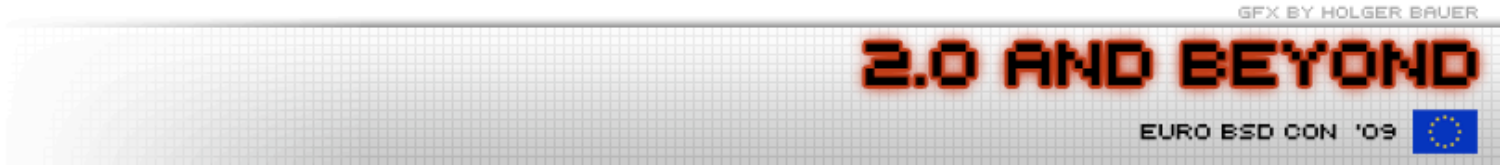
pfSense - 2.0 and beyond

Chris Buechler - cmb@pfsense.org



Introduction to pfSense

- Customized FreeBSD distribution tailored for use as a firewall and router.
- Entirely managed via web interface
- Configuration stored in single XML file
- Founded in 2004 as fork of m0n0wall
  - Initially full PC focused
  - Expandability a focus
  - “Making sense of PF” for the average point-and-click user
    - for lack of a better name
- 18 active developers contributed in past 12 months
  - 29 have contributed since the project’s inception

Near future – 1.2.3

- Maintenance release
- Update to FreeBSD 7.2 base
- Minor edge case bug fixes
- Outbound load balancing replaced
  - slbd replaced with apinger
- IPsec reload improvements
  - Dynamic DNS endpoint support
  - NAT-T added, then removed
- Embedded switched to nanobsd base

New nanobsd embedded

- 1.2.3 and newer
- Multiple partition/firmware support
- Reliable remote upgrades
- Package support
- Future support for additional architectures
  - MIPS
  - ARM

Book release

- pfSense: The Definitive Guide, from Reed Media
- Roughly 500 pages
- Will be finished this coming week, available soon

2.0 Release

- FreeBSD 8.0 base
- Vast changes to numerous features
- 3 years of feature additions

New features (base)

- New traffic shaper
- User Manager
- OpenVPN, IPsec enhancements
- L2TP VPN added
- PHP 5
- Certificate Manager
- Routing / Gateways improvements
- Dashboard
- Load balancer changes
- Web based PFTOP, TOP
- IGMP proxy

New features (continued)

- Complete new interface system
- Multiple DynDNS account and interface support
- DHCP Server improvements
- New libalias based in-kernel FTP helper
- Improved load balancing (incoming and outgoing)

New traffic shaper

- Rewritten from scratch by Ermal Luci
- Supports HFSC, CBQ, FairQ, PriQ
- Uses ALTQ
- Now works on more than 2 interfaces
  - Multi-WAN
  - Multi-LAN
  - etc.
- Layer 7 classifier
  - ipfw-classifyd by Mike Makonnen modified for pf
  - Using Linux l7-filter protocol patterns
- All major limitations are now gone!

User Manager

- Full user manager with user and groups support
- Can allow an account to specific areas
- Consolidating all accounts in various areas
  - Administrators
  - Captive Portal
  - All VPNs – IPsec, L2TP, OpenVPN, PPTP
  - PPPoE server
- LDAP authentication support
- Per user certificate support

IPsec

- Major overhaul by Matthew Grooms, ipsec-tools committer and author of Shrew Soft IPsec client - http://shrew.net
- Multiple Phase 2 per Phase 1
- Transport mode support added

IPsec

- Xauth - user and group authentication
  - pfSense local user database
  - LDAP
    - Microsoft Active Directory
    - Novell eDirectory
    - and others...
  - RADIUS
    - Microsoft Active Directory
    - many others
- Now a drop-in replacement for Cisco VPN concentrators, PIX firewalls, and routers

OpenVPN

- Major overhaul
- More options exposed in the GUI
- Standardization with other VPN types
- Client exporter
  - Pre-configured Windows installer
  - Configuration file for Viscosity

New interfaces

- GRE
- gif
- PPP (dial up POTS modems, 3G cellular wireless)
- QinQ VLANs
- Interface groupings
- lagg(4) interface bonding
  - failover
  - load balance
  - round robin
  - Etherchannel
  - LACP

Bridging enhancements

- all of if_bridge capabilities supported
- 18 Advanced configuration options available
- STP and RSTP - fully configurable
- SPAN port capable

Certificate Manager

- Certificate authority support
- Generate OpenVPN certificates
- Generate user certificates
- Generate HTTPS certificate
- Generate IPsec certificates
- Revocation support
- Import existing certificates

Routing / Gateway Additions

- New gateway group feature
- Failover threshold supports RTT or packet loss triggers
- Groups now employ a "Tier" type system
  - Supports balancing
  - Supports interface failover ordering
- Can fail on X% loss, 100% down, and/or high latency
  - User-definable thresholds

Dashboard

- Allows quick access to system information
- Added RSS widget
- Added picture widget
- Added gateways widget with RTT and loss reporting
- New AJAX CPU utilization widget

Load Balancer changes (relayd)

- Layer3 balancing
- Layer7 balancing
- New monitoring features
  - Send/expect
  - DNS
  - HTTP
  - HTTPS

Web based pftop

Diagnostics: PFTop

Sort type: bytes

pfTop: Up State 1-8/8, View: default, Order: bytes

PR	D	SRC	DEST	STATE	AGE	EXP	PKTS	BYTES
icmp	O	10.211.55.4:49131	10.211.55.1:0	0:0	4310	9	8618	538K
tcp	I	10.211.55.2:55974	10.211.55.4:80	4:4	20	86400	117	83530
tcp	I	10.211.55.2:55957	10.211.55.4:80	9:9	128	7	101	35020
tcp	I	10.211.55.2:55961	10.211.55.4:80	9:9	80	55	101	35014
tcp	I	10.211.55.2:55973	10.211.55.4:80	10:10	32	70	36	11145
udp	I	10.211.55.2:52094	10.211.55.255:137	0:1	19	11	3	234
udp	I	10.211.55.2:52095	10.211.55.255:137	0:1	19	11	3	234
udp	O	10.211.55.4:14829	66.250.45.2:123	2:1	14	16	2	152

Web based top

Diagnostics: System Activity

```
last pid: 23231;  load averages:  0.35,  0.13,  0.08  up 0+01:18:20    10:46:36
31 processes:  1 running, 30 sleeping

Mem: 28M Active, 21M Inact, 23M Wired, 16K Cache, 22M Buf, 52M Free
Swap: 256M Total, 256M Free


  PID USERNAME  THR PRI NICE   SIZE    RES STATE    TIME   WCPU COMMAND
39838 root        1  -8    0 41812K 21400K piperd   0:07  0.00% php
60351 nobody      1  44    0  3156K  1224K select   0:03  0.00% apinger
41067 root        1   8   20  3492K  1460K wait     0:02  0.00% sh
39077 root        1   4    0  6328K  3464K kqread   0:02  0.00% lighttpd
23011 root        1   8   20  3156K   796K nanslp   0:01  0.00% check_reload_status
26241 root        1 -58    0  5716K  2028K bpf      0:00  0.00% tcpdump
50476 root        1  44    0  4920K  3152K select   0:00  0.00% openvpn
24619 _ntp        1  44    0  3156K  1228K select   0:00  0.00% ntpd
 8770 root        1  44    0  3268K  1280K select   0:00  0.00% syslogd
39387 root        1   8    0 39688K  9036K wait     0:00  0.00% php
11546 root        1   8    0  3492K  1380K wait     0:00  0.00% sh
12192 root        1   8    0  3240K  1268K nanslp   0:00  0.00% cron
25095 root        1   5    0  3508K  2212K ttyin    0:00  0.00% tcsh
26527 root        1  -8    0  3156K   788K piperd   0:00  0.00% logger
24767 root        1  44    0  3156K  1240K select   0:00  0.00% ntpd
61308 root        1   8    0  3516K  1472K wait     0:00  0.00% login
23698 root        1   8    0  3156K   900K nanslp   0:00  0.00% minicron
63397 root        1   8    0  3492K  1388K wait     0:00  0.00% sh
```

IGMP Proxy

- Compatibility with multicast services
- IP TV
- Phone systems for broadcast announcements

New interface system

- All interfaces treated equally - no special status for LAN/ WAN.
- Multi interface PPPoE support (WAN)
- Multi interface PPTP support (WAN)
- Allows just one interface to be assigned (appliance mode)
- QinQ VLAN support
- Interface groups

DHCP Server improvements

- Dynamic DNS client name registration support
- Definable NTP Servers
- LDAP URI Integration
- Now allows duplicate IP address registration for multiple MAC addresses
- Ability to add any custom DHCP option

Appliance building

- pfSense builder system can now automatically generate custom "Appliances" from an overlay file.
- Simply add files that you want to include into a directory and define the directory in pfsense_local.sh custom_overlay directive
- Also used for rebranding

- Coming appliances
  - DNS server
  - FreeSWITCH VoIP PBX

2.0 Release Timeline

- When?
  - When it's ready…
  - Aim for release candidate status by end of 2009

Revision control

- Converted from CVS to git
- More open development
- Cloning available to all
- Eases collaborative development and testing

https://rcs.pfsense.org

Further down the road

Post 2.0 release (2010 and beyond)

- Shorter release cycles
- Each release more evolutionary, less revolutionary

Commercial side

- Commercial support and development offerings
- One full time employee, many contractors around the world
- Commercial support is growing with satisfied customers
- Most new 2.0 functionality the result of funded development
- Funds conference attendance, and the projects we use

Thanks for attending!

Questions?

Comments?

cmb@pfsense.org