BSD Firewalling with pfSense

and a bit on entrepreneurship and open source

NYCBSDCon 2010

Chris Buechler - cmb@pfsense.org

pfSense Overview

- FreeBSD-based firewall 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
- Currently 20 active developers (committed in past year)
  - 53 have contributed since the project’s inception

pfSense Overview

- Many base features and can be extended with the package system including one click installations of popular third party applications (Squid, Squidguard, Snort, many more)
- Includes most or all features found in commercial products such as Cisco ASA, Sonicwall, Watchguard, etc.
- Many support avenues available; mailing lists, forum and commercial support.
- Free in every sense - our code base all BSD licensed, most included underlying services BSD as well

Project statistics

- millions of downloads served since inception
- current rate of over 30,000 downloads a month
- over 30,000 forum members
- ~1200 mailing list users
- 53 developers since inception
- 24 active developers (committed in the last year)
  - "This is one of the largest open-source teams in the world, and is in the top 2% of all project teams on Ohloh."
- Millions of page views per month across all sites
- Average month sees visitors from 200 different countries
  - as reported by Google Analytics

Primary usage scenarios

- Hosting/colocation environments
- ISPs / WISPs
- Hot spot providers
- Virtual firewalls
- Public sector
- Service providers
- Universities
- Non-profits
- Every type of business imaginable, small to large
  - Largely except huge companies
- Home users

Why FreeBSD?

Primary reasons in 2004

- Wireless support
- Network performance
- Familiarity and ease of fork
- Inadequate resources for multiple OS support

Current reasons

- Relationship with FreeBSD project
- Attracted considerable FreeBSD talent
- Performance now and into the future

Downside

- Older versions of OpenBSD-native software

Why use pfSense?

- Hides complexity
- Ease of management
- Ease of training non-BSD administrators
- Proven, customized OS base focused and tailored as a firewall and router

Why not use pfSense?

- All administrators already familiar with underlying software
- Learning experience
  - Time to burn

pfSense Platforms

- Live CD
- Full Install
- Embedded

Versions

- 1.2.3 stable – FreeBSD 7.2 base
- 2.0 beta, soon RC1 - FreeBSD 8.1 base

Project's Workings 2004-2008

- Founded by Scott Ullrich and Chris Buechler
- Others came along early on
- People come and go
- Project grows considerably, gains large deployed base
- Typical open source operation
  - Filling own needs
- Demand for services grows
  - Support
  - Paid development

Start of commercial side

- Founded BSD Perimeter LLC in late 2006
  - Holder of copyright on project and trademark on pfSense
- Started offering commercial support in 2007
  - Per-install basis
    - Not really suitable for open source
    - Problematic for firewalls
      - Problem? Has to be the firewall!
    - Have to limit scope
    - Wrong incentives for us

Start of commercial side

- Transition to hourly support in 2008
  - portal.pfsense.org
  - Improved marketing on services offered
  - things take off

Commercial side today

- Four full time employees
- Several additional contractors
- Hundreds of support customers
  - In 30 countries, on 6 continents
- Dozens of reseller subscribers
  - Hardware resellers
  - Rebranded resellers
- Several dozen rebranded commercial offerings
  - Some entirely stock
  - Some with proprietary add ons
    - Industrial protocol filtering for SCADA protection
- Funds conference attendance

Project's Workings 2008-Present

- Bulk of work on project done by those we employ
- What gets done is what people pay us to do
  - aside from general maintenance
- Still many outside contributors

2.0 New Features (base)

- New traffic shaper
  - HFSC, CBQ, FairQ, PriQ
- Limiters - dummynet in pf(4)
- Layer 7 QoS
- User Manager
- OpenVPN Improvements
- PHP 5
- Certificate Manager
- Routing / Gateways improvements
- Dashboard
- Load balancer changes
- Web based PFTOP, TOP
- IGMP proxy

2.0 New Features (continued)

- Complete new interface system
- Multiple Dynamic DNS support
- DHCP Server improvements
  - Definition of custom options
- GRE NAT Improvements

User Manager

- Full user manager with user and groups support
- Can allow an account to specific areas
- Consolidating all accounts in various areas (VPN users, etc)
- 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
- NAT-T support
- 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
- mode-cfg support (IP, DNS, etc. assignment)
- Now a drop-in replacement for Cisco VPN concentrators, PIX/ASA firewalls, and routers

OpenVPN

- Major overhaul
- Integrated certificate management
- Setup wizard
- Client export
  - Windows installer bundled with certificates
  - Bundled zip file for BSD, Linux, OS X, etc.
  - Viscosity export for Mac OS X

New interfaces

- GRE
- gif
- PPP (3G cellular wireless, dial up POTS modems)
- 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 packet loss % or 100% down situations

Dashboard

- Allows quick access to system information

Load Balancer changes (relayd)

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

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

Post-2.0 release plans

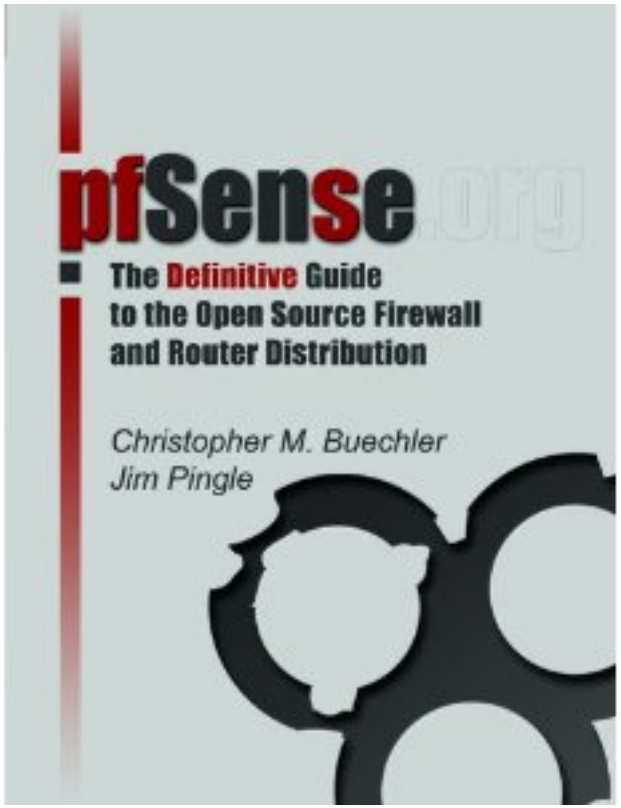
- Faster release cycles
- 2.1 features
  - Full IPv6 support
  - …?

Book

pfSense: The Definitive Guide [Paperback]

Christopher M. Buechler (Author), Jim Pingle (Author), Michael W. Lucas (Foreword)

(20 customer reviews)



Available for only $20 at the Reed Media table here at the conference

$33 from Amazon

Questions?

Comments?

Thanks for attending!

cmb@pfsense.org