PfSense Configuration Checklist

* Download Pre-made config file for PFSense 2.1
* Change passwords for admin
* Change WebGUI to HTTPS
* Load Config file – REBOOT
* Change passwords for admin
* Change WebGUI to HTTPS
* Download PFSense 2.1/FreeBSD 8.3 p11 update – auto update amd64
* Wait for download to complete – REBOOT
* Change WAN IP and confirm LAN/DMZ IP interfaces
* Check settings and traffic
* Load and configure snort, antivirus, nmap
* Monitor access to services and logs
* Sit back for 5 hours doing nothing because 3 Owl Moon is protecting us…. HAHA!!!

Configuration Settings – (pre-configured from file)

* Assign IP
  + WAN IP – 172.31.2x.2 mask - /29 static DHCP-no
  + LAN IP -- 172.20.241.254 mask - /24 static DHCP-no
  + DMZ IP – 172.20.240.254 mask - /24 static DHCP-no

General Setup

* Assign DNS settings
  + DNS Server 8.8.8.8 Gateway = WAN
  + Allow DNS Server list to be overridden… CHECKED
  + Do not use DNS Forwarder as DNS server… UNCHECKED
* Assign Time zone
  + Americas/Chicago
  + Default time server
  + Theme = metallic

Advanced Setup

* HTTPS - TCP Port = 44480
* Disable webConfigurator login autocomplete… CHECKED
* Disable DNS Rebinding Checks… CHECKED
* Password protect the console menu… CHECKED
* Networking – Allow IPv6 UNCHECKED

Interfaces

* WAN
  + Static IPv4 only Address: 172.31.2x.2 /29 GW-172.31.2x.1
  + Block Private Networks UNCHECKED
  + Block Bogon Networks CHECKED
* LAN
  + Static IPv4 only Address: 172.20.241.254 /24
  + Block Bogon Networks CHECKED
* DMZ
  + Static IPv4 only Address: 172.20.240.254 /24
  + Block Bogon Networks CHECKED

Firewall

* Create Alias list
  + CentOSEcommerce (DMZ) – 172.20.240.11
  + UbuntuDNS (DMZ)- 172.20.240.23
  + DebianEmail (LAN)- 172.20.241.39
  + Windows2003FTP (LAN)- 172.20.241.9
  + Windows2008DFS (LAN)- 172.20.241.3
  + WindowsR2\_ADDNS (LAN)- 172.20.241.27
  + DMZside (DMZ subnet)- 172.20.240.0/24
  + LANside (LAN subnet)- 172.20.241.0/24
  + WANside (WAN subnet)- 172.31.2x.0/29
  + WebPorts (80 and 443)- TCP 80; TCP 443
  + EmailPorts (25, 110, 143)- TCP 25; TCP 110; TCP 143
  + FTPPorts (20,21)- TCP/UDP 20; TCP 21
* User Manager
  + NightOwl - pw= <as assigned by list> group=admins
  + Admin- pw=<as assigned by list> group=admins \*\*disabled\*\*
* Rules – Inbound Interface
  + WAN
    - Pass
      * DNS to UbuntuDNS
      * WebPorts to CentOSEcommerce
      * SSH to ???
      * EmailPorts to DebianEmail
      * FTPPorts to Windows2003FTP???
  + DMZ
    - Pass
      * DNS from UbuntuDNS
      * WebPorts to Any – Updates only
  + LAN
    - Pass
      * DNS to Any
      * WebPorts to Any
      * Any to Any – Testing Only
  + Floating
    - Pass
      * ICMP Any to Any – Testing Only
      * Traceroute Any to Any – Linux Testing Only
      * Any to Any – Testing Only

Packages

* Install Snort
* Install AV
* Install nmap