Securing Your Network with pfSense

ILTA-U
Dale Qualls
Pattishall, McAuliffe, Newbury, Hilliard & Geraldson LLP
dqualls@pattishall.com
Housekeeping

• Please turn off cell phones or put them on silent
• We’re recording this session to share with those that were unable to attend... If you have a question please wait for the microphone to make it to you.
• Please fill out the survey after the session
Housekeeping

• 2 Hyper-V virtual machines
  – To release the mouse the right ALT, CTRL and Left Arrow simultaneously

• Helpers are here for you
What is pfSense

- Firewall
- Router
- Load balancer (bi-directional)
- VPN solution
- Internet filter
- Usage monitor
- Provides a Captive portal capabilities
• Based on FreeBSD PF (Packet Filter) project, ported from OpenBSD to FreeBSD in 2004
• Forked from the m0n0wall project in 2004 by Chris Buechler and Scott Ullrich
• Focus is not running on embedded systems but an embedded offering is available.

Beastie the Daemon
What’s in a name?

• pfSense
  - pf (from the original project name)
  - Sense, as in making sense of pf

• Domain name availability, or lack thereof, helped dictate the name.
  - was though by some to stand for “Plain F...... Sense”.

$35 at Amazon
I will be giving one away today!
FreeBSD is used as a platform for devices and products from many of the world's largest IT companies, including:

- Apple
- Cisco
- Juniper Networks
- NetApp
FreeBSD runs some of the busiest sites on the Internet!
How do I get started? What do I need

• Properly sized hardware:
  – 100MHz Pentium CPU
  – 128 MB of RAM

• Requirements specific to individual platforms follow.
  – Live CD
    CD-ROM drive
    USB flash drive or floppy drive to hold configuration file
  – Hard drive installation
    CD-ROM for initial installation
    1 GB hard drive
  – Embedded
    128 MB Compact Flash card
    Serial port for console
Let’s Get Started!

Open Hyper-V
Welcome to pfSense 1.2.3-RELEASE...

Mounting filesystems... done.
Creating symlinks.....done.
Launching the init system... done.
Initializing............... done.
Starting device manager (devd)...done.

[ Press R to enter recovery mode or ]
[ press I to launch the installer ]

(R)ecovery mode can assist by rescuing config.xml
from a broken hard disk installation, etc.

Alternatively the (I)installer may be invoked now if you do
not wish to boot into the liveCD environment at this time.

Timeout before auto boot continues (seconds): 9
Your selected environment uses the following console settings, shown in parentheses. Select any that you wish to change.

- Change Video Font (armscii8-8x14)
- Change Screenmap (default)
- Change Keymap (default)
- Accept these Settings
Select Task

Choose one of the following tasks to perform.

< Quick/Easy Install >
< Custom Install >
< Rescue config.xml >
< Reboot >
< Exit >

Invoke Installer with minimal questions

Status: Running
Are you SURE?

Easy Install will automatically install without asking any questions.

WARNING: This will erase all contents in your first hard disk! This action is irreversible. Do you really want to continue?

If you wish to have more control on your setup, choose Advanced Installation from the Main Menu.

< OK >  < Cancel >
/sbin/bsdlabel -B ad0s1
You may now wish to install a custom Kernel configuration.

< Symmetric multiprocesssing kernel (more than one processor) >
< Uniprocessor kernel (one processor) >
< Embedded kernel (no vga console, keyboard) >
< Developers kernel (includes GDB, etc) >

Press F1 for Help
Executing Commands

tar xzpf /kernels/kernel_uniprocessor.gz -C /mnt/boot/

[ 0% ]

< Cancel >
This machine is about to be shut down. After the machine has reached its shutdown state, you may remove the CD from the CD-ROM drive tray and press Enter to reboot from the HDD.

< Reboot >  < Return to Select Task >
pfSense is now rebooting

After the reboot is complete, open a web browser and enter http://192.168.1.1 (or the LAN IP Address) in the location bar.

*DEFAULT Username*: admin
*DEFAULT Password*: pfsense

Rebooting in 5 seconds. CTRL-C to abort.
Rebooting in 4 seconds. CTRL-C to abort.
Rebooting in 3 seconds. CTRL-C to abort.
Rebooting in 2 seconds. CTRL-C to abort.
Welcome to pfSense 1.2.3-RELEASE...

Mounting filesystems... done.
Creating symlinks......done.
Launching the init system... done.
Initializing................ done.
Starting device manager (devd)...done.
Loading configuration.......done.

Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

de0  
00:15:5d:0a:7c:14

de1  
00:15:5d:0a:7c:15

Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y/n]?
Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

de0  00:15:5d:0a:7c:14
de1  00:15:5d:0a:7c:15

Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y/n]? n

*NOTE* pfSense requires *AT LEAST* 2 assigned interfaces to function. If you do not have two interfaces you CANNOT continue.

If you do not have at least two *REAL* network interface cards or one interface with multiple VLANs then pfSense *WILL NOT* function correctly.

If you do not know the names of your interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection:
Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

de0  00:15:5d:0a:7c:14
de1  00:15:5d:0a:7c:15

Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y/n]? n

*NOTE*  pfSense requires *AT LEAST* 2 assigned interfaces to function.
If you do not have two interfaces you CANNOT continue.

If you do not have at least two *REAL* network interface cards or one interface with multiple VLANs then pfSense *WILL NOT* function correctly.

If you do not know the names of your interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection: de0
Network interface mismatch -- Running interface assignment option.

Valid interfaces are:

de0 00:15:5d:0a:7c:0b
de1 00:15:5d:0a:7c:0c

Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y/n]?

*NOTE* pfSense requires *AT LEAST* 2 assigned interfaces to function.
If you do not have two interfaces you CANNOT continue.

If you do not have at least two *REAL* network interface cards or one interface with multiple VLANs then pfSense *WILL NOT* function correctly.

If you do not know the names of your interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection: de0
Valid interfaces are:

de0     00:15:5d:0a:7c:0b  
de1     00:15:5d:0a:7c:0c

Do you want to set up VLANs first?
If you are not going to use VLANs, or only for optional interfaces, you should say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y/n]? n

*NOTE*  pfSense requires *AT LEAST* 2 assigned interfaces to function. If you do not have two interfaces you CANNOT continue.

If you do not have at least two *REAL* network interface cards or one interface with multiple VLANs then pfSense *WILL NOT* function correctly.

If you do not know the names of your interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto-detection.

Enter the LAN interface name or 'a' for auto-detection: de0

Enter the WAN interface name or 'a' for auto-detection: de1
Do you want to set up VLANs first? If you are not going to use VLANs, or only for optional interfaces, you should say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now? [y/n]? n

*NOTE* pfSense requires AT LEAST 2 assigned interfaces to function. If you do not have two interfaces you CANNOT continue.

If you do not have at least two REAL network interface cards or one interface with multiple VLANs then pfSense WILL NOT function correctly.

If you do not know the names of your interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection: de0

Enter the WAN interface name or 'a' for auto-detection: de1

Enter the Optional 1 interface name or 'a' for auto-detection (or nothing if finished):
**NOTE**  pfSense requires *AT LEAST* 2 assigned interfaces to function. If you do not have two interfaces you CANNOT continue.

If you do not have at least two *REAL* network interface cards or one interface with multiple VLANs then pfSense *WILL NOT* function correctly.

If you do not know the names of your interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto detection.

Enter the LAN interface name or 'a' for auto-detection: de0

Enter the WAN interface name or 'a' for auto-detection: de1

Enter the Optional 1 interface name or 'a' for auto-detection (or nothing if finished):

The interfaces will be assigned as follows:

LAN  ->  de0
WAN  ->  de1

Do you want to proceed [y/n]?
Enter the LAN interface name or 'a' for auto-detection: em1

Enter the WAN interface name or 'a' for auto-detection: em0

Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

LAN  -> em1
WAN  -> em0

Do you want to proceed [y/n]? y

Updating configuration...done.
Cleaning backup cache...done.
Setting up extended sysctls...done.
Syncing user passwords...done.
Starting Secure Shell Services...done.
Setting timezone...done.
Setting up microcode and tx/rx offloading...done.
Configuring LAN interface...done.
Configuring WAN interface...
Welcome to pfSense 1.2.3-RELEASE-pfSense on pfSense

LAN* -> de0 -> 192.168.1.1
WAN* -> de1 -> 10.5.32.208 (DHCP)

pfSense console setup

0) Logout (SSH only)
1) Assign Interfaces
2) Set LAN IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) PFtop
10) Filter Logs
11) Restart webConfigurator
12) pfSense Developer Shell
13) Upgrade from console
14) Enable Secure Shell (sshd)

Enter an option: 8

Status: Running
pfSense console setup

0) Logout (SSH only)
1) Assign Interfaces
2) Set LAN IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) PFtop
10) Filter Logs
11) Restart webConfigurator
12) pfSense Developer Shell
13) Upgrade from console
14) Enable Secure Shell (sshd)

Enter an option: 8

# ifconfig de0 down
# ifconfig de1 down
# ifconfig de0 up
# ifconfig de1 up
ifconfig de0 down
ifconfig de0 up
ifconfig de1 down
ifconfig de1 up
Hardware Sizing

• When sizing hardware for use with pfSense, two main factors need to be considered.
  – Throughput required
  – Features that will be used

• Throughput Considerations
  – If you require less than 10 Mbps of throughput, you can get by with the minimum requirements. For higher throughput requirements we recommend following these guidelines, based on our extensive testing and deployment experience. These guidelines offer a bit of breathing room because you never want to run your hardware to its full capacity.
Hardware Sizing

• 10-20 Mbps - No less than 266 MHz CPU
• 21-50 Mbps - No less than 500 MHz CPU
• 51-200 Mbps - No less than 1.0 GHz CPU
• 201-500 Mbps - server class hardware with PCI-X or PCI-e network adapters, or newer desktop hardware with PCI-e network adapters. No less than 2.0 GHz CPU.
• 501+ Mbps - server class hardware with PCI-X or PCI-e network adapters. No less than 3.0 GHz CPU.
Hardware Sizing

• Feature Considerations
  - Most features do not factor into hardware sizing, though a few have significant impact on hardware utilization.
  - **VPN** - Heavy use of any of the VPN services included in pfSense will increase CPU requirements. Encrypting and decrypting traffic is CPU intensive. The number of connections is much less of a concern than the throughput required. A 266 MHz CPU will max out at around 4 Mbps of IPsec throughput, a 500 MHz CPU can push 10-15 Mbps of IPsec, and relatively new server hardware (Xeon 800 FSB and newer) deployments are pushing over 100 Mbps with plenty of capacity to spare. Supported encryption cards, such as several from Hifn, are capable of significantly reducing CPU requirements.
Hardware Sizing

- **Captive portal** - While the primary concern is typically throughput, environments with hundreds of simultaneous captive portal users (of which there are many) will require slightly more CPU power than recommended above.

- **Large state tables** - State table entries require about 1 KB of RAM each. The default state table, when full at 10,000 entries, takes up a little less than 10 MB RAM. For large environments requiring state tables with hundreds of thousands of connections, ensure adequate RAM is available.

- **Packages** - Some of the packages increase RAM requirements significantly. Snort and ntop are two that should not be installed on a system with less than 512 MB RAM.
Hardware Compatibility List

- pfSense 1.2.3 is based on FreeBSD 7.2, its hardware compatibility list is the same as FreeBSD's.
- The pfSense kernel includes all FreeBSD drivers.
- Visit freebsd.org for the HCL.
  - http://www.freebsd.org/releases/7.2R/hardware.html
Firewall Features

• Firewall
  - Filtering by source and destination IP, IP protocol, source and destination port for TCP and UDP traffic
  - Able to limit simultaneous connections on a per-rule basis
  - pfSense utilizes p0f, an advanced passive OS/network fingerprinting utility, to allow you to filter by the Operating System initiating the connection. Want to allow FreeBSD and Linux machines to the Internet, but block Windows machines? pfSense can do so (amongst many other possibilities) by passively detecting the Operating System in use.
  - Option to log or not log traffic matching each rule.
Firewall Features

- Highly flexible policy routing possible by selecting gateway on a per-rule basis (for load balancing, failover, multiple WAN, etc.)
- Aliases allow grouping and naming of IPs, networks and ports. This helps keep your firewall ruleset clean and easy to understand, especially in environments with multiple public IPs and numerous servers.
- Transparent layer 2 firewalling capable - can bridge interfaces and filter traffic between them, even allowing for an IP-less firewall (though you probably want an IP for management purposes).
Firewall Features

• Packet normalization
  - 'Scrubbing' is the normalization of packets so there are no ambiguities in interpretation by the ultimate destination of the packet. The scrub directive also reassembles fragmented packets, protecting some operating systems from some forms of attack, and drops TCP packets that have invalid flag combinations.
  - Enabled in pfSense by default
  - Can disable if necessary. This option causes problems for some NFS implementations, but is safe and should be left enabled on most installations.
  - Disable filter - you can turn off the firewall filter entirely if you wish to turn pfSense into a pure router.
VPN

- pfSense offers three options for VPN connectivity:
  - IPsec
  - OpenVPN
  - PPTP
Captive Portal

• Captive Portal
  – Captive portal allows you to force authentication, or redirection to a click through page for network access. This is commonly used on hot spot networks (like the Aria), but is also widely used in corporate networks for an additional layer of security on guest wireless or Internet access.
Load Balancing

Load Balancing

• **Outbound Load Balancing**
  - Outbound load balancing is used with multiple WAN connections to provide load balancing and failover capabilities. Traffic is directed to the desired gateway or load balancing pool pool on a per-firewall rule basis.

• **Inbound Load Balancing**
  - Inbound load balancing is used to distribute load between multiple servers. This is commonly used with web servers, mail servers, and others. Servers that fail to respond to ping requests or TCP port connections are removed from the pool.
Reporting and Monitoring

• RRD Graphs
  • The RRD graphs in pfSense maintain historical information on the following.
  • CPU utilization
  • Total throughput
  • Firewall states
  • Individual throughput for all interfaces
  • Packets per second rates for all interfaces
  • WAN interface gateway(s) ping response times
  • Traffic shaper queues on systems with traffic shaping enable
Reporting and Monitoring

• **Real Time Information**
  • Historical information is important, but sometimes it's more important to see real time information.
  • SVG graphs are available that show real time throughput for each interface.
  • For traffic shaper users, the Status -> Queues screen provides a real time display of queue usage using AJAX updated gauges.
  • The front page includes AJAX gauges for display of real time CPU, memory, swap and disk usage, and state table size.
Redundancy/High Availability

• CARP
  – Common Address Redundancy Protocol
Redundancy/High Availability

- Two or more firewalls can be configured as a failover group.
- If one interface fails on the primary or the primary goes offline entirely, the secondary becomes active.
- pfSynch ensures that state tables are also synchronized so that in the even of a failure seamless failover can occur.
Network Address Translation

- Port forwards including ranges and the use of multiple public IPs
- 1:1 NAT for individual IPs or entire subnets.
- Outbound NAT
  - Default settings NAT all outbound traffic to the WAN IP. In multiple WAN scenarios, the default settings NAT outbound traffic to the IP of the WAN interface being used.
  - Advanced Outbound NAT allows this default behavior to be disabled, and enables the creation of very flexible NAT (or no NAT) rules.
- NAT Reflection - in some configurations, NAT reflection is possible so services can be accessed by public IP from internal networks.
192.168.1.1
admin
pfsense
This wizard will guide you through the initial configuration of pfSense.
On this screen you will set the General pfSense parameters.

<table>
<thead>
<tr>
<th>General Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname:</td>
</tr>
<tr>
<td>pfSense</td>
</tr>
<tr>
<td>EXAMPLE: myserver</td>
</tr>
<tr>
<td>Domain:</td>
</tr>
<tr>
<td>local</td>
</tr>
<tr>
<td>EXAMPLE: mydomain.com</td>
</tr>
<tr>
<td>Primary DNS Server:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Secondary DNS Server:</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

[Next]
On this screen you will set the General pfSense parameters.

<table>
<thead>
<tr>
<th>General Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname: pfSense</td>
</tr>
<tr>
<td>Domain: pattihall.com</td>
</tr>
<tr>
<td>Primary DNS Server: 8.8.8.8</td>
</tr>
<tr>
<td>Secondary DNS Server: 8.8.4.4</td>
</tr>
</tbody>
</table>
Please enter the time, date and time zone.

<table>
<thead>
<tr>
<th>Time Server Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time server hostname:</strong></td>
</tr>
<tr>
<td><strong>Enter the name of the time server.</strong></td>
</tr>
<tr>
<td><strong>Timezone:</strong></td>
</tr>
</tbody>
</table>

Next
On this screen we will configure the Wide Area Network information.

### Configure WAN Interface
- **SelectedType:** DHCP

### General configuration
- **MAC Address:**
  
  This field can be used to modify ("spooﬁng") the MAC address of the WAN interface (may be required with some cable connections) Enter a MAC address in the following format: xxxxxxxx or leave blank

- **MTU:**
  
  If you enter a value in this ﬁeld, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this ﬁeld blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

### Static IP Configuration
- **IP Address:** dhcp / 1

- **Gateway:**

### DHCP client configuration
- **DHCP Hostname:**
  
  The value in this ﬁeld is sent as the DHCP client identiﬁer and hostname when
The changes have been applied successfully. You can also monitor the filter reload progress.

### General configuration

**Type**

Static

**MAC address**

Copy my MAC address

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: 00:00:00:00:00:00 or leave blank.

**MTU**

This field is used to specify the Maximum Transmission Unit (MTU) for the interface. If you enter a value in this field, then MSS clamping for TCP connections is set to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

### Static IP configuration

**IP address**

10.0.0.253

**Gateway**

10.0.0.1

### DHCP client configuration

**Hostname**

The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

### PPPoE configuration

**Username**

---
On this screen we will configure the Local Area Network information.

<table>
<thead>
<tr>
<th>Configure LAN Interface</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>LAN IP Address:</strong></td>
<td>192.168.1.1</td>
</tr>
<tr>
<td></td>
<td>Type dhcp if this interface uses DHCP to obtain its IP address.</td>
</tr>
<tr>
<td><strong>Subnet Mask:</strong></td>
<td>24</td>
</tr>
</tbody>
</table>
On this screen we will set the Admin password which is used to access the WebGUI and also SSH services if you wish to enable.

Set Admin WebGUI Password

<table>
<thead>
<tr>
<th>Admin Password:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Password AGAIN:</td>
</tr>
</tbody>
</table>

Next
pfsense
### System Overview

<table>
<thead>
<tr>
<th><strong>System information</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>pfSense.pattishall.nlm</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>1.2.3-RELEASE</td>
</tr>
<tr>
<td></td>
<td>built on Sun Dec 6 23:21:36 EST 2009</td>
</tr>
<tr>
<td><strong>Platform</strong></td>
<td>cdrom</td>
</tr>
<tr>
<td><strong>Uptime</strong></td>
<td>03:24</td>
</tr>
<tr>
<td><strong>State table size</strong></td>
<td>61/10000</td>
</tr>
<tr>
<td></td>
<td>Show states</td>
</tr>
<tr>
<td><strong>MBUF Usage</strong></td>
<td>517 / 780</td>
</tr>
<tr>
<td><strong>CPU usage</strong></td>
<td><img src="cpu_usage.png" alt="57%" /></td>
</tr>
<tr>
<td><strong>Memory usage</strong></td>
<td><img src="memory_usage.png" alt="19%" /></td>
</tr>
<tr>
<td><strong>Disk usage</strong></td>
<td><img src="disk_usage.png" alt="100%" /></td>
</tr>
</tbody>
</table>

pfSense is © 2004 - 2009 by BSD Perimeter LLC. All Rights Reserved. [view license] [Commercial Support Available]
### pfSense Overview

- **Package**: pfSense.local
- **Version**: 1.2.3-RELEASE
  - Built on Sun Dec 6 23:21:36 EST 2009
- **Platform**: pfSense
- **Uptime**: 00:03
- **State table size**: 27/10000
  - show states
- **MBUF Usage**: 517/780
- **CPU usage**: 5%
- **Memory usage**: 13%
- **SWAP usage**: 0%
- **Disk usage**: 3%
<table>
<thead>
<tr>
<th>Package</th>
<th>Type</th>
<th>Status</th>
<th>Version</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate</td>
<td>Network Management</td>
<td>BETA</td>
<td>0.9 platform: 1.2.2</td>
<td>No info, check the forum. This package adds a table of realtime bandwidth usage by IP address to Status -&gt; Traffic Graphs.</td>
</tr>
<tr>
<td>siproxd</td>
<td>Services</td>
<td>Beta</td>
<td>0.7.2 platform: 1.2.1</td>
<td>Package Info. Proxy for handling NAT of multiple SIP devices to a single public IP.</td>
</tr>
<tr>
<td>snort</td>
<td>Security</td>
<td>Stable</td>
<td>2.8.6 pkg v.1.27 platform: 1.2.3</td>
<td>Package Info. Used by fortune 500 companies and governments. Snort is the most widely deployed IDS/IPS technology worldwide. It features rules based logging and can perform content searching/matching in addition to being used to detect a variety of other attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and much more.</td>
</tr>
<tr>
<td>snort-old</td>
<td>Security</td>
<td>legacy</td>
<td>2.8.4.1_b pkg v.1.8 platform: 1.2.3</td>
<td>Package Info. WARNING: This is the old snort package. A few current snort.org rules are not supported in this package. This package will not be supported in PFSense 2.0.</td>
</tr>
<tr>
<td>squid</td>
<td>Network</td>
<td>Stable</td>
<td>2.7.9.1 platform: 1.2.1</td>
<td>No info, check the forum. High performance web proxy cache.</td>
</tr>
<tr>
<td>squid3</td>
<td>Network</td>
<td>ALPHRA</td>
<td>3.0.8.09 platform: 1.2.1</td>
<td>No info, check the forum. EXPERIMENTAL! Not all directives are ported yet! High performance web proxy cache.</td>
</tr>
<tr>
<td>squidGuard</td>
<td>Network Management</td>
<td>Beta</td>
<td>1.3-2 platform: 1.1</td>
<td>No info, check the forum. High perfomance web proxy URL filter. Requires proxy Squid package.</td>
</tr>
<tr>
<td>Package</td>
<td>Category</td>
<td>Version</td>
<td>Status</td>
<td>Notes</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>-------------</td>
<td>--------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>snort</td>
<td>Security</td>
<td>2.5.4</td>
<td>check the forum</td>
<td>Displays system facts and formats information nicely.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>0.9</td>
<td>BETA, check the forum</td>
<td>Displays information about system facts like uptime, CPU, memory, PCI devices, chassis, IDE devices, network adapters, disk usage, and more.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.2.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>siproxd</td>
<td>Services</td>
<td>0.7.2</td>
<td>Package Info</td>
<td>Provides a table of real-time bandwidth usage by IP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.2.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>snort-old</td>
<td>Security</td>
<td>Legacy 2.8.4.1</td>
<td>Package Info</td>
<td>Provides legacy support for snort.org rules not supported in this package.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.8.1.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>pkg v1.1.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.2.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>squid</td>
<td>Network</td>
<td>Stable 2.7.9</td>
<td>No info, check the forum</td>
<td>High performance web proxy cache.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>squid3</td>
<td>Network</td>
<td>ALPHRA 3.0.9</td>
<td>No info, check the forum</td>
<td>Experimental! Not all directives are supported yet. High performance web proxy cache.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2.1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>squidGuard</td>
<td>Network</td>
<td>Beta 1.3.2</td>
<td>No info, check the forum</td>
<td>High performance web proxy URL filter. Requires proxy Squid package.</td>
</tr>
<tr>
<td></td>
<td>Management</td>
<td>1.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Beginning package installation for snort...

Downloading package configuration file...
Installing snort and its dependencies.

Downloading package configuration file... done.
Saving updated package information... done.

Installing snort and its dependencies

pcre-8.02 (extracting)
## System: Package Manager

### 1.2.3-RELEASE packages

<table>
<thead>
<tr>
<th>Package Name</th>
<th>Category</th>
<th>Package Info</th>
<th>Package Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard Widget Snort</td>
<td>System</td>
<td>No info, check the forum</td>
<td>0.3</td>
<td>Dashboard widget for Snort.</td>
</tr>
<tr>
<td>snort</td>
<td>Security</td>
<td>Package Info</td>
<td>2.8.6 pkg v. 1.27</td>
<td>Used by Fortune 500 companies and governments Snort is the most widely deployed IDS/IPS technology worldwide. It features rules based logging and can perform content searching/matching in addition to being used to detect a variety of other attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMI probes, and much more.</td>
</tr>
</tbody>
</table>
## System: Package Manager

### 1.2.3-RELEASE packages

<table>
<thead>
<tr>
<th>Package Name</th>
<th>Category</th>
<th>Package Info</th>
<th>Package Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard Widget</td>
<td>System</td>
<td>No info, check the forum</td>
<td>0.3</td>
</tr>
<tr>
<td>snort</td>
<td>Security</td>
<td>Package Info</td>
<td>2.8.6</td>
</tr>
</tbody>
</table>

### Installed packages

**Snort**

- **Description**: Snort is a widely deployed IDS/IPS technology worldwide. It supports rules-based logging and can perform content matching in addition to being used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMURF probes, and more.

- **Features**: Snort integrates with other tools and can detect a wide range of threats. It is open-source and highly configurable.

- **Components**: Snort includes rule sets for various security scenarios, allowing administrators to customize their protection strategies.
### Snort Interfaces

<table>
<thead>
<tr>
<th>Snort Interfaces</th>
<th>Global Settings</th>
<th>Rule Updates</th>
<th>Alerts</th>
<th>Blocked</th>
<th>Whitelists</th>
<th>Suppress</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>If</td>
<td>Snort</td>
<td>Performance</td>
<td>Block</td>
<td>Barnyard2</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:**
This is the Snort Menu where you can see an overview of all your interface settings. Please edit the Global Settings tab before adding an interface.

**Warning:**
New settings will not take effect until interface restart.

- Click on the [+] icon to add an interface.
- Click on the [-] icon to delete an interface and settings.
- Click on the [ ] icon to start snort and barnyard2.
- Click on the [ ] icon to stop snort and barnyard2.
### General Settings

<table>
<thead>
<tr>
<th>Interface</th>
<th>Enable or Disable</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
<td><strong>WAN</strong></td>
</tr>
<tr>
<td>Choose which interface this rule applies to. Hint: in most cases, you'll want to use WAN here.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Memory Performance</th>
<th>AC-BNFA</th>
</tr>
</thead>
<tbody>
<tr>
<td>A: recommended for low end systems, Ac: high memory, best performance, ac-std: moderate</td>
<td></td>
</tr>
</tbody>
</table>

### Choose the network(s) and whitelist.

<table>
<thead>
<tr>
<th>Home net</th>
<th>AC-BANDED, AC-SPARSEBANDS, ACS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hint: Most users add a list of friendly IPs that the firewall can't see.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>External net</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose the external net you will like this rule to use. Note: Default external net, networks that are not home net.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Block offenders</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Checking this option will automatically block hosts that generate a Snort alert.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Whitelist</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose the whitelist you will like this rule to use. Note: Default whitelist adds only local networks.</td>
<td></td>
</tr>
</tbody>
</table>
LogSurfer and LogSurfer+ Resources

Contents

Introduction
Logsurfer+ features
Download
Documentation
Mailing List
Configuration examples
Links

Introduction
Logsurfer is a program for monitoring system logs in real-time, and reporting on the occurrence of events. It is similar to the well-known swatch program on which it is based, but offers a number of advanced features which swatch does not support.

Logsurfer is capable of grouping related log entries together - for instance, when a system boots it usually creates a high number of log messages. In this case, logsurfer can be setup to group boot-time messages together and forward them in a single Email message to the system administrator under the subject line "Host xxx has just booted". Swatch just couldn't do this properly.

Logsurfer is written in C - this makes it extremely efficient, an important factor when sites generate a high amount of logs.
Logwatch analyzes and reports on system logs. It is a customizable and pluggable log-monitoring system and will go through the logs for a given period of time and make a customizable report. It should work right out of the package on most systems.

Recent releases

7.3 07 Apr 2006 01:25

Changes: Numerous improvements and bugfixes were made.
Support Options

• Community Forum
• Mailing List
• IRC
• Local Support is available in these areas:
  – Louisville, Kentucky
  – Nashville, Tennessee
  – Southeast Idaho
  – Northern Utah
  – Jackson, Wyoming
  – San Diego, California
Sounds great, but...

- How much does it cost?
  - Nothing, nada, diddly squat, bupkis. It’s FREE!
- Is it secure?
  - Absolutely! However, a firewalls level of security is based entirely on how YOU configure it.
Paid Support Subscription

The base 5 hour annual subscription is $600 USD. Additional blocks of hours can be purchased if needed, at the following rates (all prices USD).

Additional Hours

Available to customers with an active support subscription

5 hours - $400
10 hours - $750
50 hours - $3500
Thank you!
Questions?