Setting up an OpenBSD Firewall in the ASU Environment

Installation

First you will need to download and install OpenBSD on a computer with the following Requirements:

The minimum requirements for the OpenBSD machine are as follows:

- 133MHz or higher x86 class processor
- 64 MB of RAM
- 1 GB hard drive space
- 2 NICs (High quality recommended, e.g., Intel, 3Com)
- Switch—Optional if you want a setup for more than one server/PC
- Scratch paper
- Network Cables
- A lot of patients

An updated list of system requirements for the OS can be found here:
http://www.openbsd.org/i386.html#hardware

If you want to install open BSD with the minimal amount of media, you can download the CD ISO from ftp.openbsd.org/pub/OpenBSD/3.8/i386

Here is information for more advanced users

floppy38.fs (Desktop PC) supports many PCI and ISA NICs, IDE and simple SCSI adapters and some PCMCIA support. Most users will use this image if booting from a floppy. Requires the Rawrite utility
floppyB38.fs (Servers) supports many RAID controllers, and some of the less common SCSI adapters. However, support for many standard SCSI adapters and many EISA and ISA NICS has been removed. Requires the Rawrite utility
floppyC38.fs (Laptops) supports the CardBus and PCMCIA devices found in many laptops. Requires the Rawrite utility
cdrom38.fs is, in effect a combination of all three boot disks. It can be used to make a bootable 2.88M floppy, or more commonly, as a boot image for a custom recordable CD. Requires the Rawrite utility
cd38.iso is an ISO9660 image that can be used to create a bootable CD with most popular CD-ROM creation software on most platforms. This image has the widest selection of drivers, and is usually the recommended choice if your hardware can boot from a CDROM.
cdemu38.iso is an ISO9660 image, using "floppy emulation" booting, using the 2.88M image, cdrom37.fs. It is hoped that few people will need this image -- most people will use cd37.iso, only use cdemu37.iso if cd37.iso doesn't work for you.

Note: Currently version 3.8 is the latest version as of this writing.
You can also use a floppy image using rawrite, and if you know your exact system requirements.

Verify that you have registered both NIC's so you can obtain a valid IP address.
Burn the ISO image with your favorite utility.
Verify your BIOS is setup for the CDROM to be the first boot device
Boot off the CDROM.

If you are having problems, more detailed instructions for the following can be found at:
http://www.openbsd.org/faq/faq4.html#Start

There will be a slight delay when you see “Boot>” Wait 5 seconds or depress the Enter key
You will be prompted for (I)nstall, (U)pgrade or (S)hell
Depress the <I> key, then <enter>

Terminal Type? [vt220]
<enter>
Kbd(8) mapping? (‘?’ for list) [none]
<enter>

Proceed with install? [no]
Type **yes <enter>**

If you are having problems, more detailed instructions for the following can be found at:
http://www.openbsd.org/faq/faq14.html#disklabel

Available disks are: ##### ← Whatever your hard drive is.
Which one is the root disk? (or ‘done’)
<enter>
Do you want to use *all* of ### for OpenBSD? ← This is up to you, I typed **yes** to make it easy <enter>

Note: if you want to see the current label setup type **p <enter>**

Type in the following commands:

d a <enter> ← This deletes the current setup
a a <enter> ← This creates your new labels

offset: [##] **<enter>** ← Accept the default for the starting sector of the partition
size: [######] ## ← This is the size of your partition. If you don’t speak sector or partitioneze add a G at the end (example type 69G for 69 Gigabytes, it’s nicer than typing 142253248.
Rounding to nearest cylinder: ###### ← Accept the default for
FS type: [4.2BSD] **<enter>** ← You can use 4.2BSD or type swap if you intend to create a swap partition due to lack of RAM
mount point: [none] / ← This is where you type in the name of the filesystem (ie. /, /var, /usr, /tmp…etc etc). Choose / for the main partition
fragment size: [2048] ← This is the size of fs block fragments, usually 2048 or 512. If you’re unsure, select the default.
block size: [16384] ← This is the size of filesystem blocks. Usually 16384 or 4096. If you’re unsure, select the default.
cpg: [16] ←Number of file system cylinders per group. Usually 16 or 8. If you’re unsure, select the default.

If you left some space for a swap partition
Type **a b <enter>**

offset: [##] **<enter>** ← Accept the default for the starting sector of the partition
size: [######] ## ← This is the size of your partition. If you don’t speak sector or partitioneze add an G at the end (example type 69G for 69 Gigabytes, it’s nicer than typing 142253248. M=Megabytes
FS type: [swap] **<enter>** Type swap if it isn’t already there by default.

Double check your work with by typing **p <enter>**

Note: if you want to see the current label setup and see the disk size in Megabytes
type p m <enter>

Type **q <enter>** ← This will save your changes and take you to the next step of the installation.

The next step *DESTROYS* all existing data on these partitions!
Are you really sure that you're ready to proceed? [no]
Type **yes <enter>**

System hostname (short form, e.g. 'foo') ← Make up a short computer name for your firewall.
Configure the network? [yes]
<enter>
Available Interfaces are: #### #### ← Make note of the interface names, you will need them later.
Which one do you wish to initialize? (or 'done') [####]
<enter>
Symbolic (host) name for ###? [#####]
<enter>
Do you want to change the media options? [no]
<enter>
Ipv4 address for ##? (or 'none' for 'dhcp')
Type **dhcp <enter>**
Ipv6 address for ###? (or 'rstool' or 'none') [none]
<enter>
Which one do you want to initialize? (or 'done') [###]
<enter>
Symbolic (host) name for ###? [#####]
<enter>
Do you want to change the media options? [no]
<enter>
Ipv4 address for ##? (or 'none' for 'dhcp')
Type dhcp <enter>
Ipv6 address for ###? (or 'rstool' or 'none') [none]
<enter>
Which one do you want to initialize? (or 'done') [###]
<enter>
Symbolic (host) name for ###? [#####]
<enter>
Do you want to change the media options? [no]
<enter>
Ipv4 address for ##? (or 'none' for 'dhcp')
Type **dhcp <enter>**

DNS domain name? (e.g. 'bar.com') [dhcp.asu.edu] ← This field should be filled in. If not, type it in.
<enter>
DNS nameserver? (IP address or 'none') [129.219.17.200 129.219.17.5 129.219.13.81] ← This field should be filled in. If not, type it in.
Use the nameserver now? [yes]
<enter>

Default Ipv4 route? (Ipv4 address, ‘dhcp’ or ‘none’) [dhcp]
<enter>
Edit hosts with ed? [no]
<enter>
Do you want to do any manual network configuration? [no]
<enter>
Password for root account? (will not echo) ← Type in a good Alphanumeric Password! Remember ASU Security Awareness week ☺
<enter>
Let’s install the sets!
Location of sets? (cd disk ftp http or ‘done’) [cd]
This is where you have multiple options, I personally like getting it directly off the internet.
Type http <enter> ← I chose http, because it is the simplest installation. For newbies, simple is good!!!
HTTP/FTP proxy URL? (e.g. ‘http://proxy:8080’, or ‘none’) [none]
<enter>
Display the list of known http servers? [yes]
<enter>
After you’ve decided on your favorite server, scroll down or press q. Then type in the number.
Note: You may have to fiddle with the locations a few times. Some don’t have the latest versions of BSD ☹
Now you will select the sets that you want installed.

Select the sets by entering a set name, a file name pattern or ‘all’. De-select sets by prepending a ‘-‘ to the set name, file name pattern or ‘all’. Selected sets are labeled ‘[x]’.

[ ] bsd
[ ] bsd.rd
[ ] bsd.mp
[ ] base38.tgz
[ ] etc38.tgz
[ ] misc38.tgz
[ ] comp38.tgz
[ ] man38.tgz
[ ] game38.tgz
[ ] xbase38.tgz
[ ] xetc38.tgz
[ ] xshare38.tgz
[ ] xfont38.tgz
[ ] xserv38.tgz

Set name? (or ‘done’)

Note: Here are the descriptions of what each set really is:

bsd - This is the Kernel.	*Required*
bsd.rd - RAM disk kernel	*Optional*
bsd.mp - Multi-processor (SMP) kernel (only some platforms)	*Depends on your hardware*
base38.tgz - Contains the base OpenBSD system	*Required*
etc38.tgz - Contains all the files in /etc	*Required*
misc38.tgz - Contains misc info, setup documentation	*Optional*
comp38.tgz - Contains the compiler and its tools, headers and libraries.	*Recommeded*
man38.tgz - Contains man pages	*Recommeded*
game38.tgz - Contains the games for OpenBSD	*Not Required for our firewall*

xbase38.tgz - Contains the base install for X11	*Not Required for our firewall*
xetc38.tgz - Contains the /etc/X11 and /etc/fonts configuration files	*Not Required for our firewall*
xshare38.tgz - Contains manpages, locale settings, includes, etc. for X	*Not Required for our firewall*
xfont38.tgz - Contains X11's font server and fonts	*Not Required for our firewall*
xserv38.tgz - Contains X11's X servers	*Not Required for our firewall*

Examples of how to add items is type the name (example, type **bsd.mp**)
To remove put a – in front of the name (example, type **–game38.tgz**)

When you're done type **done <enter>**

Ready to install sets? [yes]
<enter>

********** **Break time!!! Go take a break and have some coffee**. **********

Location of sets? (cd disk ftp http or 'done') [cd]
Type **done <enter>**
Start sshd(8) by default? [yes] ← This is used if you wish to remotely administer the firewall via ssh. The choice is yours type yes or no.
Start ntpd(8) by default? [no] ← This is the Network Time Daemon. This is handy if you want to keep accurante times and and setup a syslog server.
Do you expect to run the X Window System [yes] ← Since this is a firewall, the GUI is not required.
Change the default console to com0? [no] ← This option is not recommended since you already have a keyboard, mouse, and monitor connected.
What timezone are you in? ('?' for list) [Canada/Mountain]
Type **America <enter>**
What sub-timezone of 'America' are you in? ('?' for list)
Type **Phoenix <enter>**
Making all Device Nodes…done. ← You will have to wait a few minutes.

CONGRADULATIONS!!! Your OpenBSD install has been successfully completed!
To boot the new system, enter halt at the command prompt. Once the system has halted, reset the machine and boot from the disk.
<Remove your cdrom or floppy>
Type **halt <enter>**
<Reboot your computer>

After you have rebooted, enter your username and password.
Terminal Type? [vt220]
<enter>

If you are a VI editor and FTP pro, then you can skip the next part.

The basic ftp program doesn't offer many feature and the VI editor has enough special keystrokes to make most peoples eyes glaze over. I recommend installing the Pico editor and the NCFTP program. To install these programs follow these instructions:

Type **ftp ftp.openbsd.org <enter>**
Name (ftp.openbsd.org:root):
Type **anonymous <enter>**
Password:
Type anything then press **<enter>**
ftp>
type **cd /pub/OpenBSD/3.8/packages/i386**
ftp>
type **binary <enter>**
200 switching to Binary mode
ftp>
type **get pico-4.10.tgz <enter>**
ftp>
type **get ncftp-3.1.9.tgz <enter>**
ftp>
type **bye <enter>**
Note: To verify you received the packages type **ls <enter>**
You should see the packages you downloaded in your directory.
Now type **pkg_add pico-4.10.tgz <enter>**
Pkg_add pico-4.10: complete
Now type **pkg_add ncftp-3.1.9.tgz <enter>**
Pkg_add ncftp-3.1.9: complete

You now have a new text editor and a kick'n FTP program.

To run each of them type either ncftp or pico.

Example:
Type **pico t.txt <enter>**

or

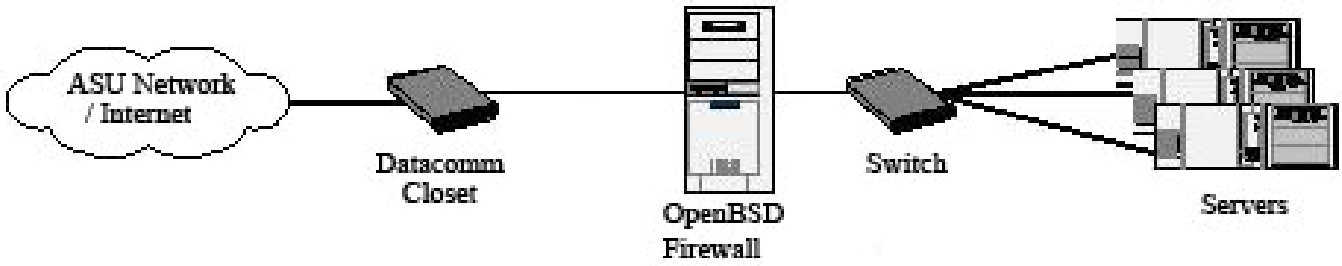
type **ncftp ftp.openbsd.org**

Creating a Bootable CDROM Firewall *<Optional>*

Not yet documented

Topology

The following diagram shows the inclusion of a PC running OpenBSD that has been inserted inline between the ASU Network and the switch.
The finished network topology will look like the diagram below.



Type **ifconfig**
Make note of the interface names on scratch paper (ie lo0, fxp0, fxp1,dxp0, etc, etc). Do not use more than two NICs. You will run into problems bridging.

Setting up the bridge

Note: for the rest of these instructions we are going to assume that your NIC's are fxp0 and fxp1. They may be called something else. Make changes where appropriate. We are also going to assume that you are using 100 MB NIC cards. Again make changes where appropriate.

Edit the /etc/sysctl.conf and uncomment (remove the #) from the line that reads:
net.inet.ip.forwarding=1

Note: Datacomm sometimes has problems with their switches auto-negotiating. We are going to set the NICs to stay at 100 Mb. This can cause problems if you plug in your servers to a 10 Mb connection (Why would you do that?!?). The *Inet media 100BaseT* is optional.

If you configured the NICs during installation delete them with the next two commands.

ifconfig fxp0 delete
ifconfig fxp1 delete

Create **/etc/hostname.fxp0**
In the file type in the following information:

Inet media 100BaseT
up

Create **/etc/hostname.fxp1**
In the file type in the following information:

Inet media 100BaseT
up

Create **/etc/bridgename.bridge0**
In the file type in the following information:

Add fxp0 add fxp1 up

Edit the /etc/resolve.conf file and verify the following information is there. If not, the type it in. (Although if you used dhcp, this should already be in there). If you want to add your own DNS servers, then create /etc/resolve.conf.tail and add your own entries. Otherwise, the DHCP will wipe out the entries on the next boot.

lookup file bind
nameserver 129.219.17.5
nameserver 129.219.17.200
nameserver 129.219.13.81

Note: We are putting the DNS entries in the host file because the DNS entries in the firewall may not work at boot time.

Reboot the computer with the following command:
shutdown –r now

Verify that the bridge is running by typing
ifconfig -a

In part of the output you should see the following line, if not then bridging isn't working:

bridge0: flags=41 <UP,RUNNING> mtu 1500

Enabling the Firewall

Edit the **/etc/rc.conf.local**

Note: Although you can edit the /etc/rc.conf file, it contains the system defaults, and should not be altered. Instead you can make your “overridden” changes in /etc/rc.conf.local, and the system will read the last, and update any changes you had made in it.

Add the following lines to the /etc/rc.conf.local file

pf=YES

Here are common terms you may see when configuring your firewall:

lo	- Loopback Interface
pflog	- Packet Filter Logging Interface
sl	- SLIP Network Interface
ppp	- Point to Point Protocol
tun	- Tunnel Network Interface
enc	- Encapsulating Interface
bridge	- Ethernet Bridge Interface
vlan	- IEEE 802.1Q Encapsulation Interface
gre	- GRE/MobileIP Encapsulation Interface
gif	- Generic IPv4/IPv6 Tunnel Interface
carp	- Common Address Redundancy Protocol Interface

FAQs:

After I type in the timezone, the computer locks up.
Some hardware, (Especially Compaq servers!!) may have problems.

My Bridge isn't working.
If you have NICs with the TI ThunderLAN chip, then this is the problem. OpenBSD does not support bridging with them.

Additional Commands:

To test a ruleset
Write your rules and save them in pf.test

To test your rules type
```
pfctl -n -v -f /etc/pf.test
```

When you are confident that you want to apply the rules type
```
cp pf.conf pf.old && cp pf.test pf.conf
```

To load your rules type
```
pfctl -v -R /etc/pf.conf
```

To show how many states are running concurrently type
```
pfctl -s info
```

To enable logging on the external interface type
```
pfctl -l rl0
```

To see rejected packets scroll on the screen type
```
tcpdump -n -e -ttt -i pflog0
```

To show the amount of free disk space type
```
df -h
```

To show the amount of CPU utilization type
```
top
```

Type Ctrl-Z to push the current job into the background and fg to return it to the forground. Ctrl-C kills the job running in the forground.

To mount a floppy type
```
mount -t msdos /dev/fd0a /mnt
```

To copy a file to floppy type
```
cp <filename> /mnt
```

To unmount the floppy type
```
umount /mnt
```

Note: Make sure your default directory isn't on /mnt when you do this or it won't unmount.

To display your current default directory type
pwd

To clear the display type
clear