pfSense Tutorial

BSDCan 2008

From zero to hero with pfSense

May 13, 2008

Chris Buechler <cmb@bsdperimeter.com>
Scott Ullrich <sullrich@bsdperimeter.com>

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

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

pfSense Stable Versions

1.0 - October 4, 2006 *

1.0.1 - October 20, 2006 *

1.2 - RELENG_1_2 - February 25, 2008

- Downloaded more than 500,000 times to date

* Not branched in CVS

pfSense Development Versions

Current Development Versions

- 1.3-ALPHA - RELENG_1
- 2.0-ALPHA-ALPHA-ALPHA - HEAD

Snapshots are built every two hours
available at http://snapshots.pfsense.org

Bonus for attendees - 1.3 snapshots available

Minimum Hardware Requirements

CPU - 100 MHz (500+ MHz for best experience)

RAM - 128 MB (256 MB or more is encouraged)

Platform Specific

- Live CD
  - CD-ROM drive (currently USB CD-ROM devices are not supported)
  - USB flash drive or floppy drive to store configuration
- Full Installation
  - CD-ROM for initial installation
  - 1 GB hard drive
- Embedded
  - 128 MB CF
  - serial port for console
  - null modem cable

Popular hardware

- NICs - Intel Pro/100 and Pro/1000
- Embedded hardware
  - PC Engines WRAP and ALIX
  - Soekris
  - Nexcom
  - Hacom
  - Mini ITX
- Most Dell servers work well
- Many HP and Compaq servers work well
- VMware - entire product line

Hardware Sizing Guidance

Throughput Considerations

- Packets per second
- Bandwidth required
  - 10-20 Mbps - No less than 266 MHz CPU
  - 21-50 Mbps - No less than 500 MHz CPU
  - 51-200 Mbps - No less than 1.0 GHz CPU
  - 201-500 Mbps - server class or newer desktop hardware
    - PCI-x or PCI-e network adapters
    - No less than 2.0 GHz CPU
  - 501+ Mbps - server class hardware
    - PCI-x or PCI-e network adapters
    - No less than 3.0 GHz CPU

Hardware Sizing Guidance

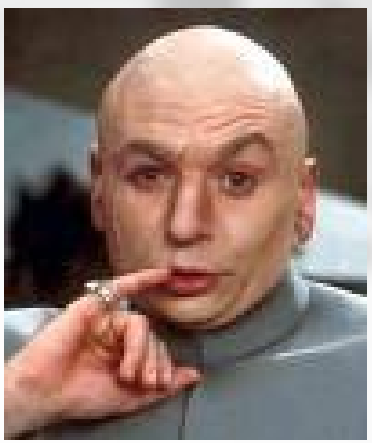
Feature Considerations

- VPN
  - Number of connections not much of a factor
  - Very CPU intensive
  - Throughput
    - 4 Mb - 266 MHz
    - 10 Mb - 500 MHz

Hardware Sizing Guidance

Feature Considerations

- Large and busy Captive Portal deployments
  - Increased CPU requirements
- Large state tables
  - 1 KB per state RAM requirement
    - 100,000 states = ~97 MB RAM
    - 500,000 states = ~488 MB RAM
    - 1,000,000 states = ~976 MB RAM
    - etc...



One million states!

Hardware Sizing Guidance

Feature Considerations

- Packages
  - RAM hungry
    - ntop
    - Snort
  - Disk I/O
    - Squid

Common Deployments

(that we're aware of)

- Perimeter firewall
  - BGP router
- LAN router
  - VLAN
  - Multiple interfaces
- WAN router
  - for Ethernet WAN services

Common Deployments

(that we're aware of)

- Appliance deployments
  - DHCP server
  - VPN server
  - Packet capture appliance
- Portable monitoring and incident response

Organizations Using pfSense

(that we're aware of)

Advertising Agencies
Application service providers
Banks
Credit unions
Churches
Coffee shops
Co-location facilities
Clothing/Apparel manufacturers
Homes
Hospitals
Hotels
Libraries
Cable TV networks
Small to mid sized ISPs
Movie studios
Restaurants
Schools
Universities
WISPs
Wineries
... and many more!

Classless InterDomain Routing (CIDR)

Subnet Mask	CIDR Prefix	Total IP Addresses	Usable IP Addresses	Number of /24 networks
255.255.255.255	/32	1	1	1/256th
255.255.255.254	/31	2	0	1/128th
255.255.255.252	/30	4	2	1/64th
255.255.255.248	/29	8	6	1/32nd
255.255.255.240	/28	16	14	1/16th
255.255.255.224	/27	32	30	1/8th
255.255.255.192	/26	64	62	1/4th
255.255.255.128	/25	128	126	1 half
255.255.255.0	/24	256	254	1
255.255.254.0	/23	512	510	2
255.255.252.0	/22	1024	1022	4
255.255.248.0	/21	2048	2046	8
255.255.240.0	/20	4096	4094	16
255.255.224.0	/19	8192	8190	32
255.255.192.0	/18	16,384	16,382	64

CIDR Summarization

Allows specification of IP ranges

- Firewall rules
- NAT
- IPsec

Must fall in subnet boundaries

<u>Examples</u>

192.168.0.0 - 192.168.3.255 = 192.168.0.0/22

10.0.0.48 - 10.0.0.63 = 10.0.0.48/28

www.subnetmask.info

Live Demo s

Running the LiveCD using a USB Keychain.

Full installation to hard disk.

Live Demo

Full installation using LiveCD.

Live Demo s

Installing to drive in VMware

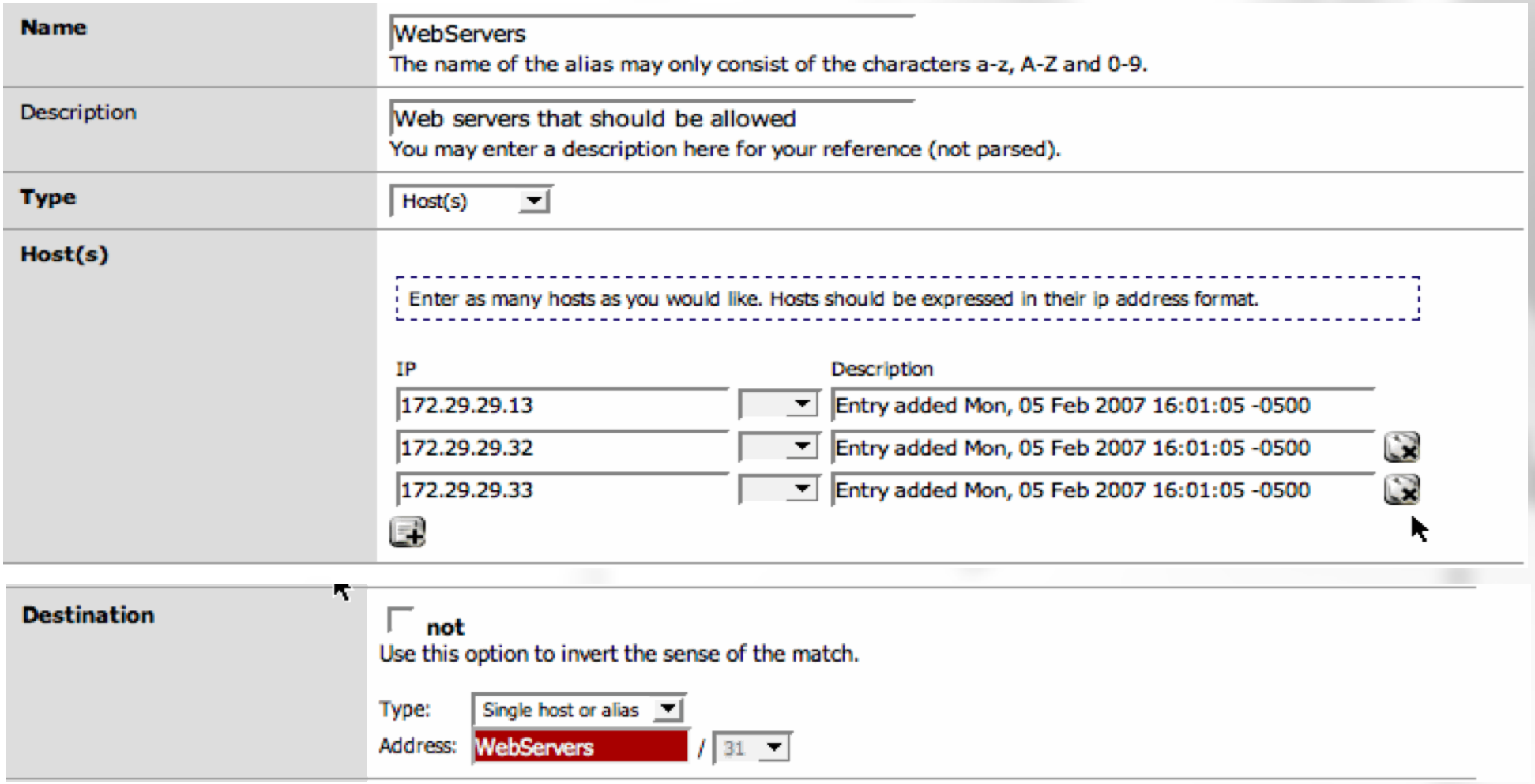
Installing with drive in another machine

Initial Configuration

- Assigning network interfaces
- Setting the LAN IP address
- Browsing into the pfSense webConfigurator
- Walk through the initial setup wizard
- Setup firewall rules for LAN and WAN interfaces
- Setup any additional NAT port forwards or 1:1 entries
- Ensure FTP helper is working as needed

Firewall aliases

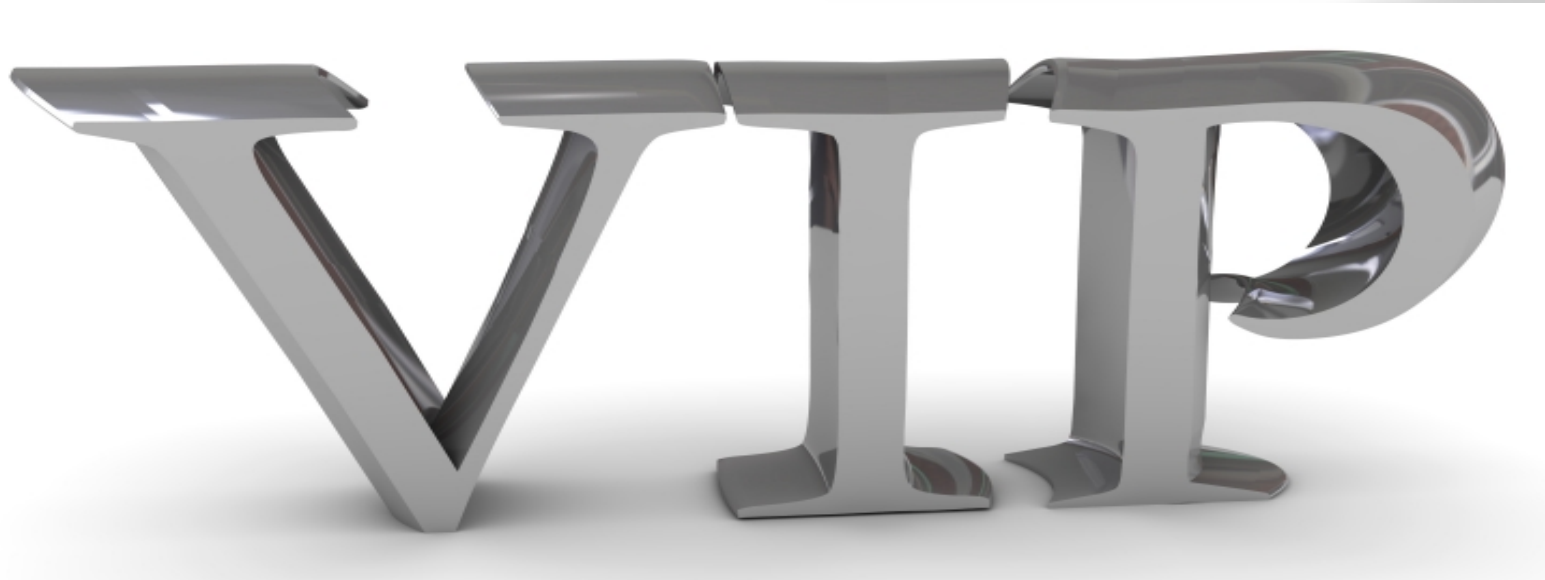
- Allows grouping of multiple IPs, subnets or ports.
- Can vastly simplify and reduce your rule sets.
- Red input boxes are alias friendly.



Firewall - VIPs

Uses

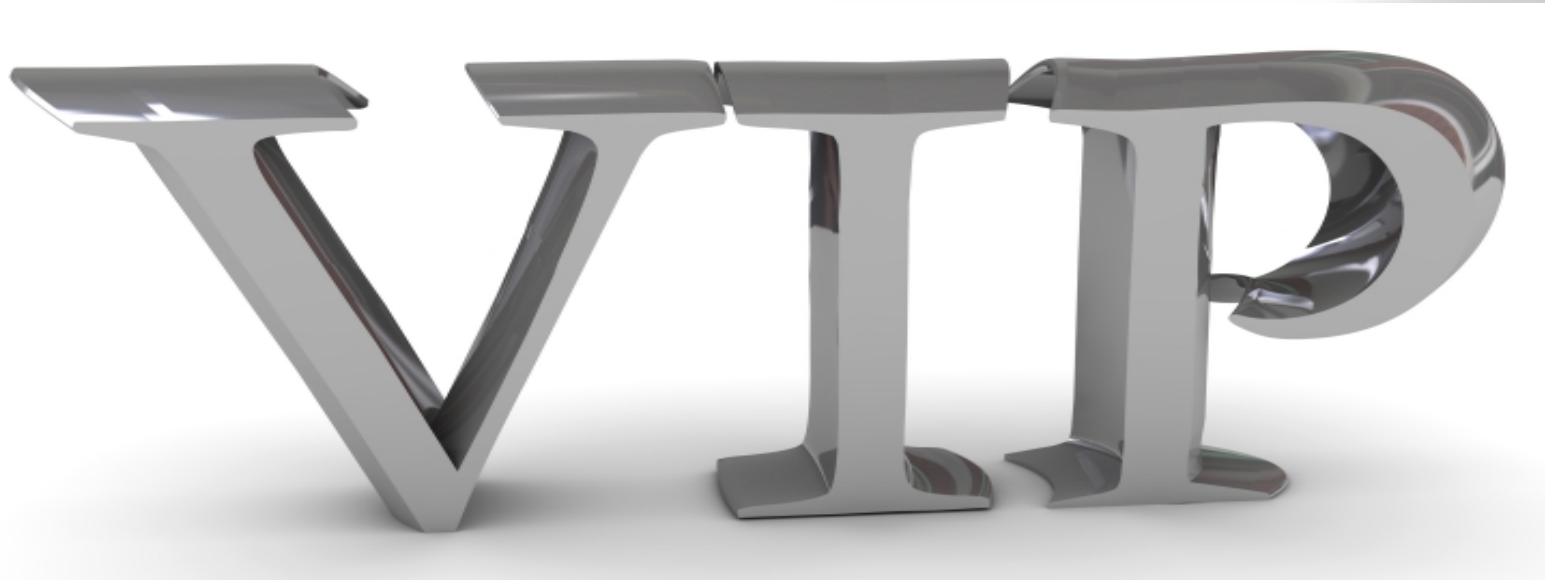
- Additional public IPs for use with NAT
- CARP deployments



Firewall - VIPs

Types

- Proxy ARP
- CARP
- Other



Firewall Rules

- Firewall rules are always evaluated on incoming traffic (therefore rules have to go to the interface tha traffic is initiated from)
- If a connection was allowed (like a client at LAN requesting a webpage from a server at WAN) it will create a state. The reverse connection (the server at WAN sending the content to the client at LAN) will then be allowed automatically (no rule at interface WAN is needed).
- Rules are always applied on a first match basis from top to down.

Firewall Rules - Troubleshooting

- Enable logging on rules
- Check firewall log in Status -> System logs -> Firewall
  - Click action icon (block, pass, reject)
- Source port is not the same as destination port
- Diagnostics -> States offers additional information for passed traffic especially in multi-WAN environments
- WAN rules - NAT applies first
  - Use private IPs as destination in NAT rules

NAT

Directions

- Outbound
  - Internal network(s) to Internet
- Inbound
  - Internet to internal network(s)

Default Configuration

- Outbound
  - NAT to WAN IP (or to any OPT-Interface that has a gateway set)
- Inbound
  - Nothing permitted

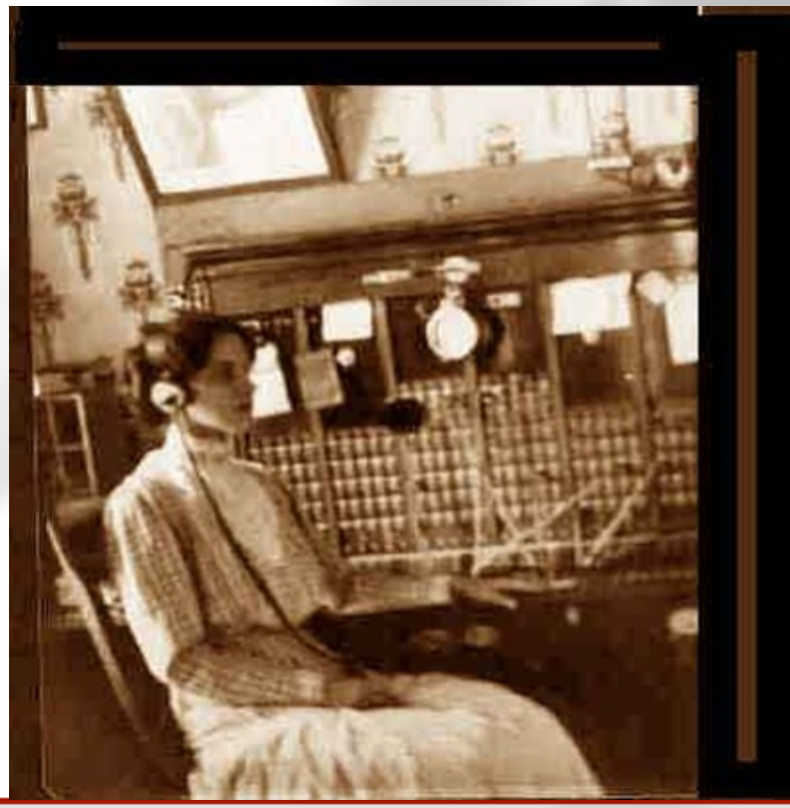
NAT - Inbound

- Simple port forwarding
- 1:1 NAT
- Does not forward connections from the LAN -> WAN -> LAN without enabling NAT Reflection

NAT - 1:1

Slightly different process than with other commercial products:

- Create a VIP (only CARP IPs can be used by the firewall itself, other VIPs can only be forwarded)
- Create a 1:1 NAT mapping between the VIP and an internal host
- Create firewall rules allowing traffic the the internal host address
- Troubleshooting - ICMP doesn't work with PARP; 1:1 NAT won't work with NAT-reflection



NAT - Outbound

- Default configuration
  - NAT all traffic out WAN to WAN IP
  - NAT all traffic out OPT WANs to OPT WAN IP
- Advanced Outbound NAT
  - Manual NAT rule creation
- Static Port

Live demo

FTP Considerations

- When using the FTP Helper and VIPs, the type must be set to CARP.
- FTP only works on primary WAN
- The helper can be disabled if you wish to port forward TCP port 21 and the TCP data port ranges that are setup in the FTP server (or use 1:1 NAT). Don't forget to permit the traffic with firewall rules!

Multi-WAN

- Ability to use multiple Internet connections
- Most are dual WAN
- Multiple installs with 6 or more WANs

Why use multi-WAN?

- Provide Internet redundancy
- Aggregate bandwidth

Multi-WAN

- Interface configuration
- Policy routing overview
- Load balancing caveats
  - Some applications do not work with load balancing (like https, ftp, sip ... use failoverpools for these)
  - Do not use sticky connections (apparently broken)
- Caveats: Services running on pfSense (like squid, DNS, IPsec) can't make use of load balancing or policy based routing. They will use the system's default gateway (you'll need to add some static routes for DNS servers or IPsec-endpoints on OPT WANs)

Multi-WAN - Choosing Connectivity

- Check and price available service
  - Cable
  - DSL
  - Metro Ethernet
  - T1
  - Fixed wireless
  - etc...
- Reliability
- Disparate ISP networks
- Cable path

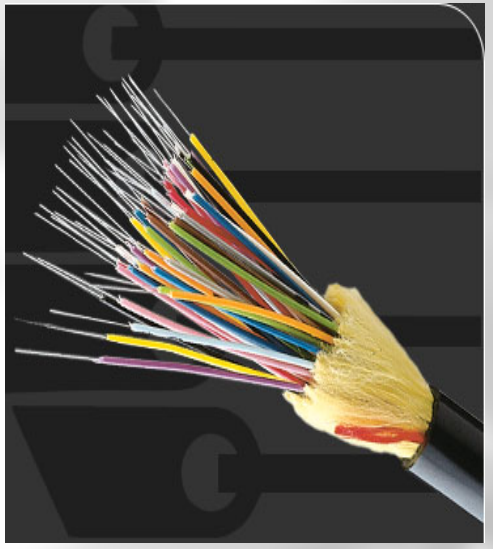
Multi-WAN - Choosing Connectivity

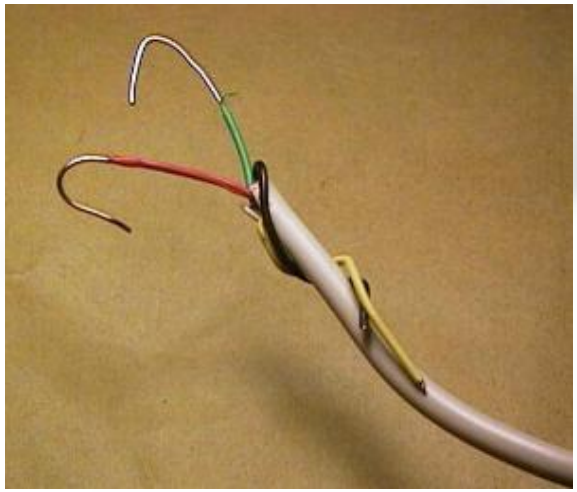
Cable seeking backhoe

Multi-WAN - Choosing Connectivity

Cable paths

- Copper services
  - T1
  - DSL
  - etc.
- Cable services
- Fiber services
  - Metro Ethernet
- Fixed Wireless





Multi-WAN and Outbound NAT

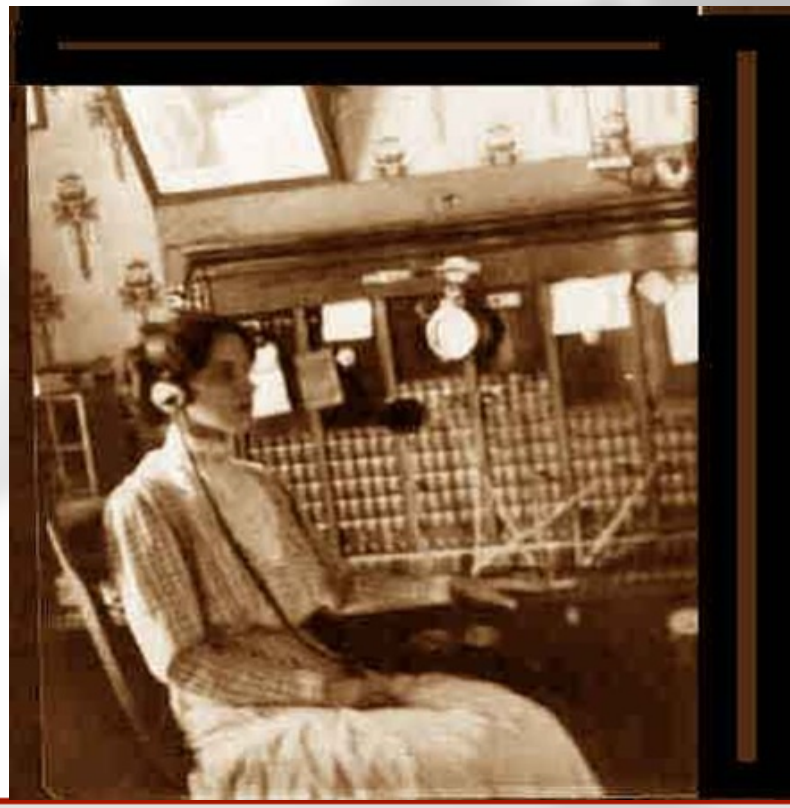
- Default outbound NAT config
  - Translates outbound traffic to IP of WAN used
- Advanced Outbound NAT

Multi-WAN and Inbound NAT

- Each port forward applies to one WAN

Multi-WAN and 1:1 NAT

- Each 1:1 NAT entry tied to specific WAN
- Host can have multiple 1:1 entries, one per WAN



Multi-WAN Failover

Enables a secondary WAN link to be used in the event the primary WAN goes offline.

- Create a Gateway Pool for failover
  - Ensure that monitor IPs are nearby and reliably respond to ICMP (not the physical link determines if a WAN is down but the failure of the monitoring ping)
- Add interfaces to the pool
- Modify the default LAN rule to use the failover pool as the gateway
- Create static routes for WAN2 DNS Servers

Multi-WAN Load Balancing

- Round robin equal distribution among selected WAN interfaces
- Not capable (yet) of unequal load distribution
- Requires unique gateway IP for each WAN (adds static routes behind the scenes for monitors to make the monitor pings leave through the correct WAN)
- Sticky connections not functional

Multi-WAN Load Balancing

- Round robin equal distribution among selected WAN interfaces
- Not capable (yet) of unequal load distribution
- Requires unique gateway IP for each WAN
- Create a Load Balancer Pool of type "Load Balancing"
  - Ensure monitor IPs are nearby and respond reliably to ICMP
- Add interfaces to the pool
- Modify the default LAN rule to use the load balancer pool as the gateway
- Create policy-based routes for WAN2 DNS Servers and non-balanced applications

VPN Capabilities

- IPsec (with filtering support)
- PPTP (with filtering support)
- OpenVPN (filtering available in 1.3)
- L2TP might appear in 1.3

VPN Uses

- Remote Access
  - IPsec
  - PPTP
  - OpenVPN
- Site to site connectivity
  - IPsec
  - OpenVPN

IPsec

- Site to site
  - Variable configuration options between vendor implementations, sometimes a square is actually a circle
  - Always double and triple check configurations on both sides of the tunnel

IPsec Site to Site Static IP

Static public IPs on both ends

- At each endpoint, create a tunnel on the interface which sees the traffic (typically WAN)
  - Do not duplicate remote subnets
- Ensure that Phase 1 and Phase 2 options match on both tunnels _exactly_
- Create firewallrules to allow traffic in coming from the tunnel (firewall -> rules, ipsec)

IPsec Site to Site Dynamic IP

Static IP on one end, dynamic on the other

- Make the endpoint with the static IP to allow mobile clients (vpn -> ipsec, mobile clients)
- Add identifiers to be used by the dynamic remote system (vpn>ipsec, preshared keys)
- On the dynamic endpoint system setup a static tunnel (vpn -> ipsec, tunnels). Use the same parameters as the static end on the mobile clients tab. Use the preshared key that you generated as identifier and secret.
- Hint: tunnel to tunnel routing works if you use a subnetmask with all remote subnets of dynamic endpoints at the static endpoint

OpenVPN

- Open source SSL VPN solution
- less problematic behind NAT (other then PPTP or IPSEC)
- Cross platform client support
  - Windows 2000, XP, 2003, Vista, 2008
  - Mac OS X
  - FreeBSD
  - NetBSD
  - OpenBSD
  - Linux
  - Windows Mobile (Pocket PC) - alpha

OpenVPN Certificate Generation

Keys must be generated on another system with 1.2

1.3 already includes all certificate management in the web interface)

Organizations with existing PKI should use it

Quick and easy way - easyrsa included with OpenVPN

PPTP Considerations

- Currently more than one client behind pfSense cannot connect to the same PPTP server at the same time
- GRE state is not kept by PF which can cause strange behavior when PPTP server is enabled for clients behind pfSense
- we'll hopefully have a fix for this in 1.3

PPPoE Server

Point to Point Protocol over Ethernet

- Layer 2 protocol using PPP
- Creates one to one network link with server
- RADIUS authentication

Common usages

- Internet Service Providers
- Locked down wireless deployments
- Anywhere layer 2 authentication is desirable

Traffic Shaper - what it is and isn't

- Current implementation in 1.2 is very limited
- Only suitable for two interface deployments - LAN and WAN
- No IPsec shaping
- Shaping at layers 3 and 4
  - No deep packet inspection
  - No application layer shaping

Traffic Shaper

- Always start with the EZ Shaper Wizard
  - Penalty Box may be IPs or an alias
  - Ensure all VOIP-participants and server IP addresses belong to an alias
  - P2P Catch-all which puts any unclassified traffic into the P2P queue.
- Editing shaper rules
  - IP TOS and TCP Flags are used to determine match, not re-written

Routing

- Disabling NAT
- Routing Protocols
  - BGP (available in packages)
  - RIP (v1 and v2)

Server Load Balancing

- Load balance traffic across multiple servers
  - Configure a server pool
  - Assign a virtual server address
  - Create firewall rules allowing traffic to server pool
- Support for multiple load balanced virtual servers - combine load balanced HTTP, SMTP and DNS services all in one box

Real F5 not included. Sorry guys.

Captive Portal

Commonly known as "hotspot". The user's web access will be redirected to an authentication page. Unless he is authenticated all traffic from his Client will be blocked.

- CP pages/elements can be hosted on pfSense itself
- CP pages can be PHP as well
- Built-in User manager or RADIUS-Support
- RADIUS-Accounting support
- Passthrough IP-/MAC-adress support

Caveats: Can't be used with Multiwan or Schedules; "Reauthenticate users every minute" option won't work for very large installs (many concurrent logged in users)

Wireless

Common Deployments

- Access Point
- Wireless WAN
- Site to site connections

Caveats: A WLAN interface can only be bridged when in access point mode. Site to site connections have to be routed and multi-point bridges are not possible.

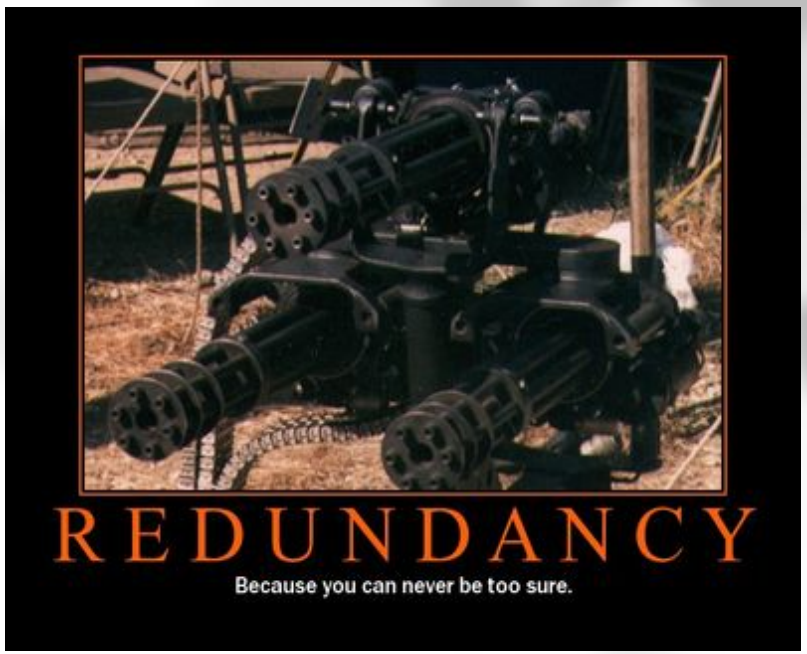
Wireless

Demo

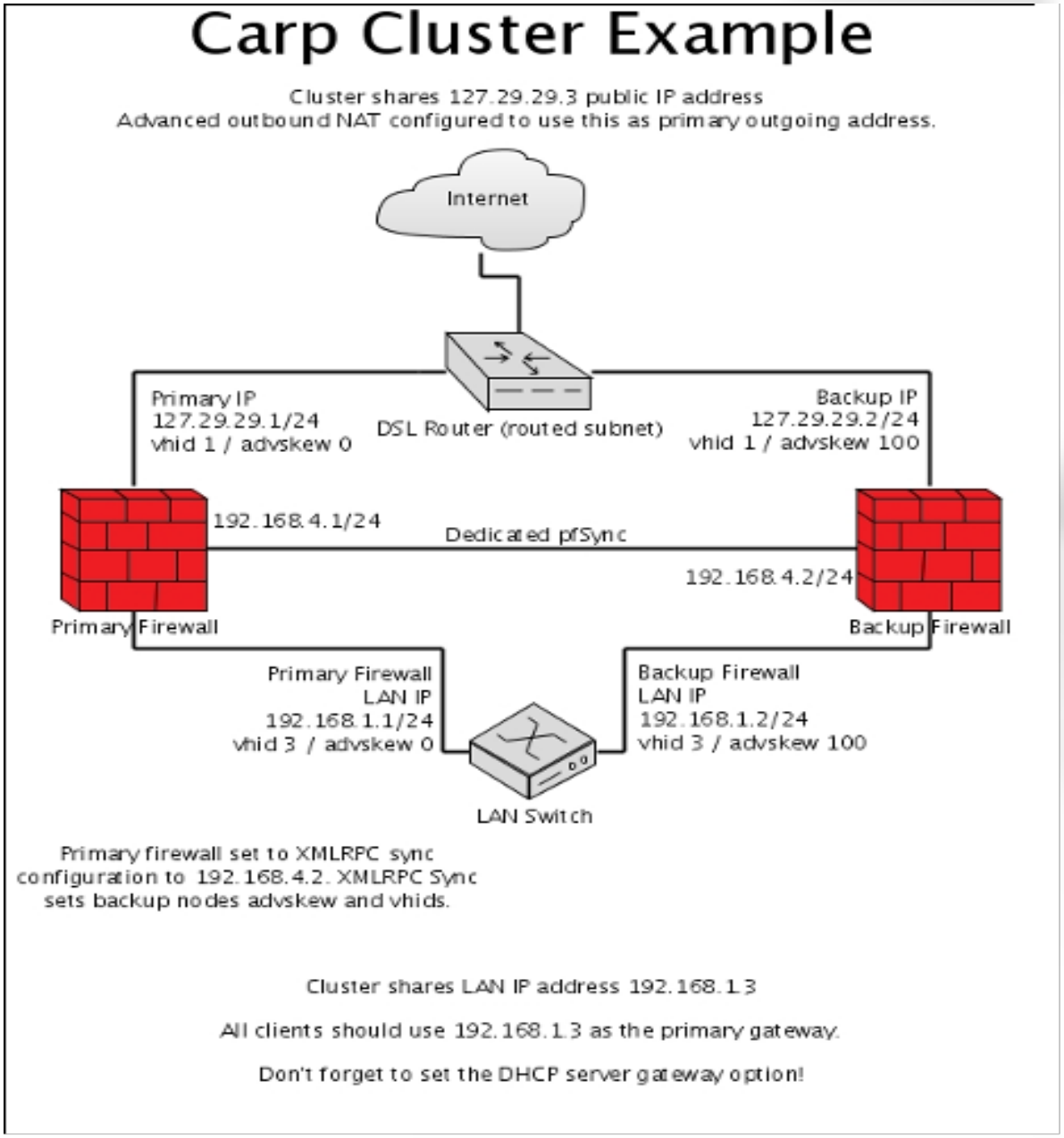
- Configuring an Access Point
- Wireless WAN
- Site to site connections

Hardware Redundancy - Overview

- CARP is used to provide high availability of service across multiple devices
- CARP Misnomers - CARP does not provide configuration synchronization of pf-state synchronization
- pfSense CARP clusters require a minimum of 3 static addresses per network segment within the same subnet until CARPdev
- VRRP traffic conflicts - ensure unique VHIDs
- Not all multicast is equal in the eyes of switch makers



Hardware Redundant Example Network



CARP VIPs

- Must be within the same subnet range as the interface they are attached to
  - Issues with the current FreeBSD implementation
  - pfSense webGUI defends against this
- VHID groups must be unique for each CARP VIP or VRRP address
- Advertising frequency (>0 for backup devices)

pfsync and XMLRPC

- PFSync is used to synchronize firewall states between multiple machines participating in a high-availability configuration such as a CARP cluster (stateful failover or "seamless" failover)
- XMLRPC is used to mirror pfSense configurations across multiple pfSense installations participating in a CARP cluster

DHCP Server

Standard ISC DHCP daemon supports typical DHCP options

Features:

- Deny unknown clients
- Dynamic DNS configuration with dynamic DHCP client registration
- DHCP Failover
- PXE boot server options

DHCP Relay

- Relay DHCP requests to DHCP server on another interface
- Append circuit ID and agent ID to requests
- Allows for the proxying of requests to a DHCP server used on the WAN subnet

DNS Forwarder

- Caching DNS service
- Works with DHCP to register and provide DNS to dynamic clients
- Option to add custom host or domain mappings
- Can be sometimes abused to override name resolution for unwanted domains

Content Filtering "Trick"

OpenDNS Setup

- Sign up for free OpenDNS account
- Add your network
- Configure category restrictions

pfSense Setup

- Permit outbound TCP/UDP port 53 only to:
  - 208.67.222.222
  - 208.67.220.220
- Configure above two DNS servers on pfSense

Dynamic DNS

pfSense can act as a Dynamic DNS client for a number of Dynamic DNS services including:

- DynDNS
- DyNS
- EasyDNS
- ODS
- DHS
- no-ip
- Zone edit

You must configure a DNS server in System: General setup or allow the DNS server list to be overridden by DHCP/PPP on WAN for dynamic DNS updates to work.

SNMP

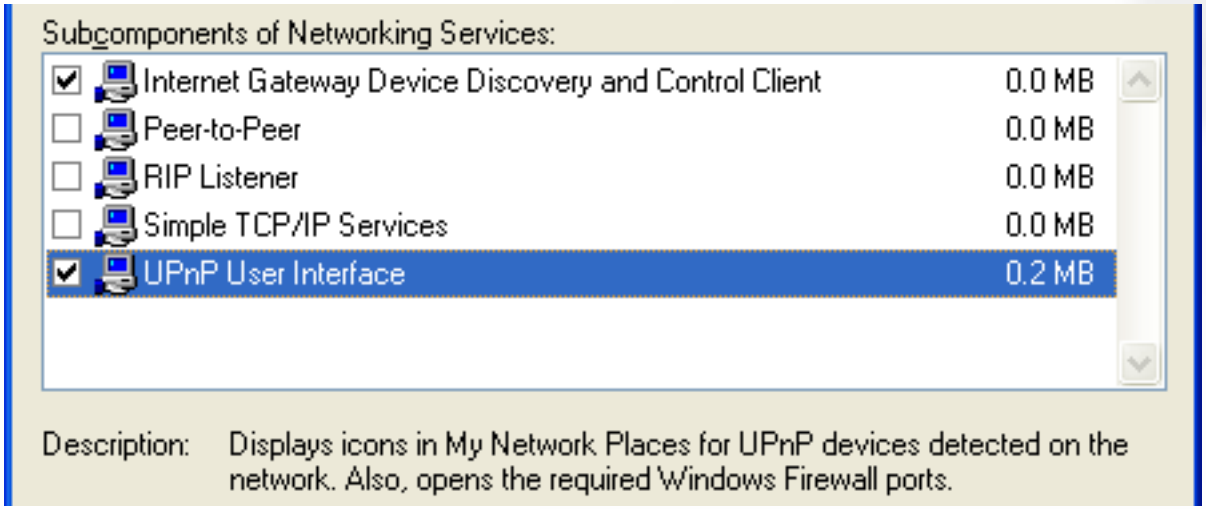
SNMP daemon for integrating with existing monitoring systems. Useful for applications like:

- Cacti
- Zabbix
- Nagios
- MRTG
- monomon (Windows)
- AirPort Flow Monitor (OSX)

UPnP

pfSense includes a UPnP daemon for supporting applications like:

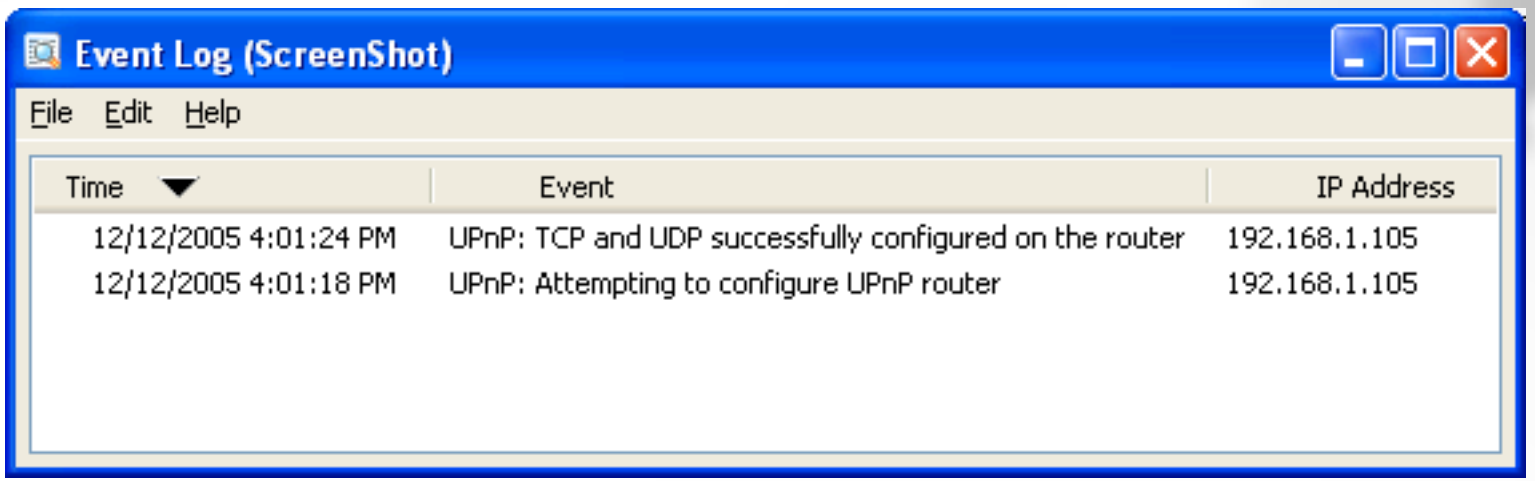
- IM (MSN Messenger)
- Some streaming audio/video applications
- P2P clients
- Xbox live
- IRC Clients



UPnP

Caveats:

- Only uses one WAN at a time
- Dynamically generated rules won't obey traffic shaper config
- Inherently risky and flawed protocol
  - restrict



Wake on LAN

- pfSense allows the administrator to store MAC addresses of WOL-supported computers and may wake up one or all machines upon mouse click.
- Easy way to become more "green" friendly

Backing up and restoring config.xml

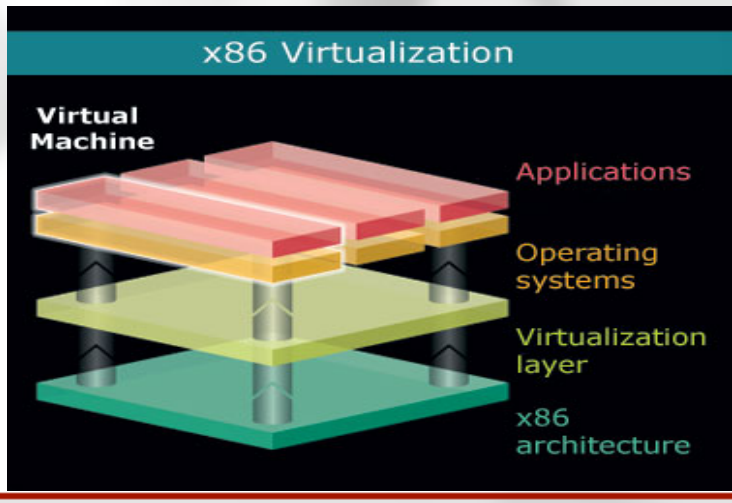
All pfSense configuration data and pfSense 3rd party package data is saved in config.xml. It is quite easy to backup this configuration file and restore it (even configuration sections).

- To backup pfSense visit Diagnostics -> Backup / restore. Click download configuration.
- To restore a pfSense config.xml backup visit Diagnostics -> Backup / restore. Click browse, locate the config.xml backup on your local hard disk / network and then click Restore configuration.

Virtualization and pfSense

Known Working Hypervisors

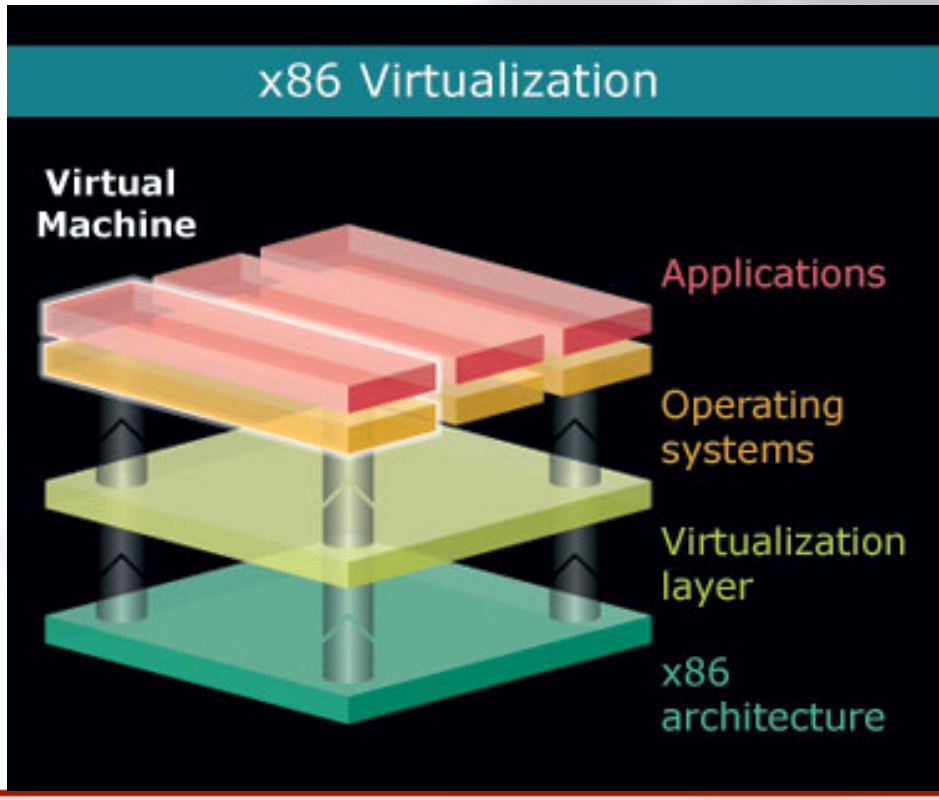
- VMware
  - Entire product line - ESX, Server, Player, Workstation, Fusion
- Parallels
- Microsoft Virtual PC and Virtual Server
  - Sort of...
    - just like it "sort of..." works for everything
- VirtualBox



Virtualization and pfSense

Uses

- Perimeter firewall
  - Not necessarily a good idea
- Segregating virtual networks from physical
- Routing between virtual networks



VMware and pfSense

- Installer tweaks
- Use VMware tools
- Use e1000 or vmxnet network adapters
- VMware support
  - Possibly limited

Packages

Packages extend the capabilities of a pfSense install by allowing users to install relevant software. Many of these packages are still under development and testing. Packages include:

- Squid - HTTP Cache
- TinyDNS - DNS server
- SpamD - Spam deferral daemon
- Siproxy - SIP proxy daemon
- Snort - Network intrusion detection daemon
- Zabbix Agent - Agent for system monitoring

DNS Server package (tinydns)

It works for Lycos. It works for citysearch.com. It works for pobox.com. It works for 1.85 million more .com's. It works for several of the Internet's largest domain-hosting companies: directNIC, MyDomain/NamesDirect, Interland, Dotster, Easyspace, Namezero, Netfirms, and Rackspace Managed Hosting. It'll work for you too.

Features

- Fully authoritative domain name server
- Does not allow zone transfers by default
- Failover support (using ping) provided by pfSense
- Helps allow for 5.9's when using multiple ISPs

SPAMD

spamd is a fake sendmail(8)-like daemon which rejects false mail. It is designed to be very efficient so that it does not slow down the receiving machine.

Features

- Greylisting - Temporarily fails a new connection. Well behaved MTAs will wait and resend the message again.
- Whitelists - Hosts that will bypass the greylist process.
- Blacklists - Hosts that will be blocked out right.

SPAMD

- RBL Support - be aware of RBL TOS and licenses, many charge for commercial use
- Stutter text - slows down the session to 300 baud like speeds
- Supports multiple SMTP servers behind pfSense

Editing config.xml

Config.xml is the main storage location for all of pfSense and it's installed packages configuration settings.

Editing the file can be accomplished via three different ways:

- Via the webConfigurator
- Via the console
- Via a remote console (SSH)

To enable SSH, visit System -> Advanced -> Enable Secure Shell

Good idea to rm /tmp/config.cache after changes to clear out the config cache ... Diagnostics -> Edit file does this for you automatically.

Example config.xml

```
<?xml version="1.0"?>
<!-- pfSense default system configuration -->
<pfsense>
    <version>2.9</version>
    <lastchange></lastchange>
    <theme>nervecenter</theme>
    <system>
        <optimization>normal</optimization>
        <schedulertype>priq</schedulertype>
        <hostname>pfSense</hostname>
        <domain>local</domain>
        <dnsserver></dnsserver>
        <dnsallowoverride/>
        <username>admin</username>
        <password>$1$dSJImFph$GvZ7.1UbuWu.Yb8etC0re.</password>
        <timezone>Etc/UTC</timezone>
        <time-update-interval>300</time-update-interval>
        <timeservers>0.pfsense.pool.ntp.org</timeservers>
        <webgui>
            <protocol>http</protocol>
```

Editing config.xml example

Setting the LAN interface to 10 baseT/UTP

```
<pfsense>
...
<interfaces>
     <lan>
          <if>sis0</if>
          <ipaddr>192.168.1.1</ipaddr>
          <subnet>24</subnet>
          <media></media>
          <mediaopt></mediaopt>
          <bandwidth>100</bandwidth>
          <bandwidthtype>Mb</bandwidthtype>
          <!--
          <wireless>
               *see below (opt[n])*
          </wireless>
          -->
     </lan>
...
</pfsense>
```

Editing config.xml example

Setting the LAN interface to 10 baseT/UTP

```
<pfsense>
...
<interfaces>
     <lan>
          <if>sis0</if>
          <ipaddr>192.168.1.1</ipaddr>
          <subnet>24</subnet>
          <media>10baseT/UTP</media>
          <mediaopt>full-duplex</mediaopt>
          <bandwidth>100</bandwidth>
          <bandwidthtype>Mb</bandwidthtype>
          <!--
          <wireless>
               *see below (opt[n])*
          </wireless>
          -->
     </lan>
...
</pfsense>
```

Introduction to pfSense 1.3

- FreeBSD 7.x base (currently 7.0 - RELENG_7_0)
- PHP 5
- Dashboard in base (available as package in 1.2)
- Improved routing and gateway support
- User manager with integration for Active Directory, Novell eDirectory and OpenLDAP
- IPsec Dynamic DNS support
- Includes latest verson of OpenBSD PF
- FreeBSD IP alias VIP support

Introduction to pfSense 1.3

- OpenVPN improvements
  - OpenVPN 2.1
    - Vista support
  - Integrated user and certificate management
  - Traffic filtering
  - User grouping for firewall rules
  - Client installer package generation

Introduction to pfSense 1.3

- Traffic shaper rewritten
  - Multiple interface capable (multi-WAN and multiple internal networks)
  - Multiple wizards for various configuration scenarios
  - IPsec shaping now possible
  - DiffServ support

Live Demo

pfSense Developer Summit

First three pfSense developers in attendance here. More than 10 years combined dedication to the project.

Chris and Scott - September 2004
pfSense name chosen, launched - November 2004
Bill Marquette - February 2005

Getting together all week to work on pfSense

Commercial Offerings

On an hourly basis

- Support
- Network design
- Configuration review
- Vulnerability assessment
  - Hourly or project basis
- Development
  - Hourly or project basis
  - Nearly all new 1.3 features are the result of sponsored development

- Helps support the project!

www.bsdperimeter.com

Questions, additional demos, etc.

At this point we would like to open the floor for questions and or give you additional demonstrations of your choosing.

Feedback

- Should be able to submit at bsdcan.org post-conference
- Can email us - coreteam@pfsense.org

Thanks for attending!