# pfSense

HEZRON MWANGI
Senior Systems Administrator
hmwangi@kenet.or.ke

06th September 2016

Kenya Education Network

# Introduction

- pfSense is a free, open source customized FreeBSD distribution based on the m0n0wall project.
- pfSense project was founded in 2004 by Chris Buechler and Scott Ullrich.
- Tailored for use as a firewall and router.
- Entirely managed in an easy to use web interface.
- No FreeBSD knowledge is required to deploy and use pfSense.
- Includes a long list of related features and a package system allowing further expandability.

# Introduction

- 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

- USB Memstick Installer
- Embedded (NanoBSD)

# Minimum Hardware Requirements

- General Requirements:
  - Minimum - CPU - 500 Mhz; RAM - 256 MB
  - Recommended - CPU - 1 Ghz; RAM - 1 GB
- Requirements Specific to Individual Platforms:
  - Full Install
    - CD-ROM or USB for initial installation
    - 1 GB hard drive
  - Embedded
    - 1 GB Compact Flash card
    - Serial port for console

# 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

# CPU Selection

- Throughput Considerations
  - Packets per second
  - Bandwidth required
    - 10-20 Mbps - a modern (less than 4 year old) Intel or AMD CPU clocked at at least 500MHz.
    - 21-100 Mbps - a modern 1.0 GHz Intel or AMD CPU.
    - 101-500 Mbps - No less than a modern Intel or AMD CPU clocked at 2.0 GHz. Server class hardware with PCI-e network adapters, or newer desktop hardware with PCI-e network adapters.
    - 501+ Mbps - Multiple cores at > 2.0GHz are required. Server class hardware with PCI-e network adapters.

# Feature Considerations

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

# Feature Considerations

- 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...

# Feature Considerations

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

# Common Deployments

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

# Common Deployments

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

# CIDR Summarization

- Allows specification of IP ranges
  - Firewall rules
  - NAT
  - IPsec
- Must fall in subnet boundaries

# Installation

- Live Demo
- Full installation to hard disk.

# 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

# Firewall Rules

- Firewall rules are always evaluated on incoming traffic (therefore rules have to go to the interface that 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 - 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

# VPN Capabilities

- IPsec (with filtering support)
- PPTP (with filtering support)
- OpenVPN (filtering available from 1.3)

# VPN Uses

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

# OpenVPN

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

# OpenVPN Certificate Generation

- All certificate management in the web interface
- Organizations with existing PKI should use it
- Quick and easy way - easyrsa included with OpenVPN

# Routing

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

# 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)

pfSense

kenet
Kenya Education Network

# 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

# 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)

# 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

# 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)

- 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

# 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.

# Q&A.

?

kenet
Kenya Education Network

kenet

Kenya Education Network

THANK YOU!