Firewalling with pfSense

Ermal Luçi
E-mail: eri@pfsense.org

The speaker - Ermal

- Works full time on pfSense
- FreeBSD developer
- ISO 27001 Lead auditor
- <insert other 2,541 certs here>

History of pfSense

- Started by Scott Ullrich as a work project 15 years ago when we (Advertising Agency) needed a internal firewall
- Originally Linux, switched to FreeBSD 2.2
- Evolution of this path shrunk the firewall down to embedded
- Moatware was started
- Met Chris Buechler during this time
- Sell a number of products
- Sales guy moves to Florida
- Moatware fails
- pfSense is forked from m0n0wall roughly 7 years ago
- Still going strong today - momentum is snowballing

pfSense Overview

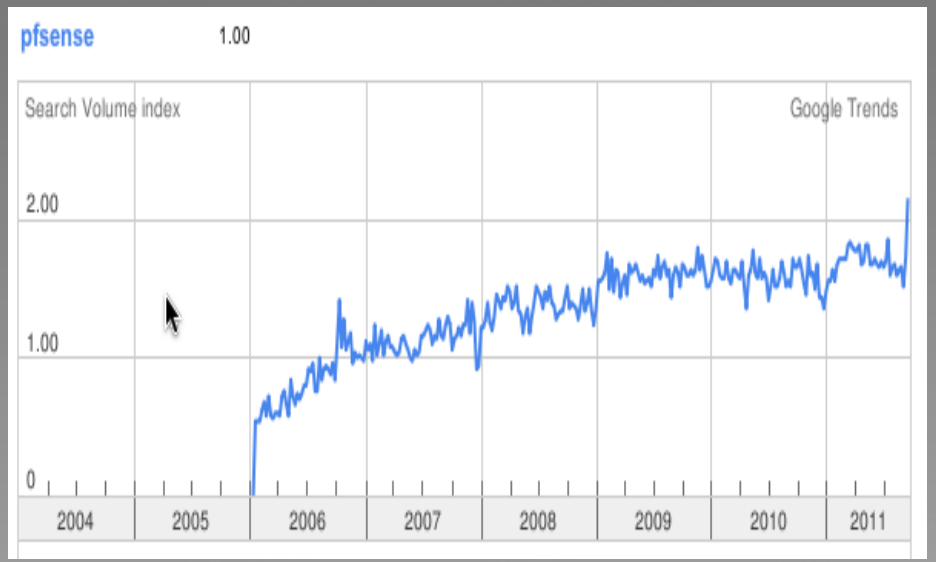
- Customized FreeBSD distribution tailored for use as a firewall and router.
- pfSense has many base features and can be extended with the package system including one touch installations of popular 3rd party packages such as SpamD (OpenBSD's spam filter) and Squid (web caching).
- Includes many features found in commercial products such as Cisco PIX, Sonicwall, Watchguard, etc.
- Many support avenues available, mailing lists, forum and commercial support.
- Has the best price on the planet.... Free!
- 2.0 released on 09/17/2011 based on FreeBSD 8.1

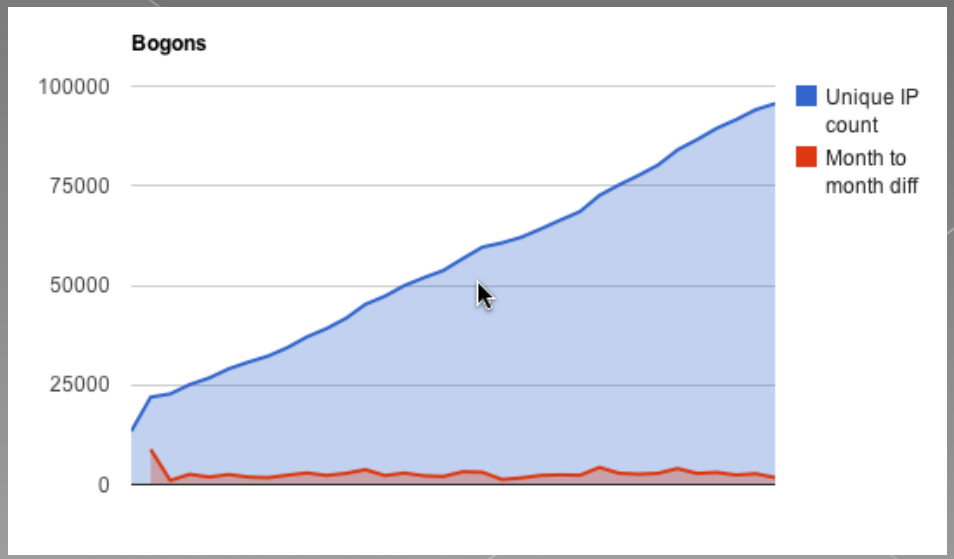
Why FreeBSD

- Primary reason was choosen on 2004
  - Wireless support
  - Network performance
  - Familiarity and ease of fork
  - Inadequate resources for multiple Oss
- Present reasons
  - Relationship with FreeBSD project
  - Attracted considerable FreeBSD talent
  - Performance now and into the future
- Downside
  - Old version of software, pf(4)

Project statistics

- millions of downloads served
- 27,914 forum members
- ~1200 mailing list users
- 25 developers
- 12 active developers (committed in the last year)
- Consistent Google growth
- 250+ IRC users on FreeNODE
- 100K+ unique IP addresses on bogons update





pfSense Platforms

- Live CD
- Full Install
- Embedded
- i386 / AMD64
- Memorystick

What all can pfSense do?

Firewalling - Protect one or more hosts
Routing - NAT, BGP, OSPF, RIP and more
VPN - Act as a VPN concentrator for road warriors
Wireless - Captive Portal
Multiwan - Use multiple internet connections
Load balancing - A form of using multiple internet connections
Quality of service (QoS)
HTTP Caching - Squid package
Intrusion Detection - Snort package
50+ packages available

Primary usage scenarios

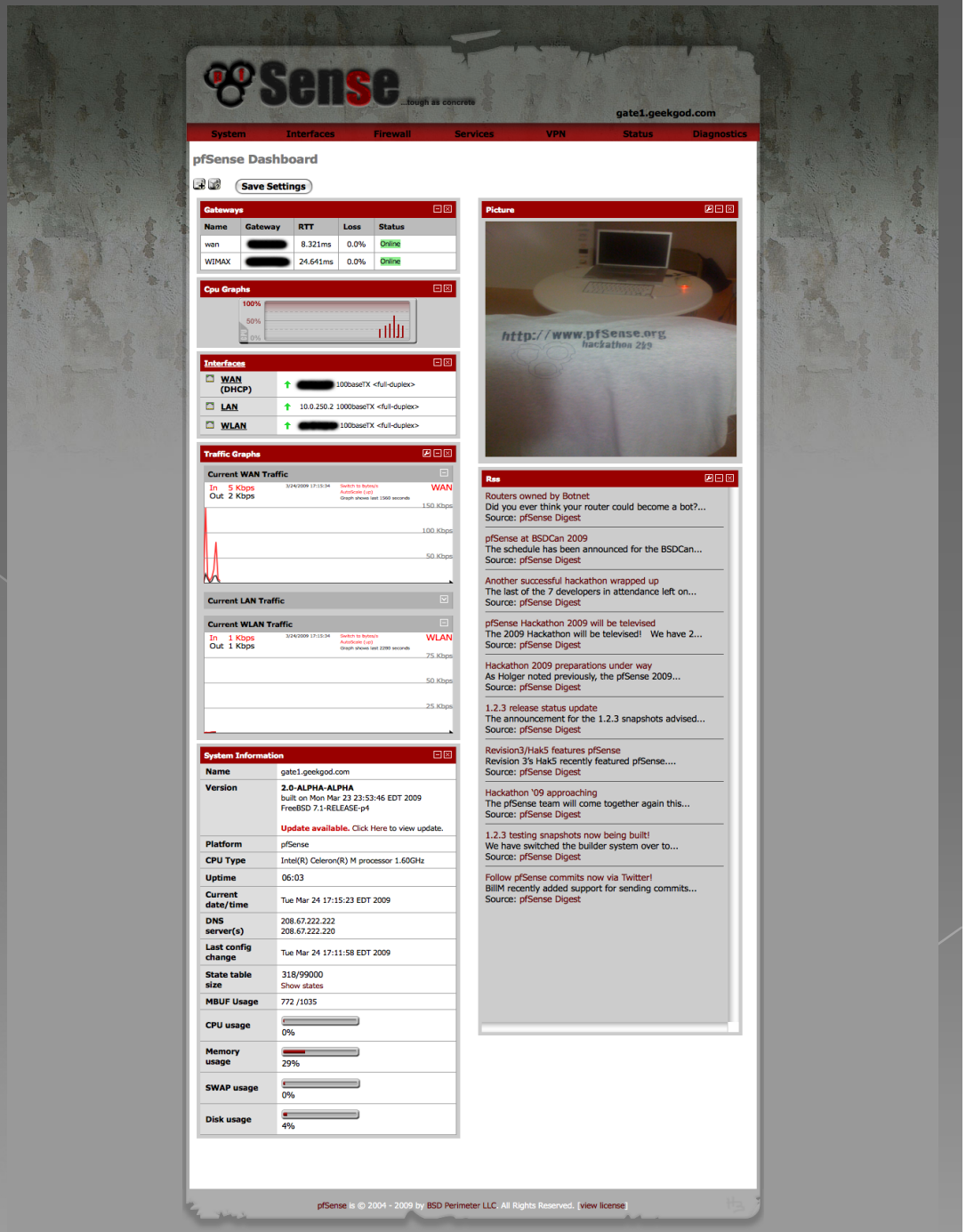
- Hosting/colocation environments
- ISPs / WISPs
- Hot spot providers
- Virtual firewalls
- Public sector
- Service providers
- Universities
- Non-profits
- Every type of business imaginable, small to large
  - Largely except huge companies
- Home users

Dashboard

- Allows quick access to system information
- Widgets include:

Available Widgets

- Captive Portal Status
- Carp Status
- Gateways
- Gmirror Status
- Installed Packages
- Interface Statistics
- Interfaces
- Ipsec
- Load Balancer Status
- Firewall Logs
- OpenVPN
- Picture
- Rss
- Services Status
- System Information
- Traffic Graphs
- Wake On Lan



Features present in 2.0.x

- Product of many years of development (3 years)
- Dashboard is the welcome screen
- Multi-wan improvements (many!)
- Network interface bonding
  - LAGG
  - Multi-link PPP
- Notifications (alerts) via SMTP and Growl
- QinQ (data centers & metro ethernet)
- Reworked alias support
  - Nested aliases
  - URL download (table aliases)

Features present in 2.0.x (cont.)

- Layer 7 (DPI) protocol filtering
  - Shaping
  - Blocking
- User manager
- Certificate manager
- OpenVPN integrated into Certificate manager
- Dial up PPP modem (3G)
- Upgraded to FreeBSD 8.1 base system
- IPSEC
  - GRE tunnel
  - GIF tunnel

Features present in 2.0.x (cont.)

- Captive portal
  - Vouchers
  - Multi-interface
  - Bandwidth control (QoS)
- Wireless
  - VAP (virtual access points)
- Global help screens available for every page

Features present in 2.0.x (cont.)

- Transparent bridging vastly improved
  - Spanning tree
  - Span Port
  - Edge ports - Connects to station, goes right to forwarding (like portfast)
  - PTP Ports (trunking) for linking to other bridges
  - Sticky ports that remember client addresses
  - Private ports - ports that cannot talk to other private ports, only public ports.

Features present in 2.0.x (cont.)

Many OpenVPN Improvements!

- Firewall rules for OpenVPN traffic
- Certificates (CA, Cert, CRL) managed in the GUI
- Shared keys can be generated in the GUI
- Status can be viewed for servers and clients
- Wizard to guide through setting up an authenticated remote access VPN, including creating necessary certificates.
- Client export package for exporting client configurations, including a Windows installer bundled with the certificates, and a Viscosity bundle.
- Improved security mechanisms
  - TLS authentication
  - User authentication, local users, RADIUS, LDAP
  - Matching of usernames to certificate common names
- GUI selection for available hardware acceleration

Features present in 2.0.x (cont.)

- Internationalization support - gettext()
- Improved packet capture
  - Can isloate ipv4/ipv6 traffic
  - Can capture on IPsec, OpenVPN as well as physical interfaces

Security by default

- HTTPS by default
- CSRF - Cross-site request forgery prevention
- DNS Rebinding detection
- HTTP Referrer check (alerts for possible MITM)
- Brute force lockout for:
  - webConfigurator
  - ssh
  - XMLRPC

What is brewing in 2.1

- ‘Full’ IPv6 support
- PBI (push button installer) package support
- OpenVPN per client policy from radius
- New PF features
  - New QoS ruleset that gets evaluated for every packet
    - Traffic total matching by host
    - Traffic total by session
    - Traffic size of packet
- J-Query
- Unbound - validating and caching DNS server
- Multi instance Captive Portal
- Stable release cycle - Target: 06/15/2012

After 2.1

- Full IPv6 support (include fragment handling)
- New PF features
  - Sync code with OpenBSD
  - Multi-core pf (scalability on multi-core machines)
- Captive Portal Payment clients (paypal, auth.net, etc..)
- IPSec NAT inside tunnel
- Periodic release cycle - Target: 6 months

Commercial Support available

Created by the founders of pfSense

- 8 employees working on various projects
- Services include
  - Rebranding
  - Technical Support
  - Custom development
  - Porting configuration from other devices (lots of PIXen)

More information

- https://portal.pfsense.org/

Any questions?

Thank you!

Visit us @ http://www.pfsense.org

Ermal Luçi- eri@pfsense.org