BSD Firewalling, pfSense and m0n0wall

Scott Ullrich (sullrich@gmail.com)
Chris Buechler (cbuechler@gmail.com)

BSDCan 2006
May 10th - May 12th

Agenda

- BSD Firewalling
  - Overview of packet filters on the BSD's
- m0n0wall
- pfSense

BSD Firewalling Options

- Which to use when
  - After looking at the comparison table, select the best filter for the task.
  - If you have a personal preference or comfortability level, go with it.
  - Userland vs kerneland NAT daemon?
  - Better handling of NAT broken protocols such as FTP, SIP depending on Firewalling stack.

Firewalling Options on FreeBSD

- IPFW
- PF
- IPFilter

Firewalling Options on OpenBSD

- PF
- IPFilter

Firewalling Options on NetBSD

- PF
- IPFilter

Firewalling Options on DragonFlyBSD

- PF
- IPFW
- IPFilter

BSD Firewalling Options

FEATURE	IPFW	IPFILTER	PF
QUEUE DUMMYNET	★		★
QUEUE ALTQ	★		★
SKIPTO	★		
RULESETS	★		
CONNECTION FORWARDING	★	★	★
IPTOS	★		
IPTTL	★		
IPPOS	★		
IPVERSION	★		
LAYER2 MATCHING	★		
MAC ADDRESS FILTERING	★		
TABLES	★		
PROBABILITY (PROB)	★		
COUNT	★		

BSD Firewalling Options

FEATURE	IPFW	IPFILTER	PF
TEE	★	★	★
"ME" SUPPORT	★	★	
IPV6	★	★	★
JAIL	★		
IPSEC	★		
IPTOS - LOW DELAY	★	★	★
IPTOS - THROUGHPUT	★	★	★
IPTOS - RELIABILITY	★	★	★
IPTOS - MINCOST	★	★	
IPTOS - CONGESTION	★	★	★
UID	★		
VERREVPATH	★		
QUICK		★	★

BSD Firewalling Options

FEATURE	IPFW	IPFILTER	PF
KEEP STATE	★	★	★
MODULATE STATE			★
SYNPROXY STATE			★
OVERLOAD SUPPORT			★
FINGERPRINT SCANNING			★
LIMIT STATES PER RULE			★

m0n0wall

Mission Statement

- m0n0wall is a project aimed at creating a complete, embedded firewall software package that, when used together with an embedded PC, provides all the important features of commercial firewall boxes (including ease of use) at a fraction of the price (free software).

- m0n0wall is based on a **bare-bones version of FreeBSD**, along with a web server, **PHP** and a few other utilities. The entire system configuration is stored in one single XML text file to keep things transparent.

- m0n0wall is probably **the first UNIX system that has its boot-time configuration done with PHP**, rather than the usual shell scripts, and that has **the entire system configuration stored in XML format**.
  - This is really cool and powerful!

m0n0wall

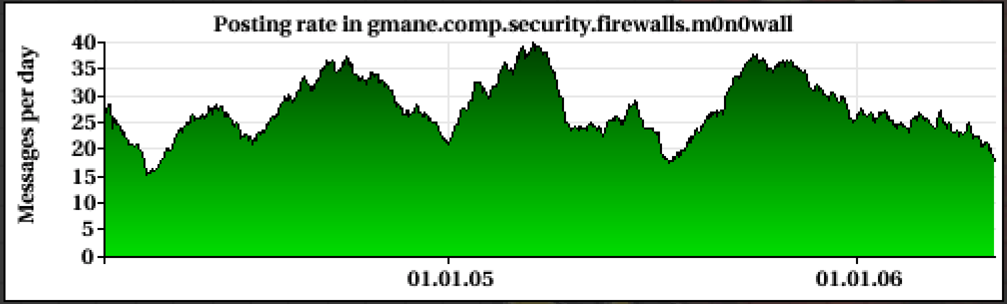
overview

- First public release February 2003
- Engineered for low footprint embedded devices
- Based on FreeBSD 4.11
  - Very fast and stable
  - Outdated hardware support
    - Limited Gigabit Ethernet
    - Very Limited Wireless
    - NO SATA

m0n0wall

community

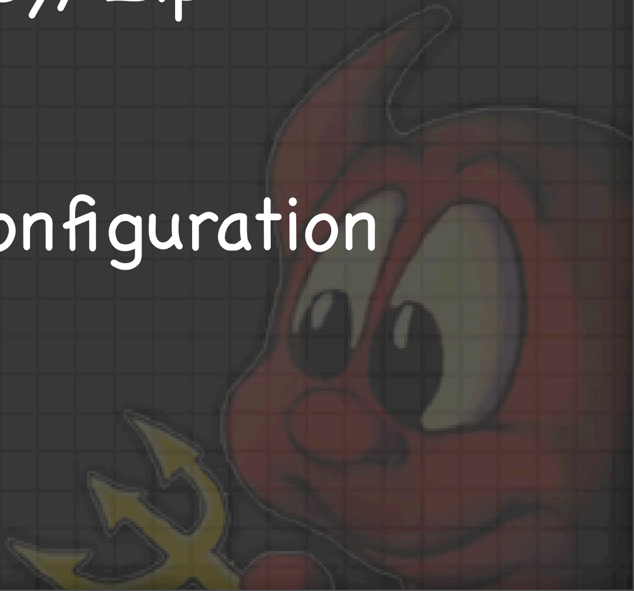
- Six committers
- Public mailing lists
- IRC channel hovers around 45 (#m0n0wall on FreeNode)
- Public SVN server
- 1530 mailing list members
- ~65000 unique web visitors a month / ~5500 per day



m0n0wall

hardware

- Minimum 64 MB RAM
- Soekris
- PC Engines WRAP
- Uses physdiskwrite.exe or DD to install to hard drive, Compact Flash, USB key, Zip drive, or other storage medium.
- CD version available that saves configuration to floppy disk.



m0n0wall

versions available

- PC-Engines WRAP
- Soekris
    - NET_45XX
    - NET_48XX
- Generic PC

m0n0wall

Why FreeBSD?

  - Manuel Kasper's personal preference

- OS of choice for version 1.3 is yet to be determined. Discussions mostly around FreeBSD 6.x and OpenBSD.

pfSense

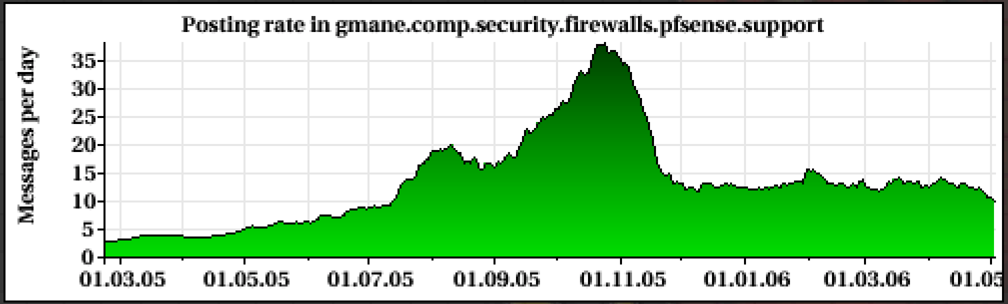
Mission Statement

- pfSense is a open source firewall derived from the m0n0wall firewall platform with radically different goals such as using OpenBSD's ported Packet Filter, FreeBSD 6.1 ALTQ (HFSC) for excellent packet queueing and finally an integrated package management system for extending the environment with new features.
- Same init system being used via php as m0n0wall making us the second known unix to use PHP completely for their init sequence.
- Maintains same 1 file XML configuration system

# pfSense

community

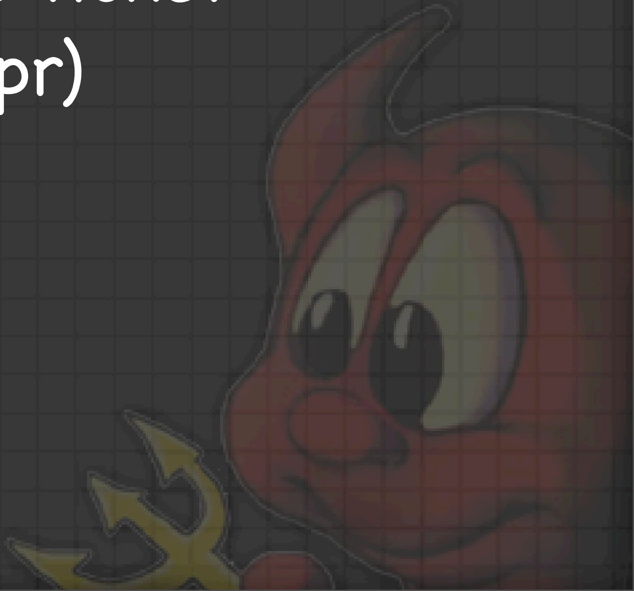
- About 800 registered forum users
- Over 400 support mailing list members
- IRC channel hovers around 80 people (##pfSense on FreeNode)



pfSense

community

- 16 committers
- CVS Server
- CVSWEB Support
- CVSTrac Support for timeline and ticket based services (similar to submit-pr)



pfSense

community

Web Forum Stats

- 750,000+ page hits
- 6614 posts in 1102 topics
- 4+ new users per day average
- Male to female ratio: 65:1

m0n0wall & pfSense

shared features

- Captive Portal
- DHCP Server and client
- PPTP, IPSEC support
- 802.1Q VLAN support
- DynDNS client & RFC2126 DNS updater
- Caching DNS Forwarder
- SNMP
- Host/network aliases
- Configuration backup/ restore
- webGUI
- Upgradable via webGUI

pfSense features

- CARP / PFSync
- Expanded alias usage
- XML configuration sync between master and backup hosts. Allowing for a single point of administration for a firewall cluster.
- Load balancing
  - Incoming
  - Outgoing
- Traffic shaping queue status graphs
- Incoming and outgoing load balancing
- Package support
- PPPoE Server
- Themes
- Setup wizard
- Multiple WAN support
- SSH
- Reduced reboots after changes
- CPU / Memory / Disk usage meters
- Many, many more tweaks

pfSense

packages

- Doorman
- NTOP
- Squid
- OpenBSD's SpamD
  Excellent spam prevention service.
- PFFlowd
  Used for converting PF status messages to Cisco Netflow Datagrams
- NMap

- ASSP
- ARPWatch
- Freeradius
- ifdepd
- SipProxD
- STunnel
- WIdentD
- IPerf

pfSense

- Engineered for faster hardware
- Includes an installer (BSD Installer) assisting in full installations
- based on FreeBSD 6.1 release
  - Excellent hardware support
  - Excellent wireless support
  - 25-35% lower network throughput than FreeBSD 4.x (non-SMP) noticeable on slower hardware such as 266 megahertz embedded gear.
- Has package support for certain platforms

pfSense

hardware requirements

- Minimum 128 MB RAM
- PC-Engines WRAP 266 MHz 128 MB
- Soekris 4801
- LinITX
- VIA

Versions available

- Developers edition
  - Most likely meant for some of you geeks(TM) attending today that tinker/write code.
  - Automatically bootstraps the developer environment after installation and builds an ISO to test this fact.
  - Can build all versions of pfSense with one command.
  - Allows power users, system administrators and OEM's to customize and roll out custom pfSense installations.

Versions available

- Embedded
  - Meant for devices with only a serial console.
  - Minimum 128 MB RAM
  - Designed for 64 MB compact flash
  - Read only environment, only mounts the flash device r/w when required.
  - Currently no package support. It's possible, but not officially supported.

Versions available

- CD-ROM
  - Runs from a CD-ROM device
  - Stores configuration on removable media (compact flash, floppies, etc)
  - No package support (RO media)
- Full Installation
  - Minimum 128 megabytes of RAM
  - 500 megabytes of hard drive space or above
  - Package support

pfSense

single point of administration

- Uses XML-RPC to automatically push configuration changes to a chain of backup hosts.
- Uses CARP to provide the underlying failover services and ease of administration via virtual IP's
- Converts cheap/decent hardware into cluster nodes
- Requires a static IP per individual carp cluster member (this will change in the future with carpdev)

pfSense

wireless mojo

- Supports Atheros line of products incredibly well
- HostAP (access point) support
- WPA Supplicant (client) support
- Turbo modes
- OLSR

  Wireless meshing support

pfSense

Why FreeBSD?

- Experience and familiarity
- Availability of PF, ALTQ, CARP, pfsync, etc.
- Wireless support
- Performance
- SMP support

pfSense

traffic shaping

- Uses ALTQ HFSC
  * Hierarchical Fair Service Curve
  * Supports CBQ in -HEAD (development tree)
- Can curb all unknown traffic to the abyss (inserts unknown traffic into slowest queue (p2pQueue)
- Can guarantee an amount of bandwidth for items such as:
  - VOIP
  - Gaming
  - Terminal Services
  - Interactive applications (SSH)

Any questions?

Presentation available at:

http://pfsense.org/bsdcan/
http://doc.m0n0.ch/bsdcan/

Thanks!

Presentation available at:

http://pfsense.org/bsdcan/
http://doc.m0n0.ch/bsdcan/

Notes - FreeBSD

- PF
  - http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls-pf.html
- IPFilter
  - http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls-ipf.html
- IPFW
  - http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls-ipfw.html