pfSense - A Beginner's Guide to a Sensible Firewall

presented by Mason Egger @ Texas Linux Fest 2016

Who are you?

- Recent Graduate of Texas State University
- Associate Software Engineer at Forcepoint
- BSD Enthusiast, Systems Engineer, Systems Administrator (Too much free time)
- Amateur YouTuber
    - BSD Synergy
    - Tin Foil Hat Security
- pfSense Enthusiast
- https://www.masonegger.com
- Presentation will be uploaded to my website under Talks after the presentation.

What is pfSense?

- Open Source operating system focused on being a router/firewall.
- Designed to be managed with an easy-to-use web interface.
- Based on FreeBSD.
- Founded in 2004 by Chris Buechler and Scott Ullrich.
- IPv4 and IPv6 compatible

Why FreeBSD?

- pf - *packet filter* - OpenBSD firewall ported to FreeBSD. Simple, easy to use, powerful.
- In 2004 OpenBSD's wireless support was limited compared to FreeBSD.
- FreeBSD's network performance is significantly better than that of OpenBSD
    - We can thank Netflix for this, an entirely FreeBSD shop that pushes the network code back upstream.
- FreeBSD's multi-processor support allows for greater scalability and is utilized by the latest versions of pfSense.
    - https://github.com/gvnn3/netperf/blob/master/Documentation/netperf.pdf

What is BSD?

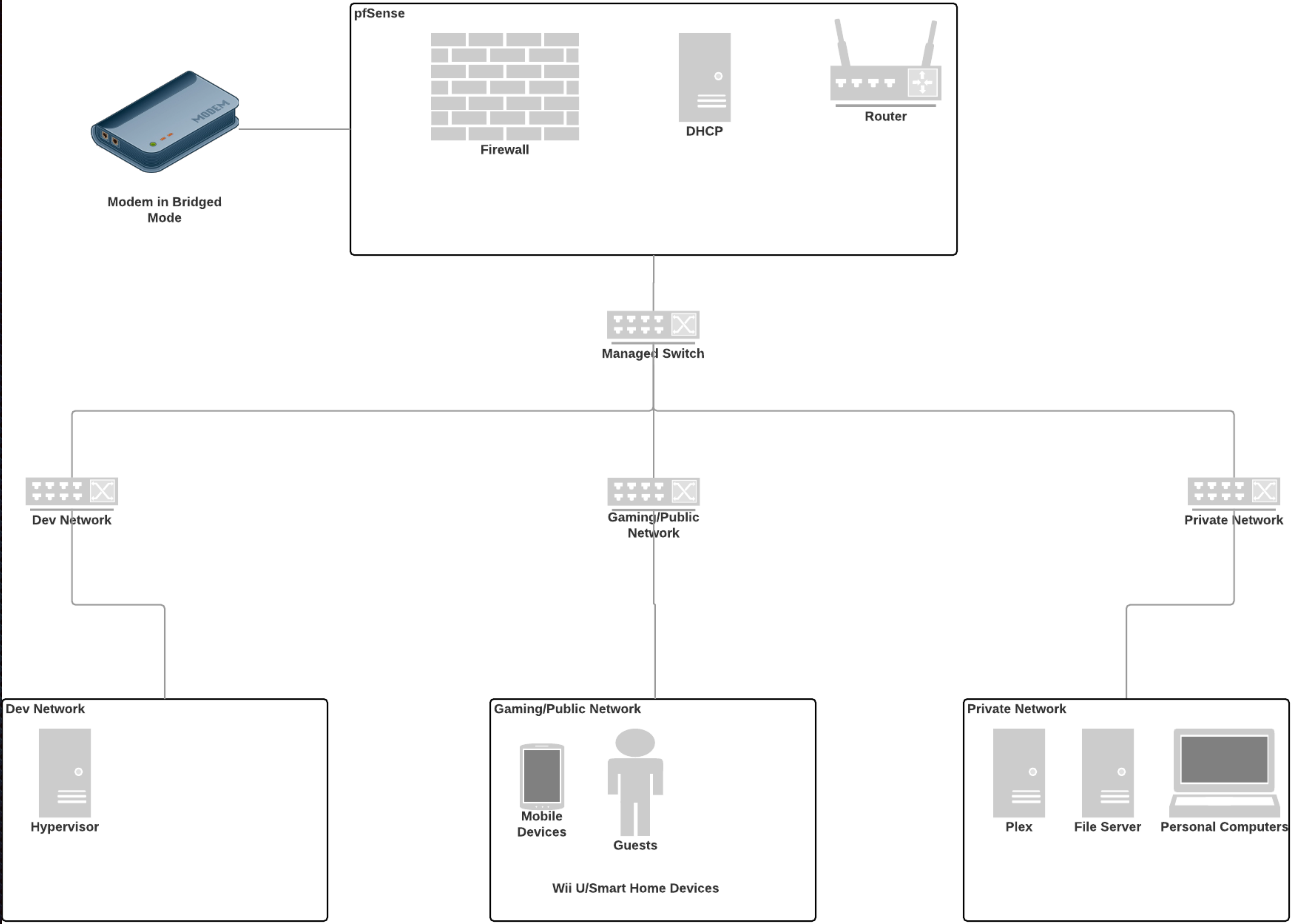
- Long discussion, talk for another day. (Or just meet with me after the talk)
- Short answer
  - Unix like Operating System, original fork of AT&T Unix
  - Berkley Software Distribution
  - Original BSDs no longer exist, 4 major forks exist today
    - FreeBSD - Focus on flexibility, ease of use, cutting edge highly scalable.
      - Looking to get into FreeBSD? Try PC-BSD, FreeBSD with a an easier to use interface.
    - OpenBSD - Focus on security. correctness and being free as possible.
    - NetBSD - Focus on portability. “Can run NetBSD on your toaster”.
    - DragonFly BSD - Focus on multi-process infrastructure. Fork of FreeBSD 4.8

Common pfSense Deployments

- Perimeter Firewall
    - Most common deployment of pfSense.
    - Supports multiple WAN, LAN, DMS.
    - BGP, connection redundancy, and load balancing also
- LAN or WAN Router
    - common as as LAN or WAN and perimeter firewall.
- Wireless Access Point.
- Special Purpose Appliances
    - VPN appliance
    - DNS Server
    - Sniffer Appliance
    - DHCP Server Appliance
- Supports VLANs

HOME NETWORK

megger | July 2, 2016



Hardware requirements

- pfSense is compatible with any FreeBSD hardware on i386 and amd64 platforms.
  - Unlike FreeBSD, pfSense does not support PowerPC, MIPS, ARM, SPARC, etc.
- pfSense 2.3.1 is based on FreeBSD 10.3
  - https://www.freebsd.org/releases/10.3R/hardware.html
  - https://www.freebsd.org/doc/en_US.ISO8859-1/books/faq/hardware.html
- Network Interfaces
  - Virtually all NICs are supported by pfSense, but not all drivers are created equal. (I have realtek cards)
  - Intel Pro/100 and Pro/1000 NICs are recommended. Solid driver support in FreeBSD.
- Wireless Adapters
  - Many cards are supported in FreeBSD, but pfSense developers work with Atheros hardware so they tend to be the most maintained.

Services

- The base install of pfSense includes fundamental services for routing and firewall configuration
    - IPv4/IPv6 DHCP Server
    - DHCP/DHCPv6 Relay
    - DNS Resolver
    - DNS Forwarder
    - Dynamic DNS
    - SNMP
    - UPnP & NAT-PMP
    - NTPD
    - Wake on LAN
    - PPPoE Server
    - IGMP Proxy

(Some) Interesting Features

- Web Configurator
- User Management
    - RADIUS
    - LDAP
- Certificate Management/Certificate Authority
- VPN Server
- Traffic Shaper
- Load Balancing
- Captive Portal
- Package Manager

Web Configurator

- All in One configuration tool for pfSense.
- While a terminal console is available, all and more can be done through the Web Configurator
- Written in PHP and uses Twitter Bootstrap for the front end, making the configurator have a great mobile experience
- Login can be over HTTP or HTTPS
- Configure setup, firewall rules, interfaces, services along with built in status and diagnostic tools
- Took advantage of Bootstrap to make some very neat graphs/statistic visuals

User Management

- pfSense supports allowing multiple users/groups to access all or a subset of pages of the Web Configurator
    - Allow access to All Pages, Dashboard, Password Manager, VPN, etc
- Can use RADIUS or LDAP for primary authentication servers, or default Local Database.
- If RADIUS or LDAP fails or is unreachable pfSense falls back on the Local Database

Certificate Manager/Certificate Authority

- pfSense can allow you to create or import a Certificate Authority and function as this role.
- pfSense can also function as an Intermediate CA
- Basic functions like creating, importing, removing and revoking certificates

VPN Server

- OpenVPN - recommendation of pfSense
    - Built directly into base Web Configurator
- PPTP VPN - support still in documentation, but…
    - “Despite the attraction of its convenience, PPTP should not be used under any circumstances because it is no longer secure.”
- L2TP with IPSec
    - Built directly into the Web Configurator
    - L2TP is purely a tunneling protocol that has no encryption, so it’s usually paired with another encryption technique, like IPSec

Traffic Shaper

- What can Traffic Shaper do for you?
    - Keep Browsing Smooth
    - Keep VoIP Calls Clear
    - Reducing Gaming “Lag”
    - Keep P2P Applications in Check
    - Enforce Bandwidth Limits

Load Balancing

- Two types of load balancing functions are available in pfSense, Gateway and Server
- Gateway load balancing enables distribution of Internet-bound traffic over multiple WAN connections
- Server load balancing manages incoming traffic so it utilizes multiple internal servers for load distribution and redundancy.
- More full feature load balancing packages for pfSense such as HAProxy and Varnish.
- pfSense load balancer built on OpenBSDs relayd

Captive Portal

- Allows for you to direct users to a web page before Internet access is permitted.
- Captive Portal Zones - Allows for separate portals for different sets of interfaces.
- Common Portal Scenarios
    - Portal Config without Authentication
    - Portal Config using Local Authentication or Vouchers
    - Portal Config Using Radius
- *Doesn’t support IPv6 yet

Package Manager

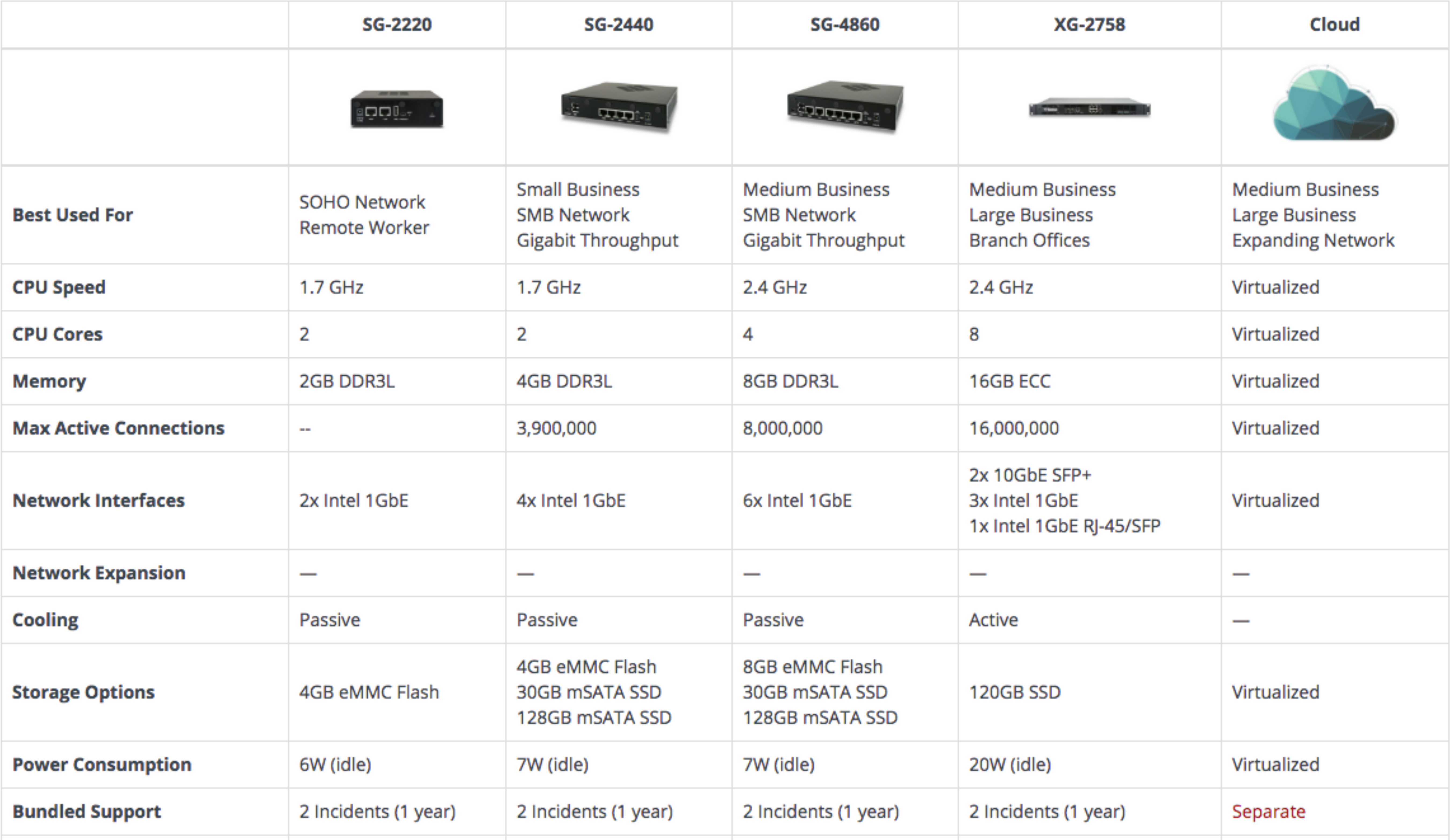
- Based on the FreeBSD package manager.
- Can install typical packages just like a server.
- Any package you install brings with it the security risks of the package.

Demo

pfSense Gold

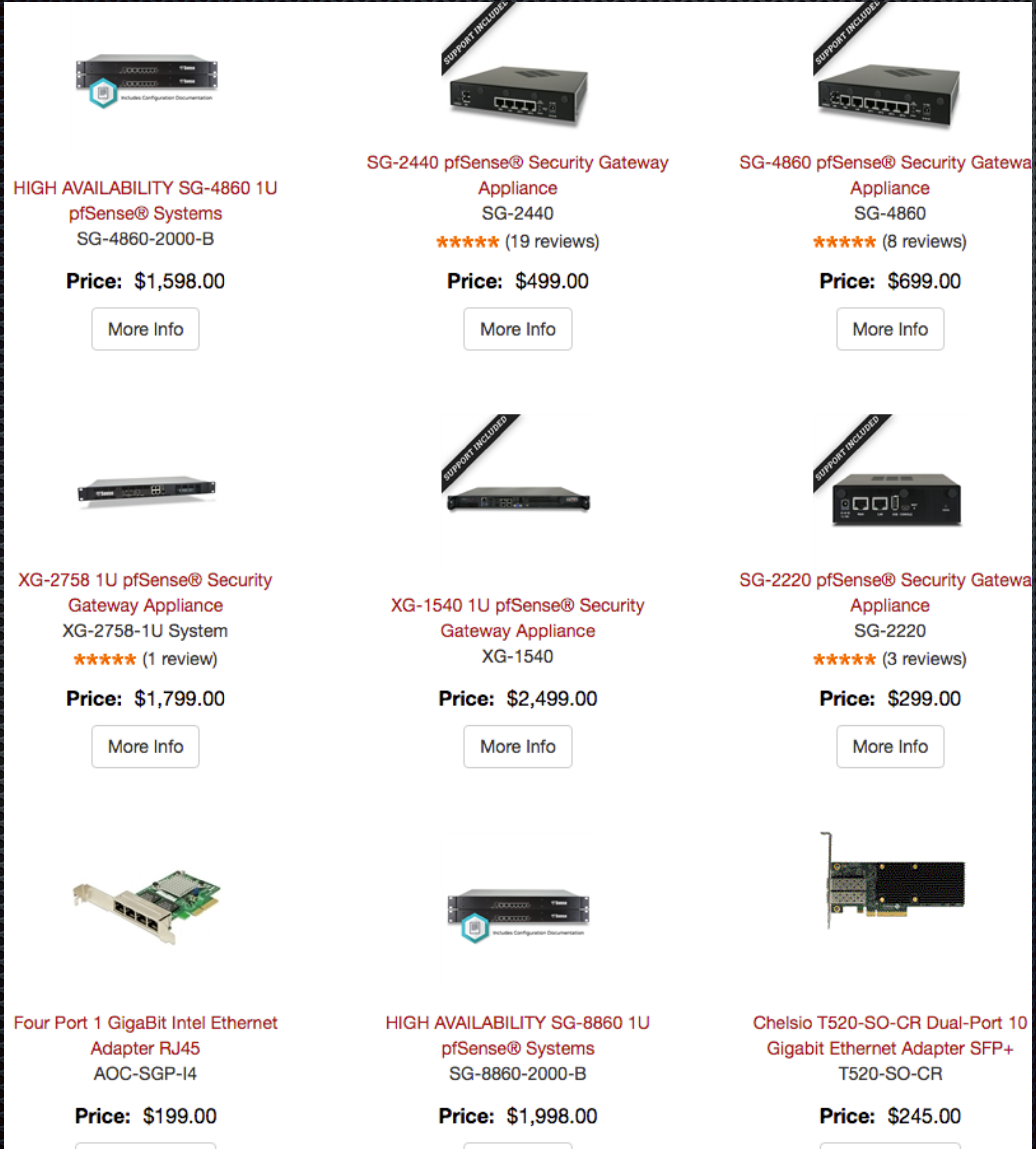
- pfSense Gold
    - Subscription program - $99 a year
    - Provides special benefits while supporting ongoing development.
    - Includes developer lead videos, living pfSense Book (Where I shamelessly got most of the information for these slides)
    - Monthly Hangouts
    - AutoConfig Backup
    - access to pfSense Virtual Security Gateway Appliance for VMWare

pfSense Hardware



	SG-2220	SG-2440	SG-4860	XG-2758	Cloud
Best Used For	SOHO Network Remote Worker	Small Business SMB Network Gigabit Throughput	Medium Business SMB Network Gigabit Throughput	Medium Business Large Business Branch Offices	Medium Business Large Business Expanding Network
CPU Speed	1.7 GHz	1.7 GHz	2.4 GHz	2.4 GHz	Virtualized
CPU Cores	2	2	4	8	Virtualized
Memory	2GB DDR3L	4GB DDR3L	8GB DDR3L	16GB ECC	Virtualized
Max Active Connections	--	3,900,000	8,000,000	16,000,000	Virtualized
Network Interfaces	2x Intel 1GbE	4x Intel 1GbE	6x Intel 1GbE	2x 10GbE SFP+ 3x Intel 1GbE 1x Intel 1GbE RJ-45/SFP	Virtualized
Network Expansion	—	—	—	—	—
Cooling	Passive	Passive	Passive	Active	—
Storage Options	4GB eMMC Flash	4GB eMMC Flash 30GB mSATA SSD 128GB mSATA SSD	8GB eMMC Flash 30GB mSATA SSD 128GB mSATA SSD	120GB SSD	Virtualized
Power Consumption	6W (idle)	7W (idle)	7W (idle)	20W (idle)	Virtualized
Bundled Support	2 Incidents (1 year)	2 Incidents (1 year)	2 Incidents (1 year)	2 Incidents (1 year)	Separate

pfSense Hardware



HIGH AVAILABILITY SG-4860 1U pfSense® Systems
SG-4860-2000-B

Price: $1,598.00

More Info

SG-2440 pfSense® Security Gateway Appliance
SG-2440
★★★★★ (19 reviews)

Price: $499.00

More Info

SG-4860 pfSense® Security Gatewa Appliance
SG-4860
★★★★★ (8 reviews)

Price: $699.00

More Info

XG-2758 1U pfSense® Security Gateway Appliance
XG-2758-1U System
★★★★★ (1 review)

Price: $1,799.00

More Info

XG-1540 1U pfSense® Security Gateway Appliance
XG-1540

Price: $2,499.00

More Info

SG-2220 pfSense® Security Gatewa Appliance
SG-2220
★★★★★ (3 reviews)

Price: $299.00

More Info

Four Port 1 GigaBit Intel Ethernet Adapter RJ45
AOC-SGP-I4

Price: $199.00

HIGH AVAILABILITY SG-8860 1U pfSense® Systems
SG-8860-2000-B

Price: $1,998.00

Chelsio T520-SO-CR Dual-Port 10 Gigabit Ethernet Adapter SFP+
T520-SO-CR

Price: $245.00

Shameless plug

- Checkout my YouTube Channels

If you like the logos, contact Rey Menchaca
rey@phatsoundsmedia.com

Questions?

- You may have them, I may or may not have the answers.
- Possibly pfSense developers in the audience, feel free to answer if I can't.
- Visit the pfSense booth in the Exhibitor Hall