pfSense - 2.0 and beyond

Chris Buechler - cmb@pfsense.org
Scott Ullrich - sullrich@pfsense.org

History of pfSense

- Started as a work project 13 years ago when we needed a internal firewall
- Originally Linux, switched to FreeBSD 2.2
- Evolution of this path shrunk the firewall down to a Soekris size
- Moatware was started
- Met Chris Buechler during this time
- Sell a number of products
- Sales guy moves to Florida
- Moatware fails
- Chris and myself debate starting over fresh
- pfSense is forked from m0n0wall roughly 4 years ago
- Still going strong today - momentum is snowballing

pfSense Overview

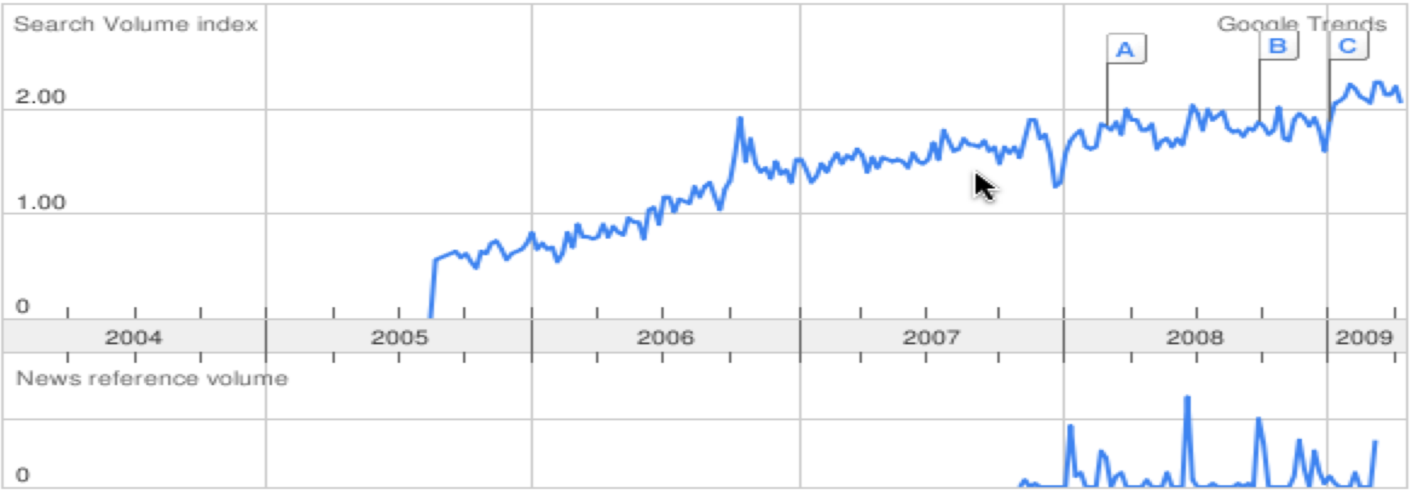
- Customized FreeBSD distribution tailored for use as a firewall and router.
- pfSense has many base features and can be extended with the package system including one touch installations of popular 3rd party packages such as SpamD (spam filter) and Squid (web caching).
- Includes many features found 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!

pfSense Platforms

- Live CD
- Full Install
- Embedded
- Developers

Project statistics

- millions of downloads served
- 11,400 forum members
- ~1200 mailing list users (support and discussion)
- 21 developers
- 12 active developers (committed in the last year)
- Consistent Google growth



New features (base)

- Layer 7 QoS
- New traffic shaper
- User Manager
- OpenVPN Improvements
- 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 interface support
- DHCP Server improvements
- PPTP Improvements
- New LIBALIAS based in-kernel FTP helper
- Improved load balancing (incoming and outgoing)

Layer 7 QoS improvements

- Based on regex matching system
- Detects BitTorrent very nicely
- Can detect between bulk and interactive traffic ?
- About X% overhead for L7
- PF peels off first X bytes of header for inspection via divert

New traffic shaper

- Rewritten from scratch by Ermal Luci
- Supports HFSC, CBQ, FairQ, PriQ
- Uses ALTQ
- Now works on more than 2 interfaces
- Supports bridging
- Pretty much all 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 (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
- 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 by Matthew Grooms
- Can now export a Windows Installer bundled with Certificates
- Now considered a first class VPN topology in pfSense

New interfaces

- GRE
- gif
- PPP (dial up POTS modems, 3G cellular wireless)
- Many 3G wireless additions
- 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

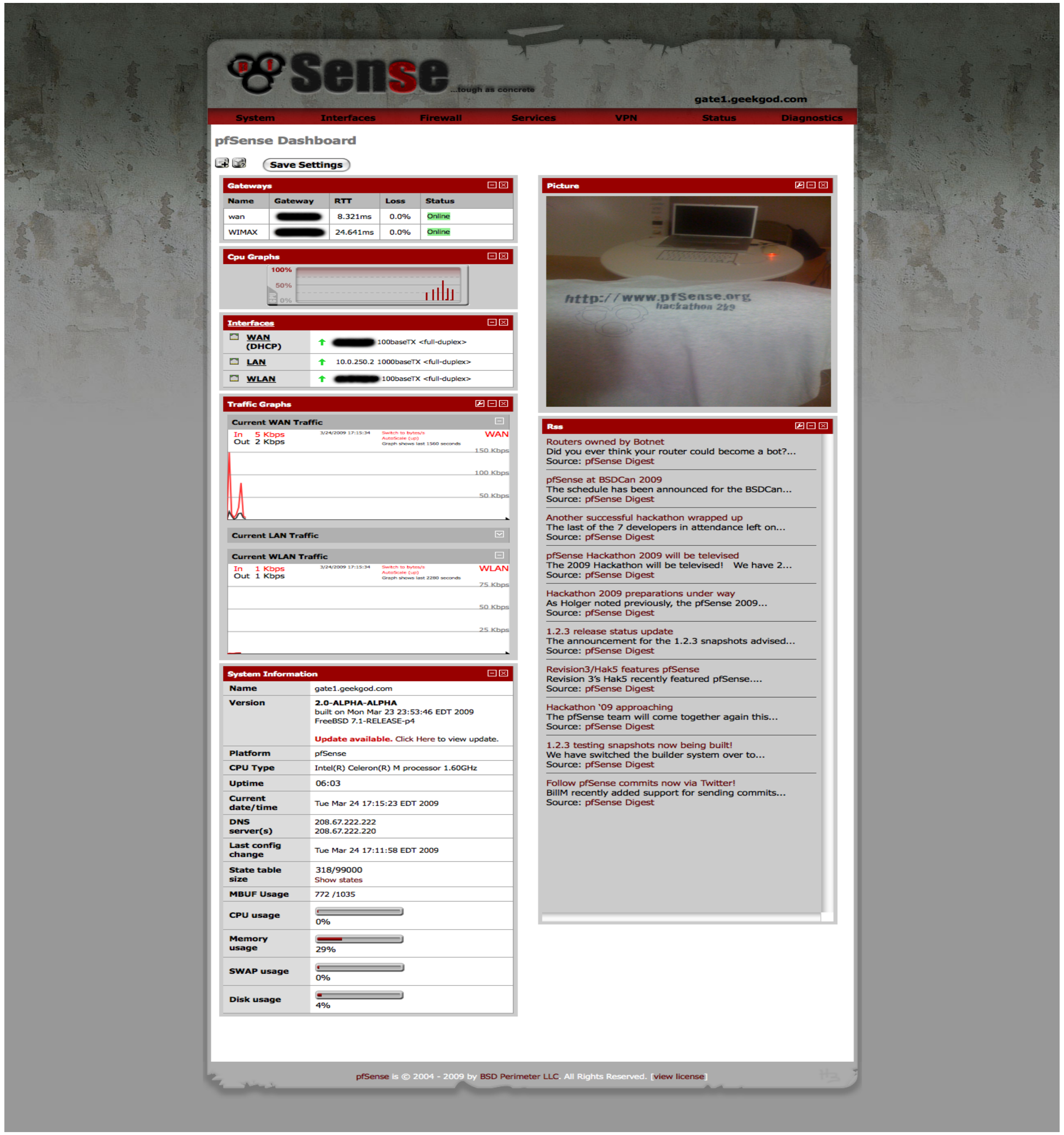
- Certificate authority support
- Generate OpenVPN certificates
- Generate user certificates
- Generate HTTPS certificate
- Generate IPsec certificates
- Revocation support
- Import existing certificates

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
- Added RSS widget
- Added picture widget
- Added gateways widget with RTT and loss reporting
- New AJAX CPU utilization widget



pfSense Dashboard

Gateways

Name	Gateway	RTT	Loss	Status
wan	[redacted]	8.321ms	0.0%	Online
WIMAX	[redacted]	24.641ms	0.0%	Online

Cpu Graphs

Interfaces

WAN (DHCP)	↑	[redacted] 100baseTX <full-duplex>
LAN	↑	10.0.250.2 1000baseTX <full-duplex>
WLAN	↑	[redacted] 100baseTX <full-duplex>

Traffic Graphs

Current WAN Traffic

In 5 Kbps
Out 2 Kbps
3/24/2009 17:15:34
Switch to bytes/s
AutoScale (up)
Graph shows last 1560 seconds
WAN

Current LAN Traffic

Current WLAN Traffic

In 1 Kbps
Out 1 Kbps
3/24/2009 17:15:34
Switch to bytes/s
AutoScale (up)
Graph shows last 2280 seconds
WLAN

System Information

Name	gate1.geekgod.com
Version	**2.0-ALPHA-ALPHA** built on Mon Mar 23 23:53:46 EDT 2009 FreeBSD 7.1-RELEASE-p4 **Update available.** Click Here to view update.
Platform	pfSense
CPU Type	Intel(R) Celeron(R) M processor 1.60GHz
Uptime	06:03
Current date/time	Tue Mar 24 17:15:23 EDT 2009
DNS server(s)	208.67.222.222 208.67.222.220
Last config change	Tue Mar 24 17:11:58 EDT 2009
State table size	318/99000 Show states
MBUF Usage	772 /1035
CPU usage	0%
Memory usage	29%
SWAP usage	0%
Disk usage	4%

Picture

Rss

Routers owned by Botnet
Did you ever think your router could become a bot?...
Source: pfSense Digest

pfSense at BSDCan 2009
The schedule has been announced for the BSDCan...
Source: pfSense Digest

Another successful hackathon wrapped up
The last of the 7 developers in attendance left on...
Source: pfSense Digest

pfSense Hackathon 2009 will be televised
The 2009 Hackathon will be televised! We have 2...
Source: pfSense Digest

Hackathon 2009 preparations under way
As Holger noted previously, the pfSense 2009...
Source: pfSense Digest

1.2.3 release status update
The announcement for the 1.2.3 snapshots advised...
Source: pfSense Digest

Revision3/Hak5 features pfSense
Revision 3's Hak5 recently featured pfSense....
Source: pfSense Digest

Hackathon '09 approaching
The pfSense team will come together again this...
Source: pfSense Digest

1.2.3 testing snapshots now being built!
We have switched the builder system over to...
Source: pfSense Digest

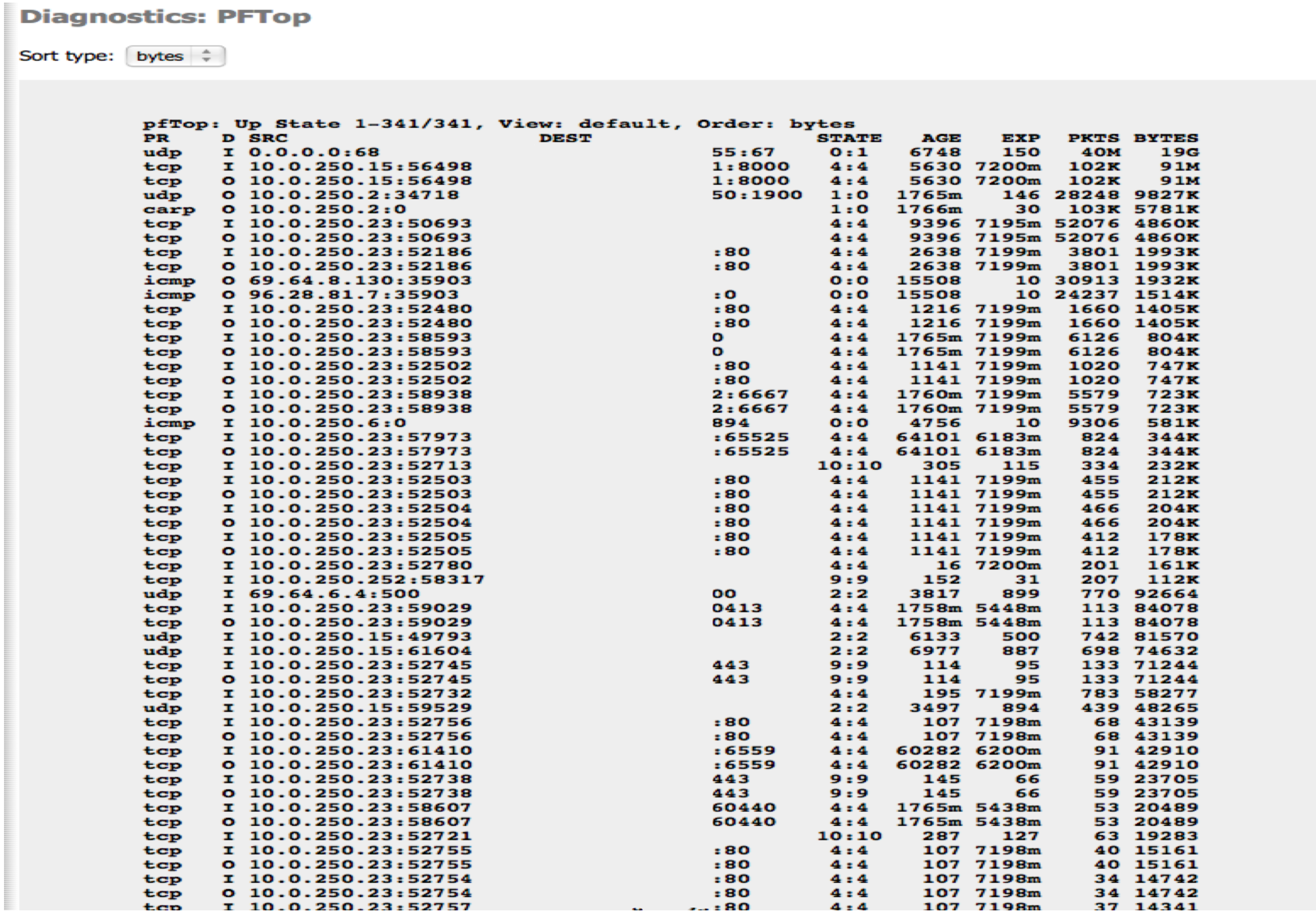
Follow pfSense commits now via Twitter!
BillM recently added support for sending commits...
Source: pfSense Digest

pfSense is © 2004 - 2009 by BSD Perimeter LLC. All Rights Reserved. [view license]

Load Balancer changes (relayd)

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

Web based pftop

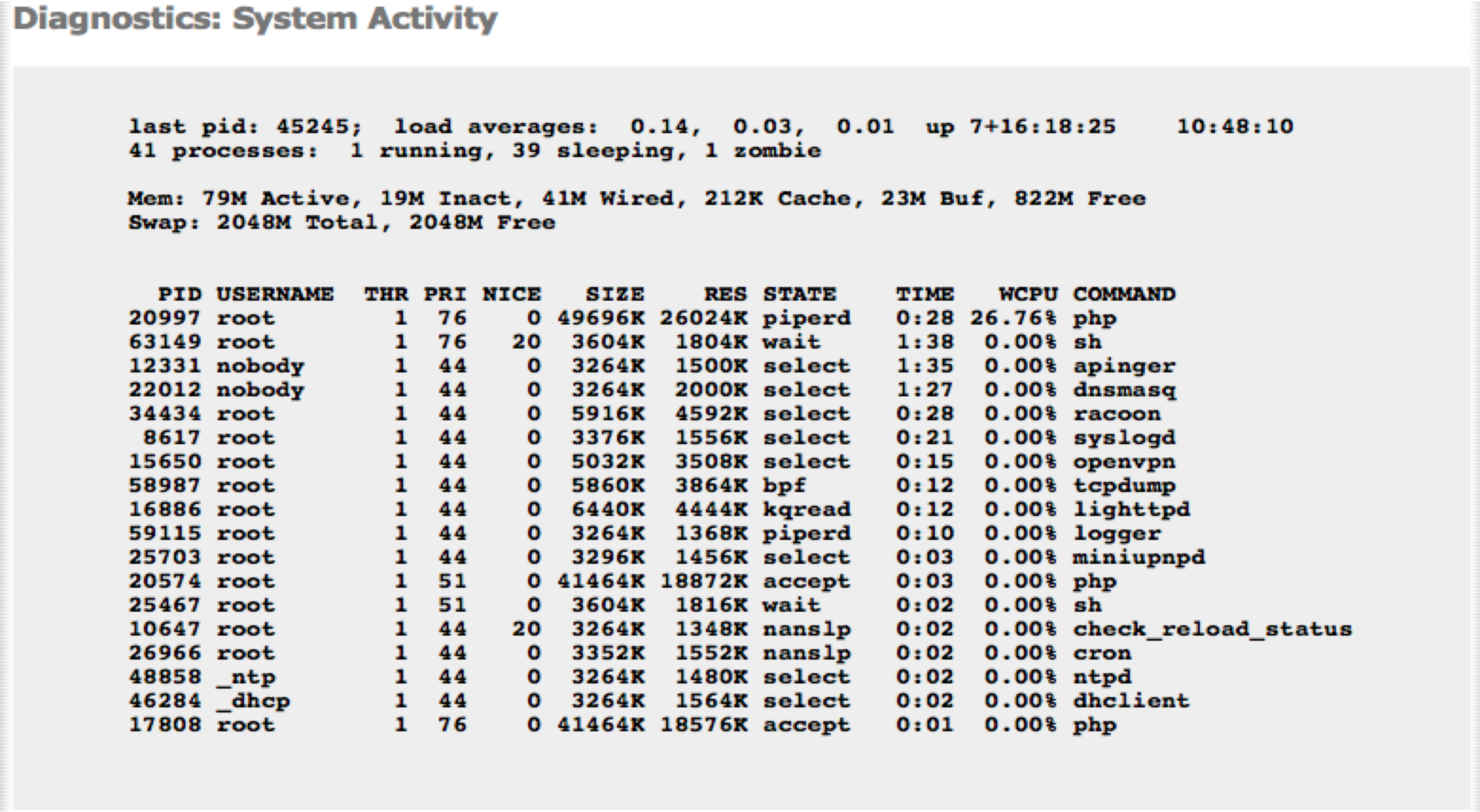


Diagnostics: PFTop

Sort type: bytes

```
pfTop: Up State 1-341/341, View: default, Order: bytes
PR    D SRC                   DEST                 STATE    AGE   EXP  PKTS BYTES
udp   I 0.0.0.0:68                         55:67     0:1    6748   150   40M   19G
tcp   I 10.0.250.15:56498                  1:8000    4:4    5630 7200m  102K   91M
tcp   O 10.0.250.15:56498                  1:8000    4:4    5630 7200m  102K   91M
udp   O 10.0.250.2:34718                   50:1900   1:0   1765m   146 28248 9827K
carp  O 10.0.250.2:0                                 1:0   1766m    30  103K 5781K
tcp   I 10.0.250.23:50693                            4:4    9396 7195m 52076 4860K
tcp   O 10.0.250.23:50693                            4:4    9396 7195m 52076 4860K
tcp   I 10.0.250.23:52186                  :80       4:4    2638 7199m  3801 1993K
tcp   O 10.0.250.23:52186                  :80       4:4    2638 7199m  3801 1993K
icmp  O 69.64.8.130:35903                            0:0   15508    10 30913 1932K
icmp  O 96.28.81.7:35903                   :0        0:0   15508    10 24237 1514K
tcp   I 10.0.250.23:52480                  :80       4:4    1216 7199m  1660 1405K
tcp   O 10.0.250.23:52480                  :80       4:4    1216 7199m  1660 1405K
tcp   I 10.0.250.23:58593                  0         4:4   1765m 7199m  6126  804K
tcp   O 10.0.250.23:58593                  0         4:4   1765m 7199m  6126  804K
tcp   I 10.0.250.23:52502                  :80       4:4    1141 7199m  1020  747K
tcp   O 10.0.250.23:52502                  :80       4:4    1141 7199m  1020  747K
tcp   I 10.0.250.23:58938                  2:6667    4:4   1760m 7199m  5579  723K
tcp   O 10.0.250.23:58938                  2:6667    4:4   1760m 7199m  5579  723K
icmp  I 10.0.250.6:0                       894       0:0    4756    10  9306  581K
tcp   I 10.0.250.23:57973                  :65525    4:4   64101 6183m   824  344K
tcp   O 10.0.250.23:57973                  :65525    4:4   64101 6183m   824  344K
tcp   I 10.0.250.23:52713                           10:10    305   115   334  232K
tcp   I 10.0.250.23:52503                  :80       4:4    1141 7199m   455  212K
tcp   O 10.0.250.23:52503                  :80       4:4    1141 7199m   455  212K
tcp   I 10.0.250.23:52504                  :80       4:4    1141 7199m   466  204K
tcp   O 10.0.250.23:52504                  :80       4:4    1141 7199m   466  204K
tcp   I 10.0.250.23:52505                  :80       4:4    1141 7199m   412  178K
tcp   O 10.0.250.23:52505                  :80       4:4    1141 7199m   412  178K
tcp   I 10.0.250.23:52780                            4:4      16 7200m   201  161K
tcp   I 10.0.250.252:58317                           9:9     152    31   207  112K
udp   I 69.64.6.4:500                      00        2:2    3817   899   770 92664
tcp   I 10.0.250.23:59029                  0413      4:4   1758m 5448m   113 84078
tcp   O 10.0.250.23:59029                  0413      4:4   1758m 5448m   113 84078
udp   I 10.0.250.15:49793                            2:2    6133   500   742 81570
udp   I 10.0.250.15:61604                            2:2    6977   887   698 74632
tcp   I 10.0.250.23:52745                  443       9:9     114    95   133 71244
tcp   O 10.0.250.23:52745                  443       9:9     114    95   133 71244
tcp   I 10.0.250.23:52732                            4:4     195 7199m   783 58277
udp   I 10.0.250.15:59529                            2:2    3497   894   439 48265
tcp   I 10.0.250.23:52756                  :80       4:4     107 7198m    68 43139
tcp   O 10.0.250.23:52756                  :80       4:4     107 7198m    68 43139
tcp   I 10.0.250.23:61410                  :6559     4:4   60282 6200m    91 42910
tcp   O 10.0.250.23:61410                  :6559     4:4   60282 6200m    91 42910
tcp   I 10.0.250.23:52738                  443       9:9     145    66    59 23705
tcp   O 10.0.250.23:52738                  443       9:9     145    66    59 23705
tcp   I 10.0.250.23:58607                  60440     4:4   1765m 5438m    53 20489
tcp   O 10.0.250.23:58607                  60440     4:4   1765m 5438m    53 20489
tcp   I 10.0.250.23:52721                           10:10    287   127    63 19283
tcp   I 10.0.250.23:52755                  :80       4:4     107 7198m    40 15161
tcp   O 10.0.250.23:52755                  :80       4:4     107 7198m    40 15161
tcp   I 10.0.250.23:52754                  :80       4:4     107 7198m    34 14742
tcp   O 10.0.250.23:52754                  :80       4:4     107 7198m    34 14742
tcp   I 10.0.250.23:52757                  :80       4:4     107 7198m    37 14341
```

Web based top



Diagnostics: System Activity

```
last pid: 45245;  load averages:  0.14,  0.03,  0.01  up 7+16:18:25    10:48:10
41 processes:  1 running, 39 sleeping, 1 zombie

Mem: 79M Active, 19M Inact, 41M Wired, 212K Cache, 23M Buf, 822M Free
Swap: 2048M Total, 2048M Free


  PID USERNAME  THR PRI NICE   SIZE    RES STATE    TIME   WCPU COMMAND
20997 root        1  76    0 49696K 26024K piperd   0:28 26.76% php
63149 root        1  76   20  3604K  1804K wait     1:38  0.00% sh
12331 nobody      1  44    0  3264K  1500K select   1:35  0.00% apinger
22012 nobody      1  44    0  3264K  2000K select   1:27  0.00% dnsmasq
34434 root        1  44    0  5916K  4592K select   0:28  0.00% racoon
 8617 root        1  44    0  3376K  1556K select   0:21  0.00% syslogd
15650 root        1  44    0  5032K  3508K select   0:15  0.00% openvpn
58987 root        1  44    0  5860K  3864K bpf      0:12  0.00% tcpdump
16886 root        1  44    0  6440K  4444K kqread   0:12  0.00% lighttpd
59115 root        1  44    0  3264K  1368K piperd   0:10  0.00% logger
25703 root        1  44    0  3296K  1456K select   0:03  0.00% miniupnpd
20574 root        1  51    0 41464K 18872K accept   0:03  0.00% php
25467 root        1  51    0  3604K  1816K wait     0:02  0.00% sh
10647 root        1  44   20  3264K  1348K nanslp   0:02  0.00% check_reload_status
26966 root        1  44    0  3352K  1552K nanslp   0:02  0.00% cron
48858 _ntp        1  44    0  3264K  1480K select   0:02  0.00% ntpd
46284 _dhcp       1  44    0  3264K  1564K select   0:02  0.00% dhclient
17808 root        1  76    0 41464K 18576K accept   0:01  0.00% php
```

IGMP Proxy

- Useful for Video in some cases
- Some phone systems use IGMP for overhead speakers
- IP TV
- Gaming

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
- Network booting related additions
    - Next-server
    - Filename
    - root-path-string

New features (packages)

- Jails
- FreeSWITCH
- Squid 3
- Avahi
- Open-VM Tools
- PHP Service
- OpenVPN Client Export Utility (Windows)
- TFTP Server (useful for upgrading Cisco/HP Switches, etc)

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
- We will go over a quick appliance build later in this presentation

FreeSWITCH Appliance

Can be run on pfSense directly or as a dedicated appliance.
Features:

- Voice Mail
- Voice Mail to e-mail (one or more email addresses, also can be sent to special email addresses for SMS Text Messages)
- Auto Attendant
- Music on Hold (.wav)
- Recordings
- Follow Me
- Text to Speech (flite)

FreeSWITCH Appliance

Features Continued:

- Call Park
- Call Forward
- DISA (Direct Inward/Outward System Access)
- Call Queues
- SIP (TLS) and SRTP and more.
- Simple to call between multiple systems using the Internet.
- Call Eavesdrop (aka barge)
- Call Recording
- Call Intercept by Group, Global, Extension

FreeSWITCH Appliance

Features Continued:

- Call Park
- Google 411

Email: markjcrane@gmail.com

Wiki: http://doc.pfsense.org/index.php/FreeSWITCH

IRC: #pfsense-freeswitch

DNS Server Appliance

- Many features removed such as DHCP Server, VPN, etc
- Two versions released so far, newest based on FreeBSD 8
- Based on TinyDNS from DJ Bernstein
- Automatically synchronizes changes to 5 other hosts
- Automatically fail to backup records on host failure using ICMP
- Automatically fail to backup record if WAN RTT > X
- Automatically fail to backup record if RTT to host Y.Y.Y.Y > X
- Zone transfer support for the BIND folks
- Configuration data stored in master config.xml file

Creating an appliance (overview)

- Install FreeBSD 7
- Follow http://devwiki.pfsense.org/DevelopersBootStrapAndDevIso
- Excute these shell commands:
  - cd /home/pfsense/tool/builder_scripts
  - cp builder_profiles/pfDNS/pfsense_local.sh
  - ./build_iso.sh

Creating your own appliance (Overview)

- `cd /home/pfsense/tools/builder_scripts/builder_profiles/`
- `cp -R pfDNS MyAppliance && cd MyAppliance`
- `grep -R "pfDNS" * | cut -d":" -f1 | sort -u`

  ```
  README
  config/config.xml
  copy_overlay/boot/beastie.4th
  copy_overlay/etc/inc/globals.inc
  copy_overlay/usr/local/share/dfuibe_lua/conf/pfSense.lua
  pfsense_local.sh
  ```
- Edit the above files to your liking

Building your appliance (overview)

- `cd /home/pfsense/tools/builder_scripts`
- `cp builder_profiles/MyAppliance/pfsense_local.sh .`
- `./build_iso.sh`
- See http://devwiki.pfsense.org/CreatingAnAppliance

BSD Perimeter milestones

- Chris is now working Full Time
- BSD Perimeter coordinating MIPS port for RouterStation
- pfSense book will be released in the next couple months
- Commercial support is growing with satisfied customers
- Sponsored IPsec improvements
- Sponsoring various misc projects on behalf of customer, IGMP package for 1.2.*, etc

Questions?

Comments?

Thanks for attending!

sullrich@pfsense.org
cmb@pfsense.org