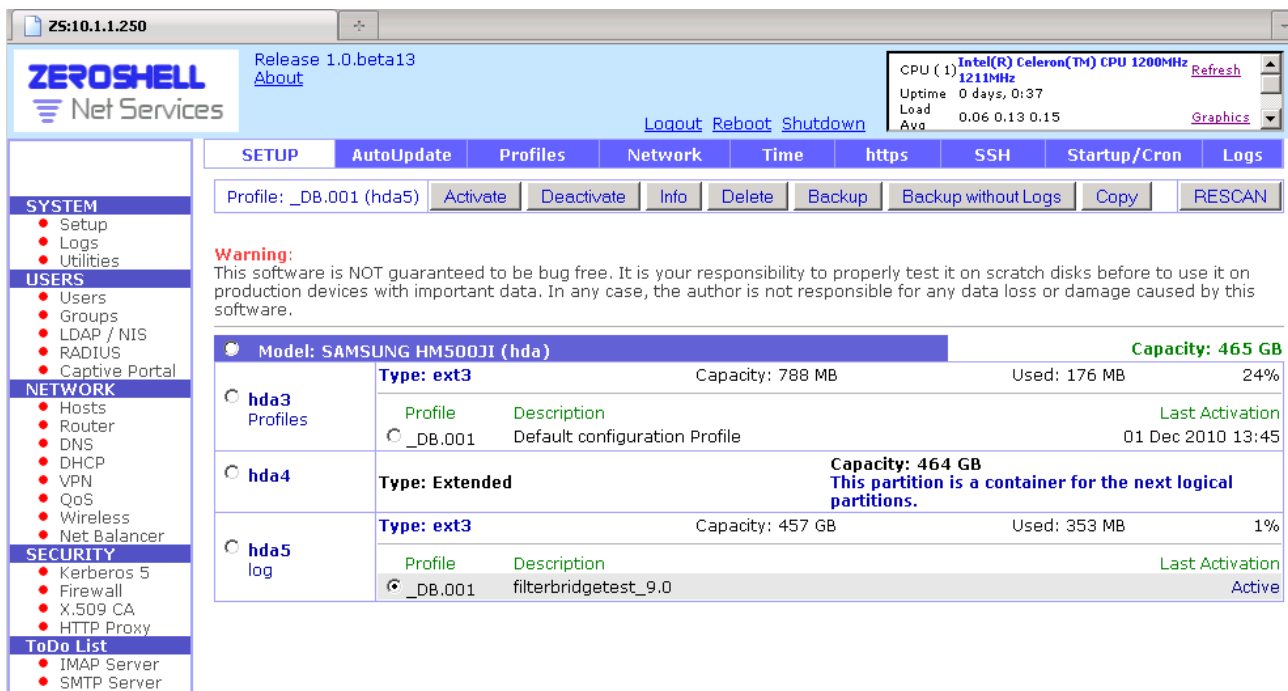


You will see this dialog box, fill in all missing entries.



You can choose the ethernet port you want to use for the webinterface here, it can be part of the bridge later too, but not necessarily. Assign the desired ip-address, netmask and default gateway. Then click on „Create“.

Now you are back in the Profiles menu, select your new created Profile, and click on „Activate“



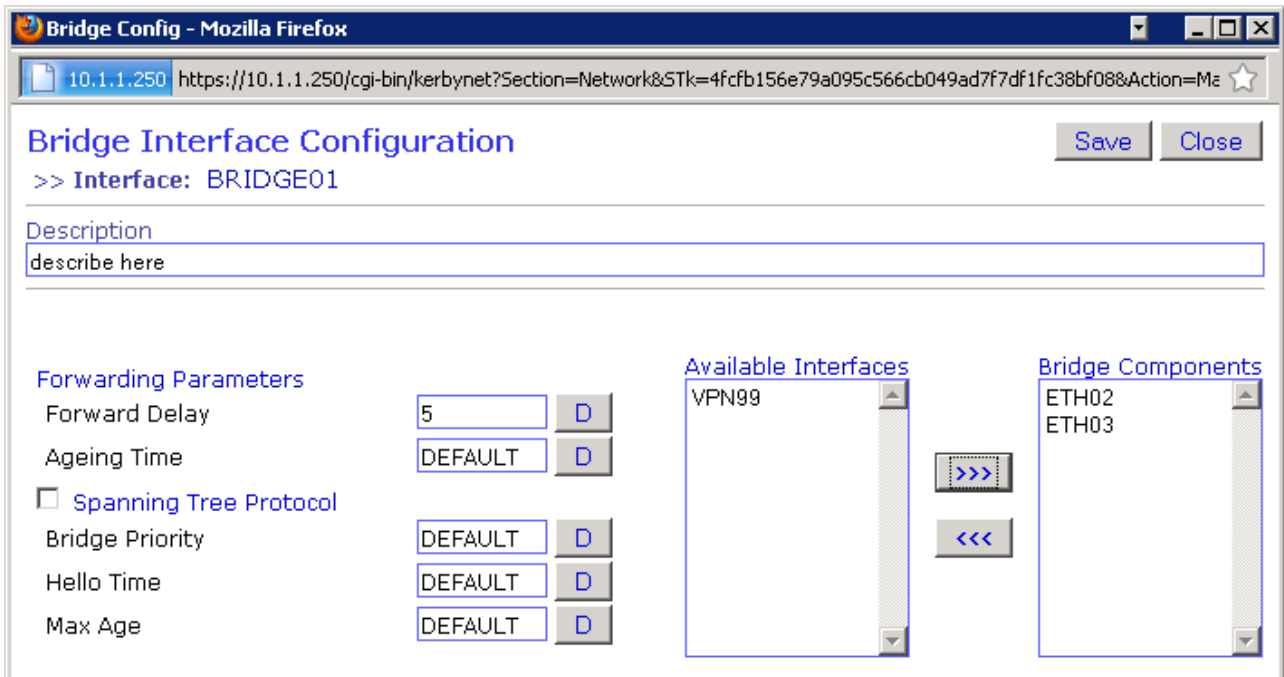
After activating the new Profile, zeroshell will reboot!

If all went well, it should come back up with your new settings for IP-address and password.. Don't forget to set your PC's network parameters accordingly, if necessary.

After logging in, click again on „Setup“, then „Network“

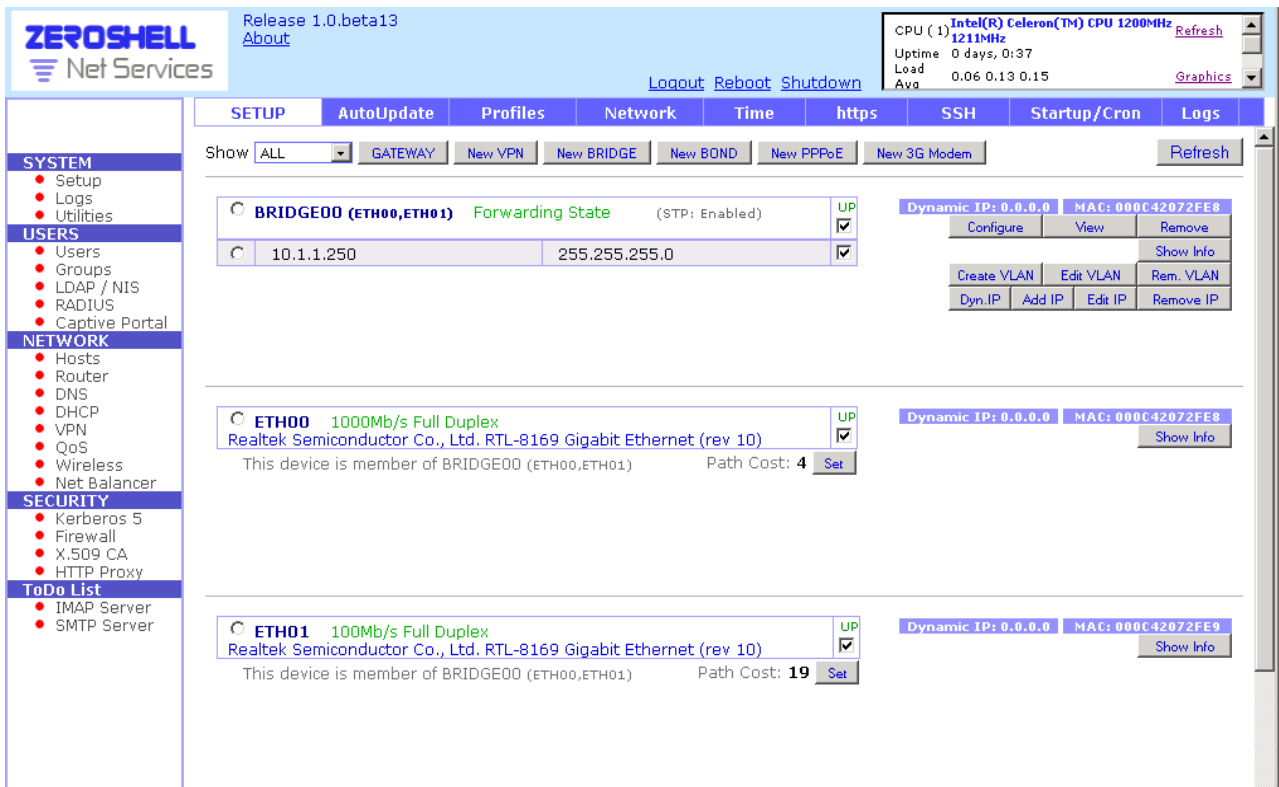
Now click on „New Bridge“

Choose the interfaces you want to add to your filtering bridge, and give that child a name!



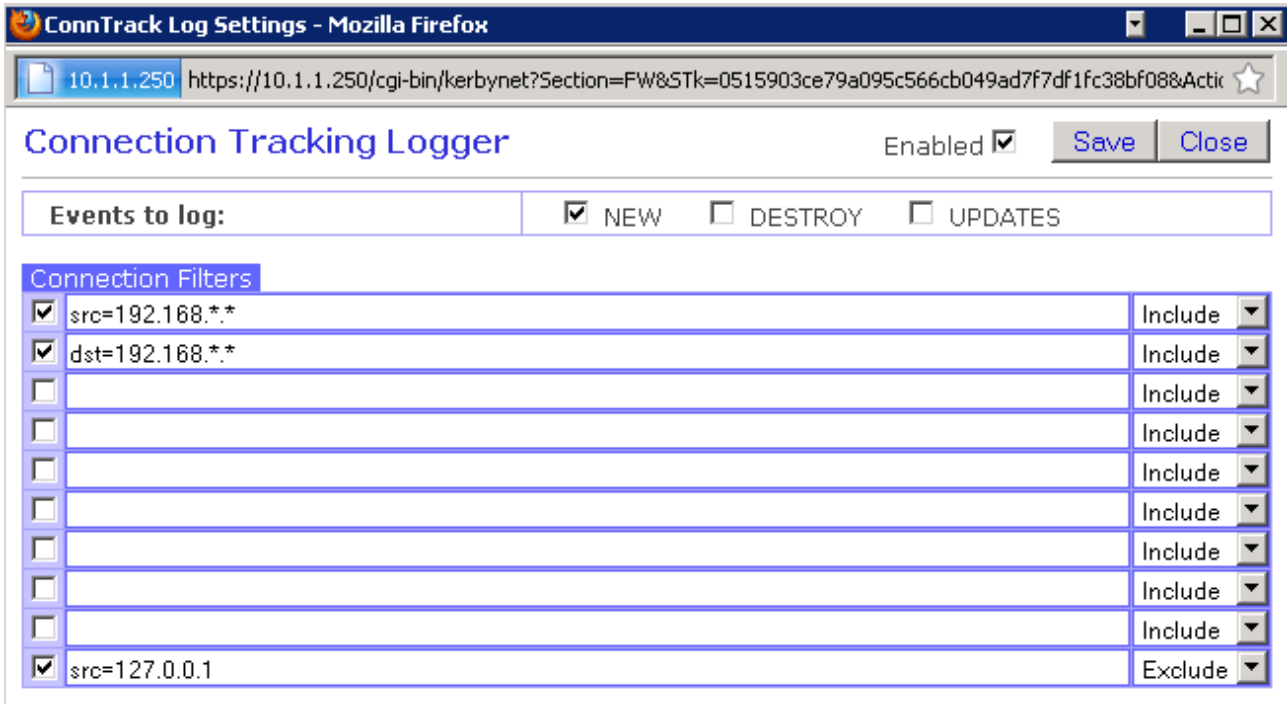
After clicking on „Save“, you will have your newly made bridge ready.

If none of the chosen bridge interfaces had an Ip-address, you can give the bridge an IP now (Not necessary for the purpose, but might come in handy for configuration from any PC in the bridge network (or a potential security risk, as someone could access the webinterface from that network, which he could not, if it had no IP assigned at all... decide for yourself))



In my scenario where this zeroshell is in use, I have a Network 192.168.0.0/24 for users, and a 10.1.1.0/24 for Administration. Since non of my users has Admin rights, they won't change their IP-addresses and therefore won't pose a risk to security (And if anyone tried, my cattleprod is charged and ready... ;)

Now for the connection tracking, click on „Security/Firewall“, then on „Connection Tracking“, then „Configure“.



It took me some time, to figure out the correct syntax, since everywhere i looked for contrack syntax, it told me something along the lines of „192.168.0.0/24“ or similar. But with trial and error I found out, the Asterisk is used for „any“, hence „src=192.168.*.*“ means source of connection inside 192.168.0.0 to 192.168.255.255. If you only want to have one /24 subnet, just do something like: „src=192.168.0.*“ The same works for destination of connection, of course. Make sure you activate „Connection Tracking Logger“ on top too, then „Save“.

Now your log will fill with entries, if traffic passes through your filtering bridge.

BTW, the built in Syslog is able to provide logging services for other devices in your network too, just set it in the LOG tab accordingly. Or you can send your logfiles to another log-server, if you already have one.

Transparent Proxy with Web Antivirus

For Antivirus proxy, you have to click on “Security/HTTP Proxy“

The screenshot displays the Zeroshell Net Services web interface. At the top, it shows the release version (1.0.beta13) and system information including CPU (Intel(R) Celeron(TM) CPU 1200MHz), uptime (0 days, 2:37), and load averages (1.77 0.95 0.43). The main navigation menu includes SYSTEM, USERS, NETWORK, and SECURITY. The 'HTTP PROXY' section is active, showing the configuration for 'Transparent Proxy with Web Antivirus'. The status is 'DOWN' and the proxy is not enabled. The configuration includes HTTP Capturing Rules (Rule: ETH01, Action: Capture), HAVP Configuration (Access Logging: Only URL containing Virus), ClamAV Antivirus Configuration (Virus Scanning: Enabled, Check Images: Disabled, AutoUpdate Virus Signatures: Enabled, Number of Checks per Day: 12, Country of the Mirror: Germany), and URL Management (Blacklist and Whitelist: Disabled).

There were some downloads running using htrack to simulate traffic (2000 connections, about 8 to 15 MBit/s) while i wrote this script, and the „Server“ running zeroshell is not powerful enough to do Antivirus for 10+ Mbit/s, (as u can see on the load AVG, I switched Antivirus on for a short time, and it went through the roof, while contrack with logging is using between 20 and 30 % of it's processors power.

ETH01 is the Network interface facing our internal network, so I chose it for HTTP Capturing Rules. After setting that up, you just need to click on „Enabled“, and then „Save“. Now the Antivirus updates should be downloaded, given your bridge has access to the internet. After a while it will change it's status from down to up (may need a refresh of your browser, to show correctly.)

But as mentioned above, be careful with the load Antvirus may imply to your processor. An embedded board like Alix or a slow cpu as the one I used for testing will not be able to scan a lot of traffic and slow your internet connection down.

There is a post in the forum, indicating a possible speedup for havp proxy, look here:

<http://www.zeroshell.net/eng/forum/viewtopic.php?t=1916>

But even with this patch, my test-zeroshell was not able to scan as fast as I desired. I guess there's no alternative to MORE CPU POWER AND RAM.

Bandwithd

A nice feature is Bandwithd, which is accessible through „Router / Bandwithd“

Status on Subnets **ACTIVE**

Thu Dec 2 09:08:48 2010



Programmed by David Hinkle, Commissioned by [DerbyTech](#) wireless networking

- [Daily](#) -- [Weekly](#) -- [Monthly](#) -- [Yearly](#) -

Pick a Subnet:

- [Top20](#) -- [192.168.0.0](#) -- [192.168.100.0](#) -- [192.168.99.0](#) -

Top 20 IPs by Traffic - Daily

Ip and Name	Total	Total Sent	Total Received	FTP	HTTP	P2P	TCP	UDP	ICMP
Total	10.1G	754.3M	9.4G	175.1K	7.4G	2.4M	9.5G	534.0M	17.9M
192.168.0.57	1.9G	51.1M	1.8G	0	98.0M	28.5K	1.9G	4.7M	186.0K
192.168.0.187	1.4G	43.4M	1.4G	0	1.4G	0	1.4G	1.4M	3.1K
192.168.0.39	1.2G	26.2M	1.2G	0	1.2G	143.7K	1.2G	311.0K	7.7K

You have to Enable it, choose the interface it will monitor for you, then choose the subnets you want to log like „192.168.0.0/24“, if you want to monitor more than one, just separate them with a space, then click on „Save“. After approx. 5 minutes the list and graphs will begin to show which IP is hogging how much bandwidth at any given time. You can choose daily, weekly, monthly or yearly view, top 20 up/downloaders or whole subnets with all IP's producing traffic.

If you have a bridge in your system enabled, the choice of „ANY“ Interface is not a good one, since all your traffic will be counted twice, your numbers will be double the REAL throughput. Not sure if the same happens with NAT / Routing enabled, since I cannot test it quite now.

Jens Reinacher