

An Introduction to Firewalls and Routers Using pfSense

Created for WNYLUG

By Neal Chapman

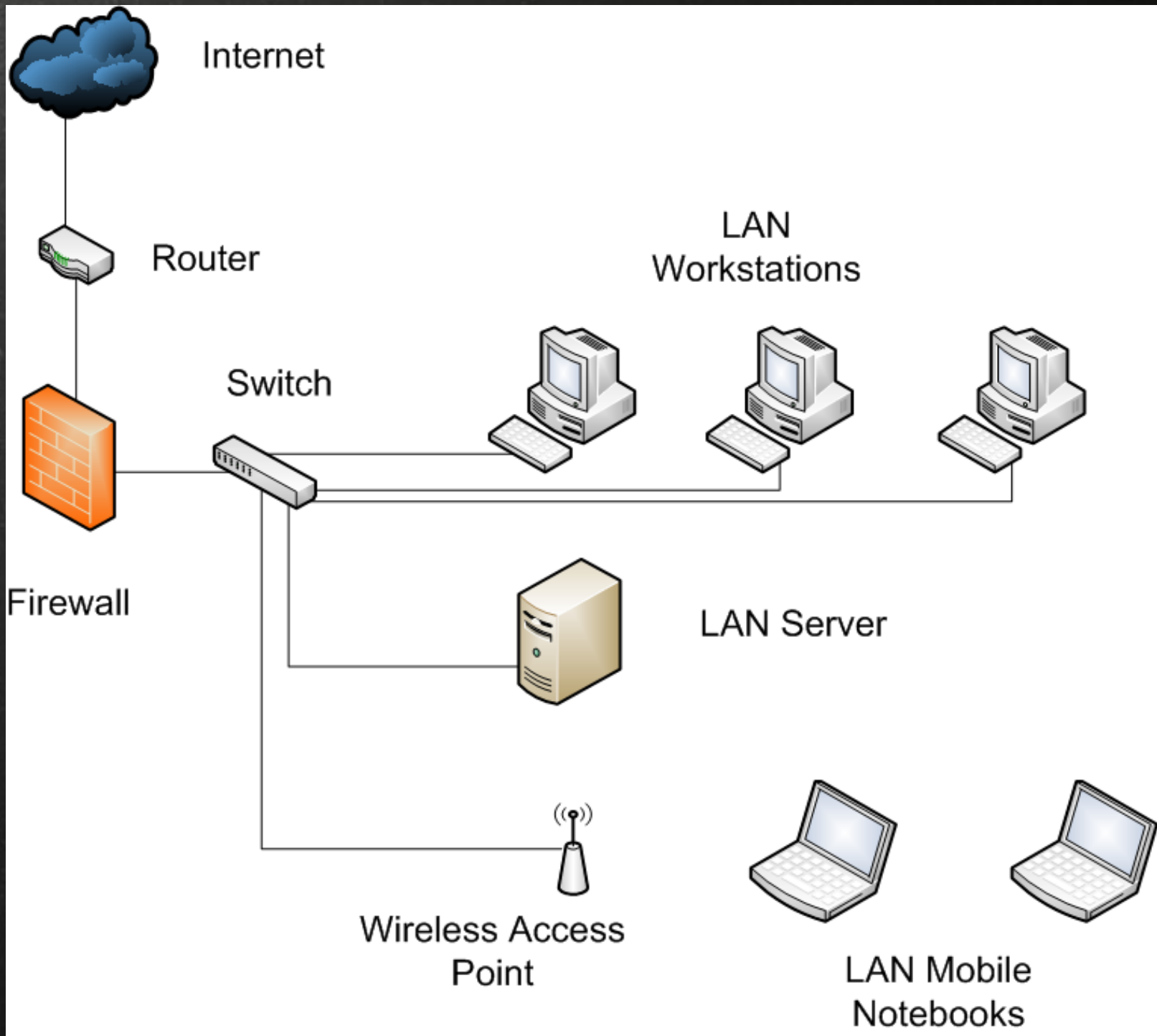
08/12/2009

Topics To Cover

- The Firewall And The Router
- pfSense - Overview
- WAN, LAN, DMZ
- pfSense - Interfaces
- Blocking Ports
- pfSense - Rules
- Network Address Translation
- pfSense - NAT
- Services - DHCP
- Services - Dynamic DNS
- Services - Load Balancer
- Services - PPTP
- Services - OpenVPN
- Services - Traffic Shaping
- Diagnostics
- Packages

The Firewall And The Router

- The Internet and complex private networks consist of many different smaller networks
- Even simple networks need a router
- Router moves data in and out of networks
- Focusing on routing networks to private
- Protecting private networks with a firewall
- Filtering inbound traffic
- Filtering outbound traffic
- Monitoring traffic



pfSense - Overview

- Features:
 - Combined firewall and router
 - Additional services
 - Installs on common hardware
 - Console interface
 - Web interface (first time setup)
- General Setup
- Advanced Setup

pfSense - Console Interface

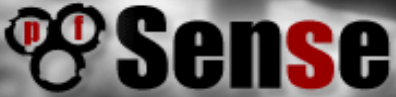
```
WAN*          ->  em0          ->  192.168.55.181 (DHCP)
LAN*          ->  em1          ->  192.168.49.1
OPT1(OPT1)   ->  le0          ->  NONE
```

pfSense console setup

- 0) Logout (SSH only)
- 1) Assign Interfaces
- 2) Set LAN IP address
- 3) Reset webConfigurator password
- 4) Reset to factory defaults
- 5) Reboot system
- 6) Halt system
- 7) Ping host
- 8) Shell
- 9) PFtop
- 10) Filter Logs
- 11) Restart webConfigurator
- 12) pfSense PHP shell
- 13) Upgrade from console
- 14) Enable Secure Shell (sshd)
- 98) Move configuration file to removable device

Enter an option: █

pfSense - Web Interface







pfSenseVM.local


System Interfaces Firewall Services VPN Status Diagnostics

System Overview

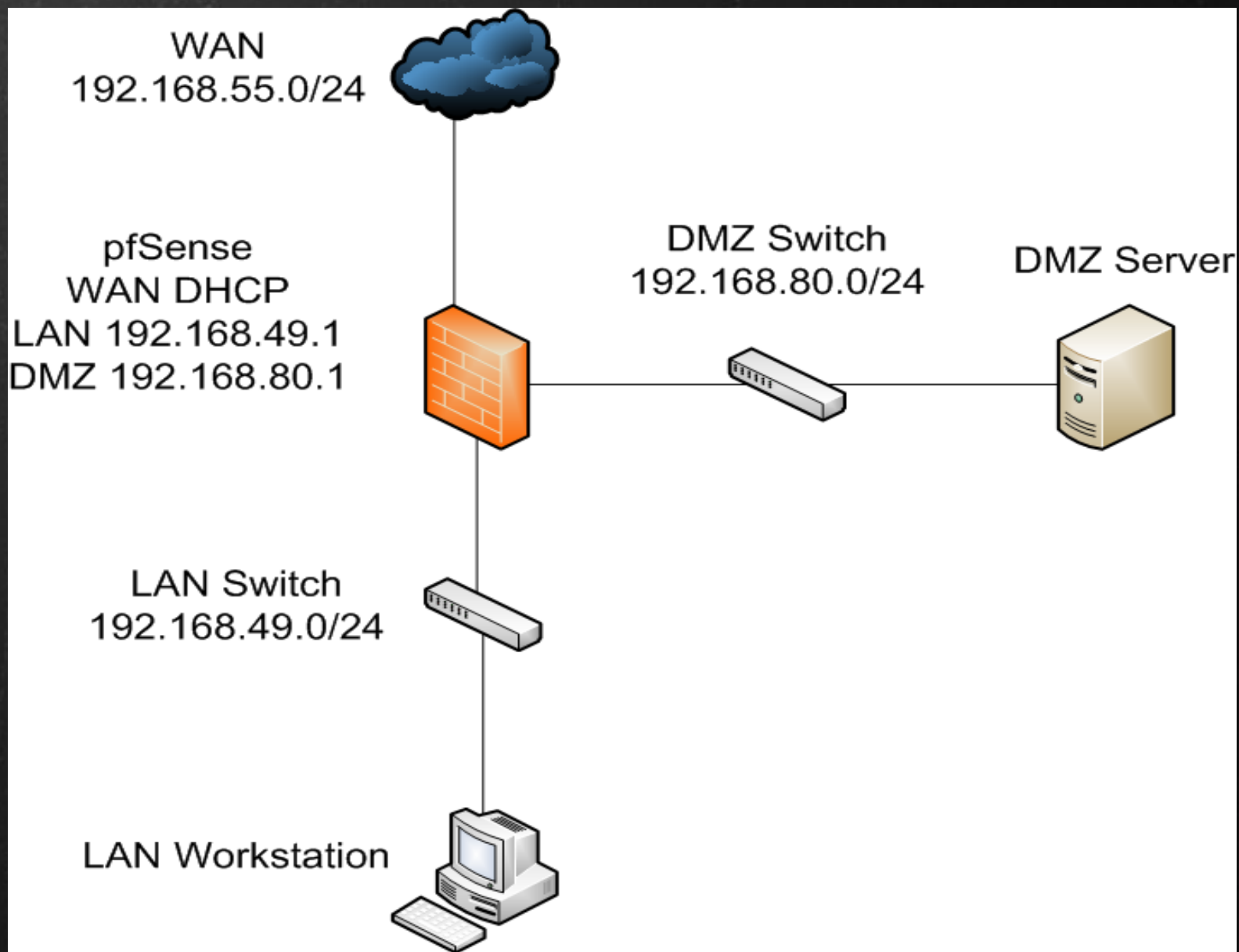
System information

Name	pfSenseVM.local	
Version	1.2.2 built on Thu Jan 8 22:30:24 EST 2009	
Platform	pfSense	
Uptime	00:30	
State table size	20/10000 Show states	
MBUF Usage	515 /1410	
CPU usage		2%
Memory usage		37%
SWAP usage		0%
Disk usage		4%

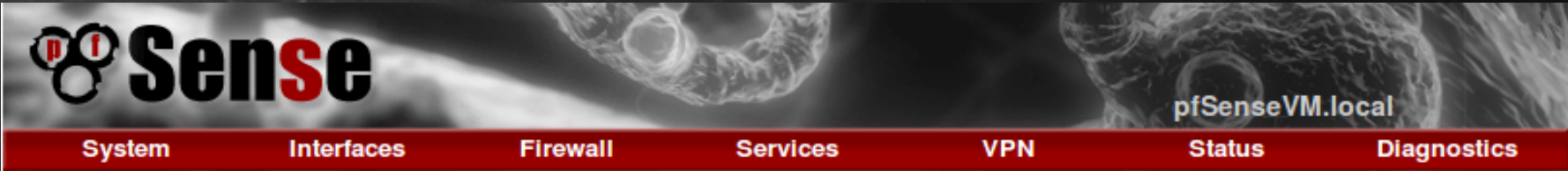
pfSense is © 2004-2008 BSD Perimeter LLC. All Rights Reserved. [\[view license\]](#)
[Commercial Support Available]

powered by
 FreeBSD®

WAN, LAN and DMZ



pfSense - Interfaces



pfSenseVM.local

System Interfaces Firewall Services VPN Status Diagnostics

Interfaces: Assign

Interface assignments **VLANs**

Interface	Network port
LAN	em1 (00:0c:29:23:e7:76) ▾
WAN	em0 (00:0c:29:23:e7:6c) ▾
OPT1	le0 (00:0c:29:23:e7:80) ▾

Save

- change the IP address of your computer
- renew its DHCP lease
- access the webGUI with the new IP address

pfSense is © 2004-2008 BSD Perimeter LLC. All Rights Reserved. [view license]
[Commercial Support Available]

powered by
FreeBSD®

Blocking Ports

- What are ports?
- Inbound vs. outbound
- Some common ports:
 - 20 FTP Data
 - 21 FTP Control
 - 22 SSH
 - 23 Telnet
 - 25 SMTP
 - 80 HTTP
 - 443 HTTPS
 - 3389 RDP/Terminal Services
 - 5900 VNC
- Why block ports?

pfSense - Rules

pfSense pfSenseVM.local

System Interfaces **Firewall** Services VPN Status Diagnostics

Firewall: Rules

LAN **WAN** OPT1

	Proto	Source	Port	Destination	Port	Gateway	Schedule	Description	
<input type="checkbox"/>	TCP	*	*	*	80 (HTTP)	*		Block outbound LAN HTTP	
<input type="checkbox"/>	*	LAN net	*	*	*	*		Default LAN -> any	

pass block reject log
 pass (disabled) block (disabled) reject (disabled) log (disabled)

Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

pfSense is © 2004-2008 BSD Perimeter LLC. All Rights Reserved. [view license]
[Commercial Support Available]

powered by FreeBSD®

Network Address Translation (NAT)

- In computer networking, network address translation (NAT) is the process of modifying network address information in datagram packet headers while in transit across a traffic routing device for the purpose of remapping a given address space into another.
- Port forwarding
- 1:1
- Outbound

pfSense - Port Forward NAT

pfSenseVM.local

System Interfaces Firewall Services VPN Status Diagnostics

Firewall: NAT: Port Forward

Port Forward 1:1 Outbound

<input type="checkbox"/>	If	Proto	Ext. port range	NAT IP	Int. port range	Description	
<input type="checkbox"/>	WAN	TCP	3389 (MS RDP)	192.168.80.10 (ext.: 192.168.55.181)	3389 (MS RDP)	Allow DMZ RDP	

pfSense is © 2004-2008 BSD Perimeter LLC. All Rights Reserved. [view license]
[Commercial Support Available]

powered by
FreeBSD®

pfSense - Port Forward Rules

The screenshot shows the pfSense web interface. At the top, the pfSense logo is on the left, and the hostname 'pfSenseVM.local' is on the right. A navigation bar contains links for System, Interfaces, Firewall, Services, VPN, Status, and Diagnostics. The 'Firewall: Rules' page is active, with tabs for LAN, WAN, and DMZ. The DMZ tab is selected, showing a table of firewall rules. One rule is visible: 'NAT Allow DMZ RDP'. The rule is enabled (checkbox checked) and has a green play icon. The rule details are: Proto: TCP, Source: *, Port: *, Destination: 192.168.80.10, Port: 3389 (MS RDP), Gateway: *, Schedule: (empty), and Description: NAT Allow DMZ RDP. To the right of the table are icons for editing, deleting, and adding rules. Below the table is a legend for rule actions: pass (green play), pass (disabled) (grey play), block (red X), block (disabled) (grey X), reject (yellow X), reject (disabled) (grey X), log (blue i), and log (disabled) (grey i). A 'Hint' section explains that rules are evaluated on a first-match basis. The footer contains copyright information for BSD Perimeter LLC and the FreeBSD logo.

pfSense

pfSenseVM.local

System Interfaces Firewall Services VPN Status Diagnostics

Firewall: Rules

LAN WAN DMZ

	Proto	Source	Port	Destination	Port	Gateway	Schedule	Description	
<input checked="" type="checkbox"/>	TCP	*	*	192.168.80.10	3389 (MS RDP)	*		NAT Allow DMZ RDP	

pass
 pass (disabled)

block
 block (disabled)

reject
 reject (disabled)


log
 log (disabled)

Hint:
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

pfSense is © 2004-2008 BSD Perimeter LLC. All Rights Reserved. [view license]
[Commercial Support Available]

powered by
FreeBSD®

Services - DHCP



pfSenseVM.local

System Interfaces Firewall Services VPN Status Diagnostics

Services: DHCP server

LAN DMZ

Enable DHCP server on LAN interface

Deny unknown clients
If this is checked, only the clients defined below will get DHCP leases from this server.

Subnet	192.168.49.0	
Subnet mask	255.255.255.0	
Available range	192.168.49.0 - 192.168.49.255	
Range	<input type="text" value="192.168.49.10"/>	to <input type="text" value="192.168.49.245"/>
WINS servers	<input type="text"/> <input type="text"/>	
DNS servers	<input type="text"/> <input type="text"/>	
	NOTE: leave blank to use the system default DNS servers - this interface's IP if DNS forwarder is enabled, otherwise the servers configured on the General page.	
Gateway	<input type="text"/>	
	The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not	

Services - Dynamic DNS

- Configure dynamic DNS service such as DynDNS
- Work around for using a public host name on an ISP that provides dynamic IP addresses (DHCP)

Services - Load Balancing

- Method for using multiple WAN connections
- Single or multiple pfSense systems
- Load balancing - Traffic shared across multiple WAN connections
- Failover - WAN connection to switch to when a WAN connection fails

Services - VPN PPTP

- The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP does not provide confidentiality or encryption; It relies on the protocol being tunneled to provide privacy. PPTP has been made obsolete by Layer 2 Tunneling Protocol (L2TP) and IPSec.

Services - VPN OpenVPN

- OpenVPN is a free and open source virtual private network (VPN) program for creating point-to-point or server-to-multiclient encrypted tunnels between host computers. It is capable of establishing direct links between computers across network address translators (NATs) and firewalls. It was written by James Yonan and is published under the GNU General Public License (GPL).

Services - Traffic Shaper

- Traffic shaping (also known as "packet shaping") is the control of computer network traffic in order to optimize or guarantee performance, lower latency, and/or increase usable bandwidth by delaying packets that meet certain criteria.
- Practicality

pfSense - Diagnostic Tools

- DHCP leases
- Interfaces
- Load balancer
- Queues (traffic shaper)
- Services
- System
- ARP table
- Ping
- Traceroute
- Packet capture
- RRD graphs
- Traffic graph

pfSense - Packages

- pfSense can be expanded using packages
- Useful packages:
 - Dashboard - Adds pfSense dashboard
 - Darkstat - Network statistics gather
 - NTOP - Network probe
 - Snort - Lightweight intrusion detection
 - Squid - High performance web proxy