An Introduction to Firewalls and Routers Using pfSense

Created for WNYLUG

By Neal Chapman

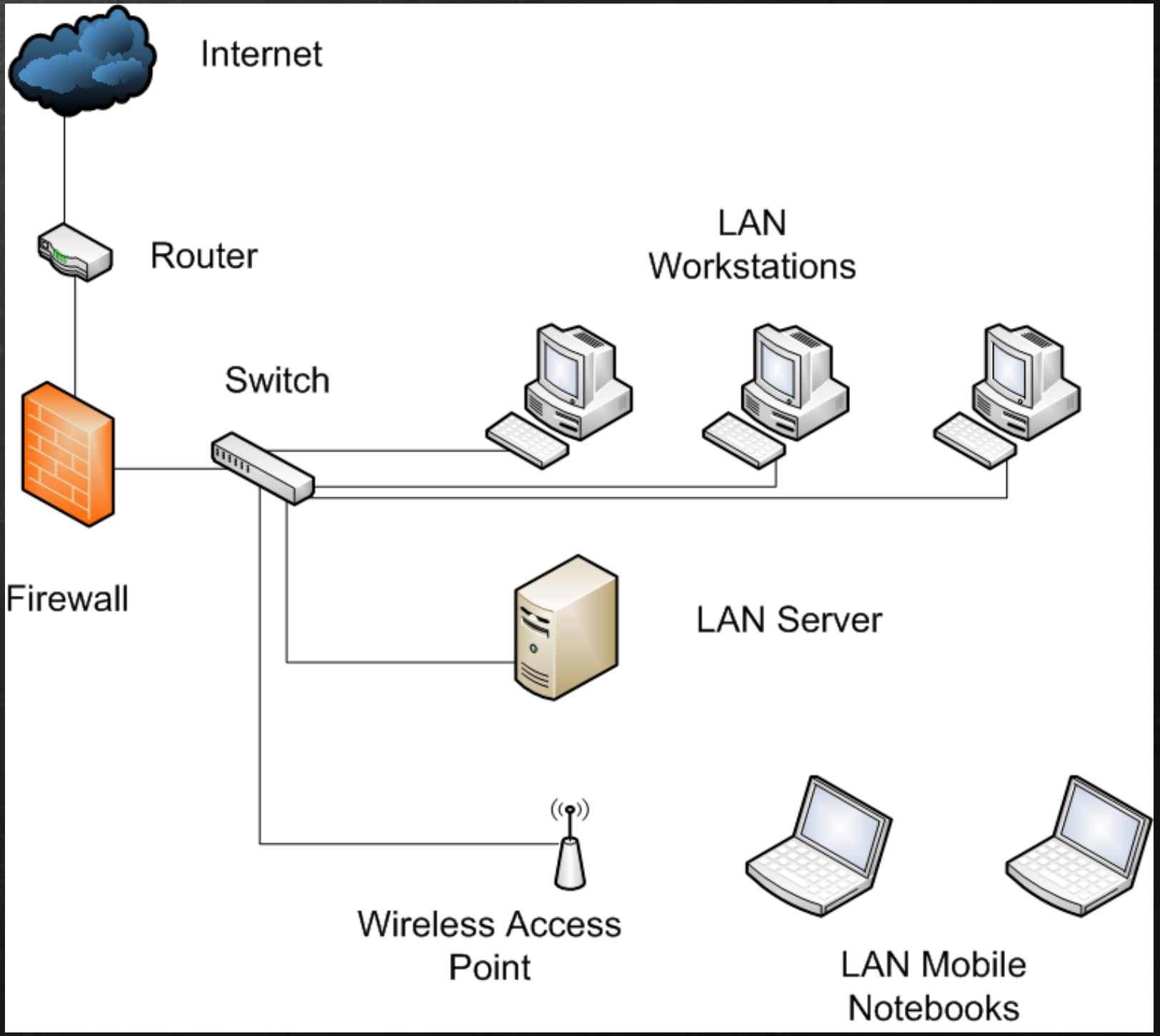
08/12/2009

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


Internet
Router
LAN
Workstations
Switch
Firewall
LAN Server
Wireless Access
Point
LAN Mobile
Notebooks

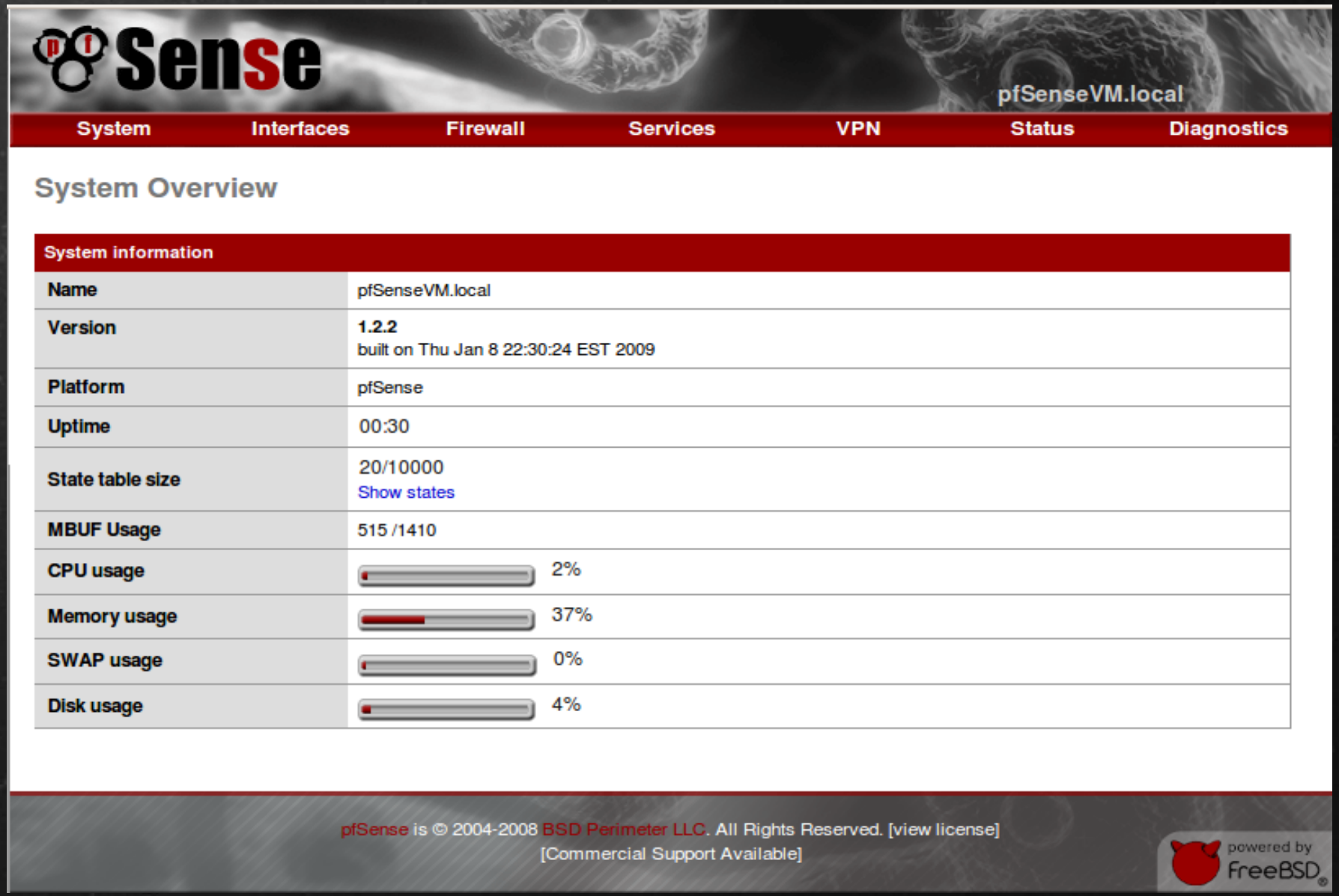
pfSense - Overview

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

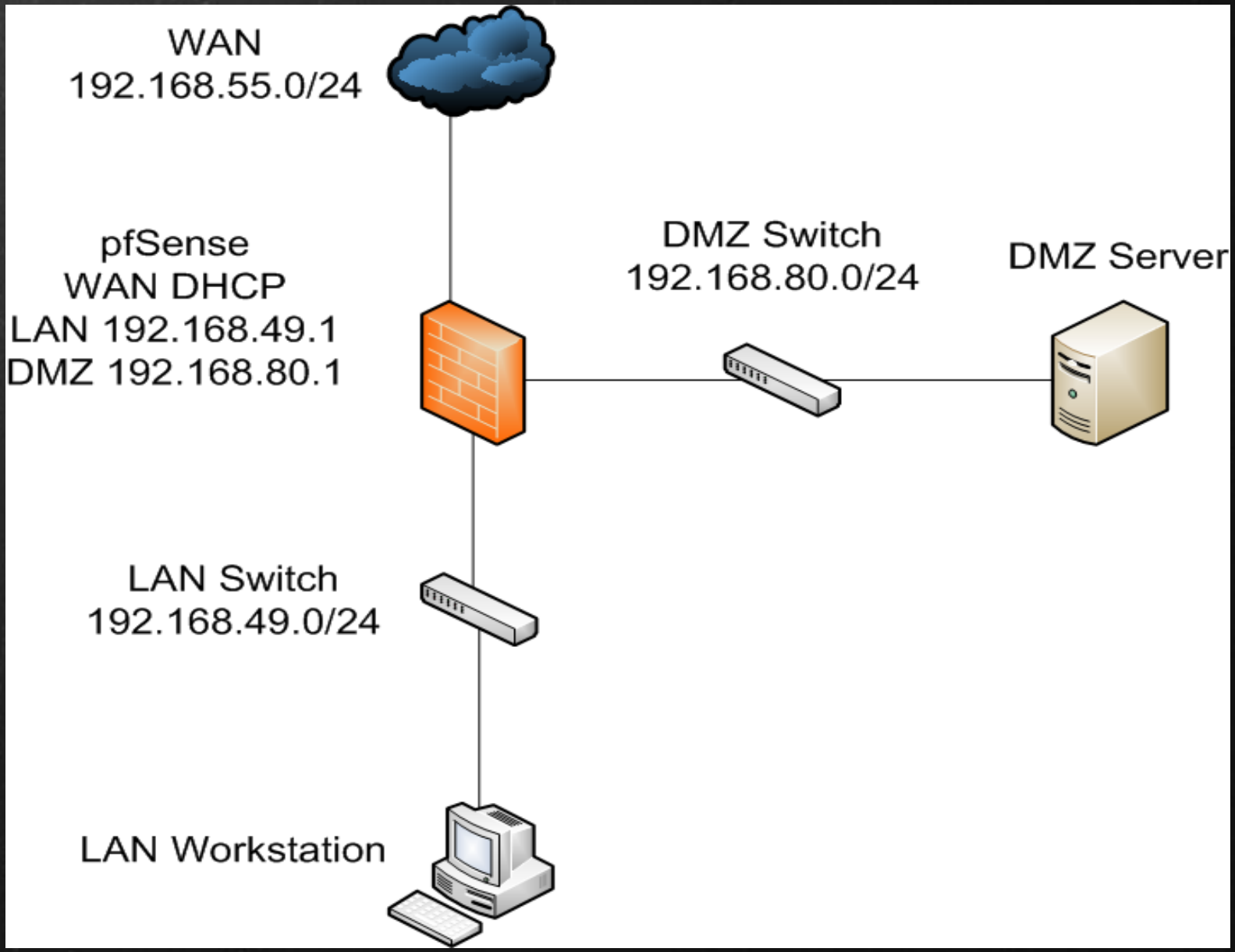
pfSense - Console Interface

```
 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:
```

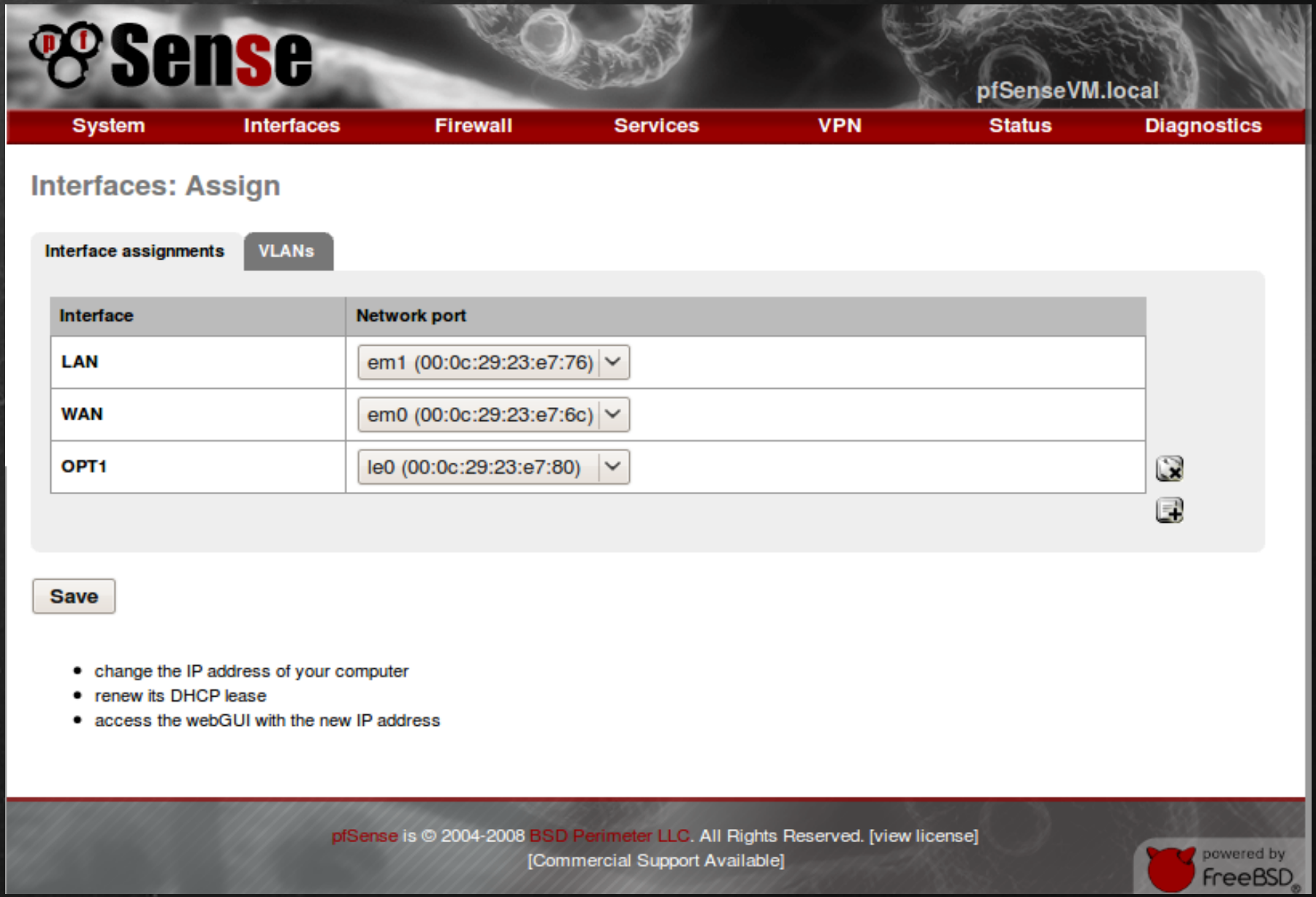
pfSense - Web Interface



WAN, LAN and DMZ



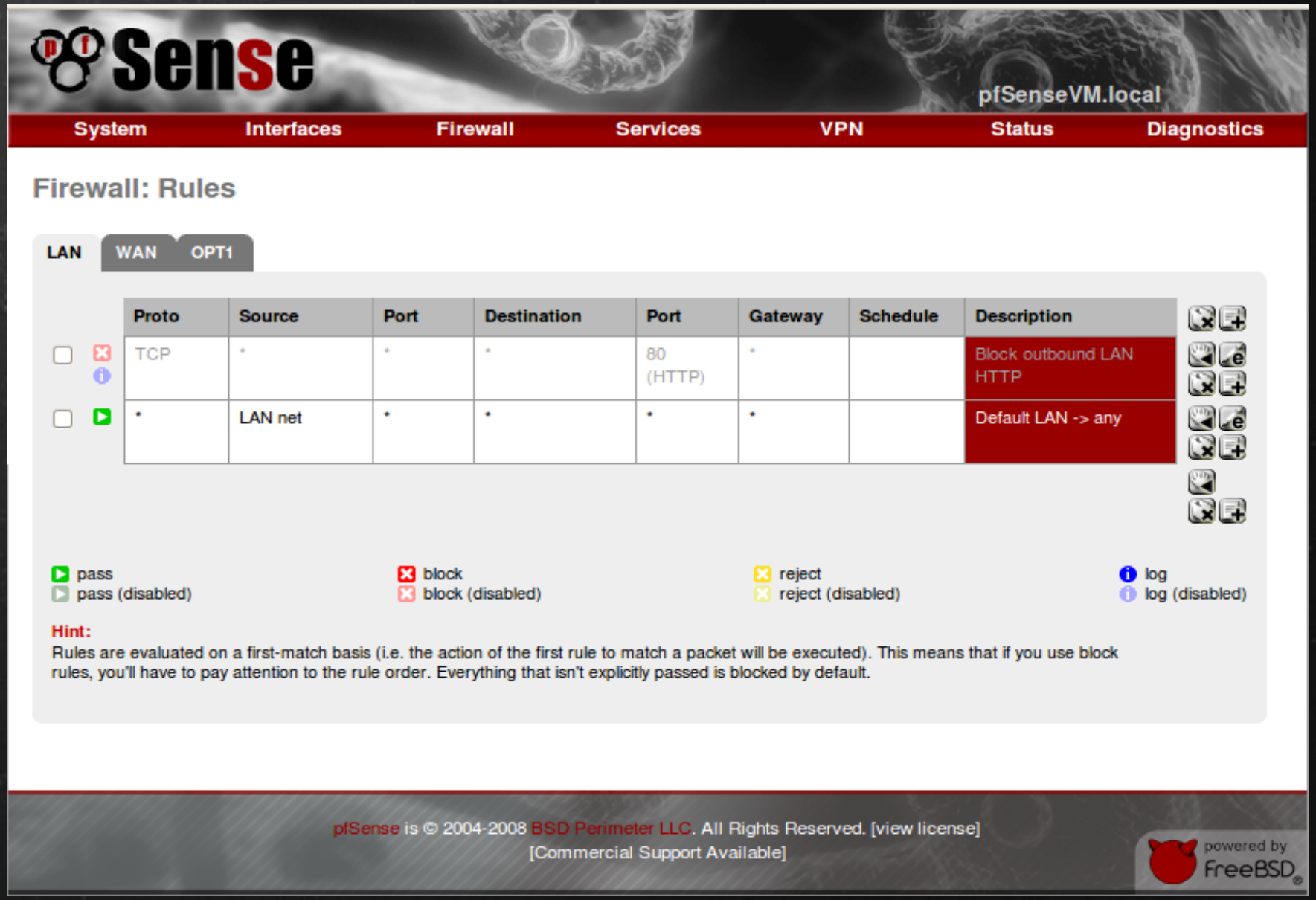
pfSense - Interfaces



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?

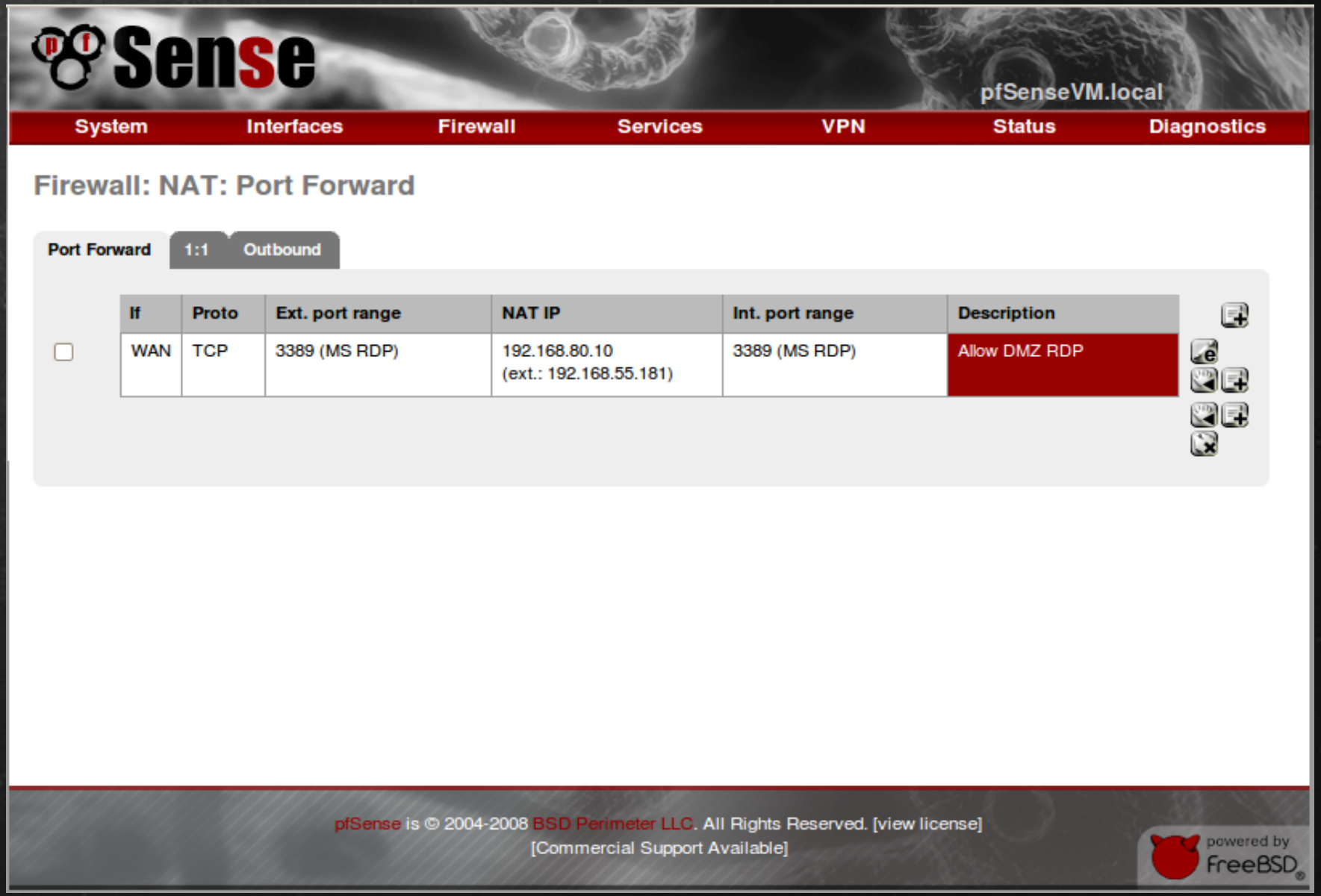
pfSense - Rules



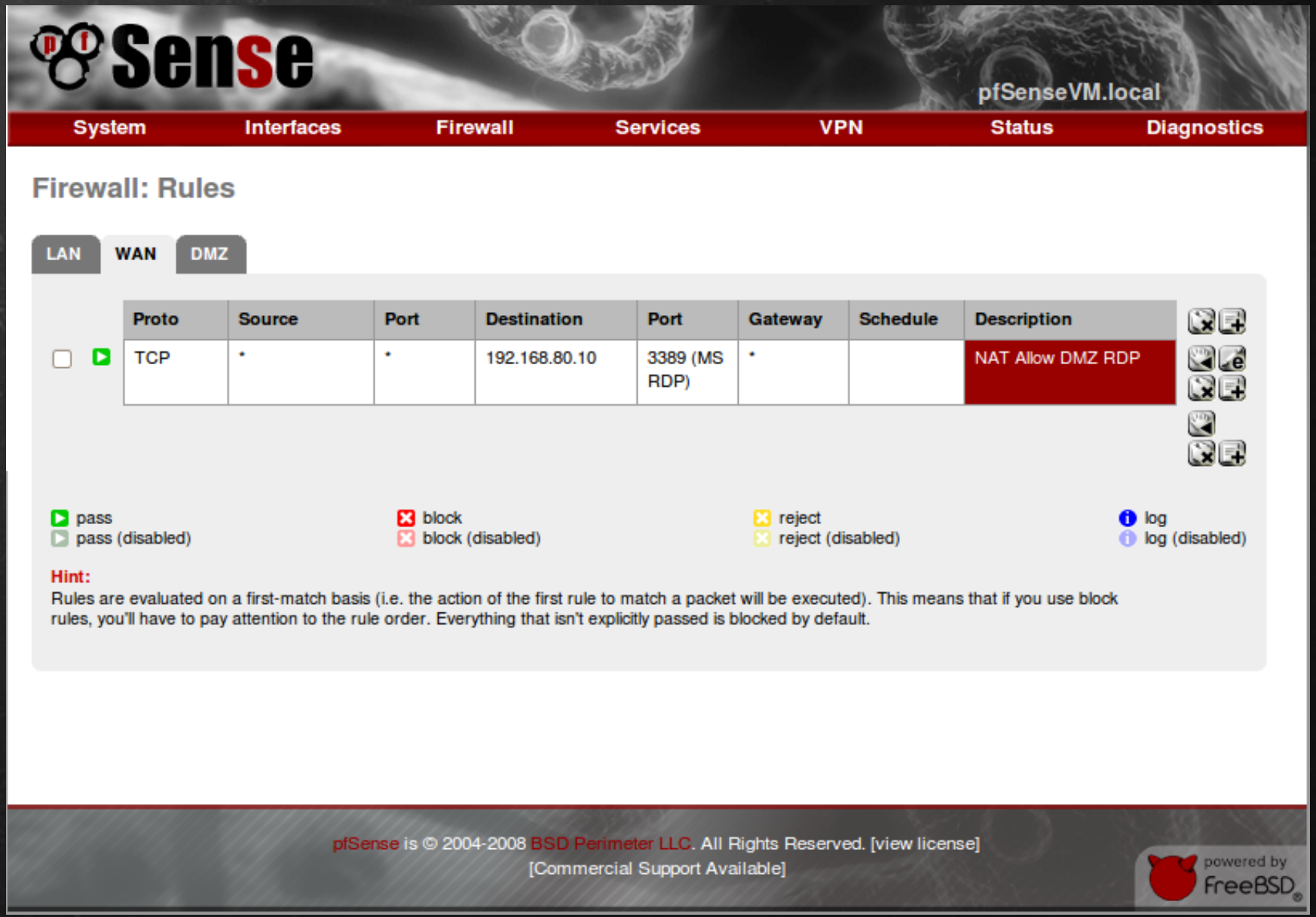
Network Address Translation (NAT)

- 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

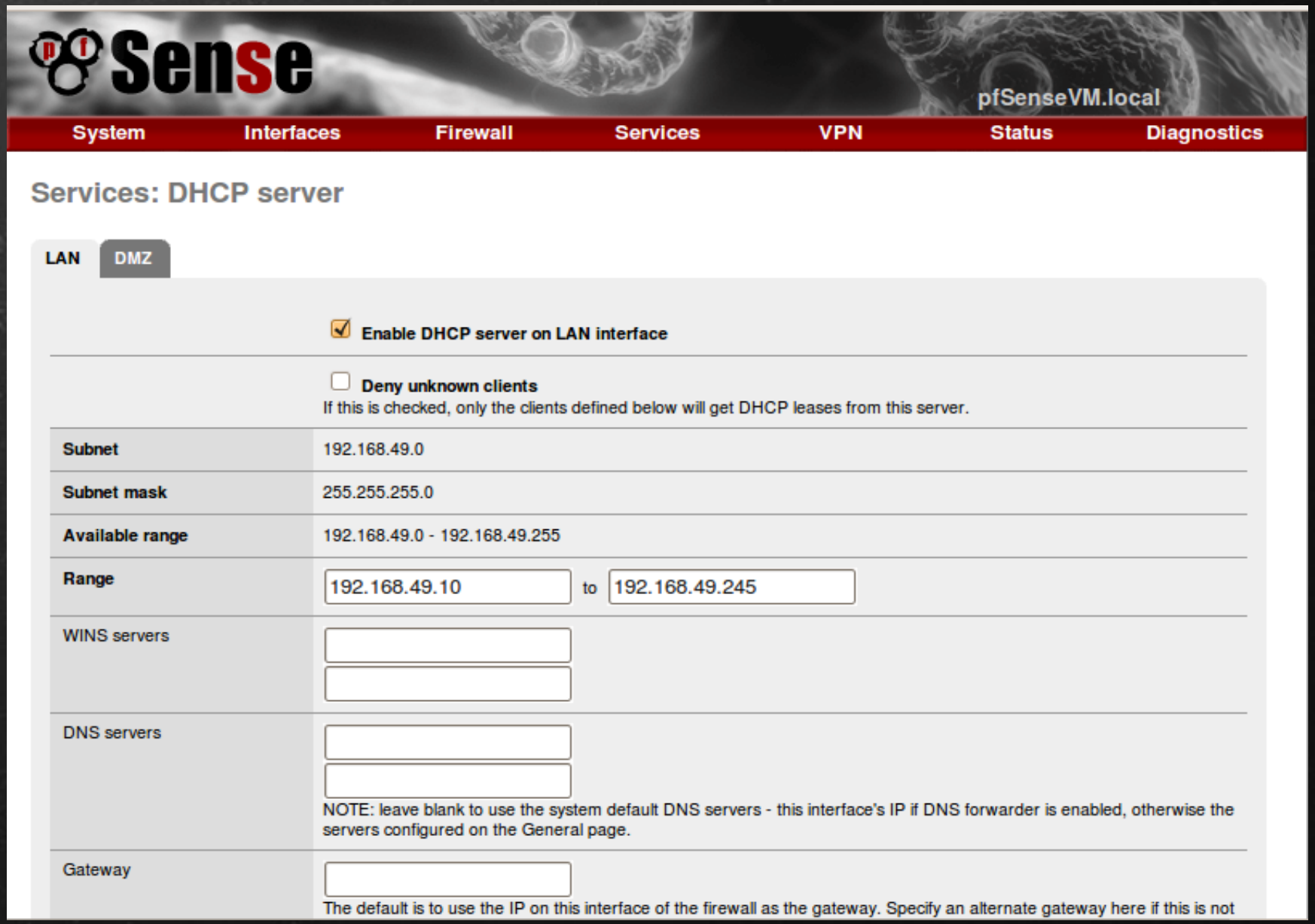
pfSense - Port Forward NAT



pfSense - Port Forward Rules



Services - DHCP



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 balencer
- 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