**Fire wall infrastructure - bne-obfw45**

2010-08-30

Michael Spence

**Introduction**

This is the primary documentation for the APEagers Ltd firewall infrastructure provisions as related to the APEagers Ltd Qld/NT network. This document includes information regarding the specific operation system and server SOE installation. Passwords ant other secure information are not included in this document.

The APEagers Firewall Infrastructure document contains the necessary information regarding the core firewall for the APEagers QLD/NT network, including an overview of the setup and configuration of the server/s.

**Assumptions**

This document assumes an understanding of network, virtualization and data backup and restoration technologies. The target audience is restricted to Network, System and Security administrators.

**Server Administration**

Infrastructure administration is broken into two areas of responsibility.

The server and hardware infrastructure is supported, administered and managed by the APEagers Ltd Information Services Department's Systems Administrator.

Position: Network and Telephony Coordinator

Name: Michael Spence

Mobile: 0439 535 950

Email: mspence@apeagers.com.au

Managed WAN and IPMAN infrastructure is supported, administered and managed by Telstra. Refer to Telstra manual for contact details.

**Primary Site**

The Eight Mile Plains Fujitsu data centre is the primary site for the server and related infrastructure. Other site locations are connected to the primary site via Telstra Managed WAN infrastructure.

The primary site is physically located at 7 Brandl St Eight Mile Plains, Brisbane, Qld 4113

**Systems Inventory and Configuration**

**Inventory**

bne-obfw45 (now bne-fw1)

Server Name: bne-fw1.apeagers.com.au

VM Host: qld-esx1.apeagers.com.au

Server Role: Firewall and FTP Proxy

IP Address: (internal) 10.1.1.253

OS: OpenBSD 4.5

Hardware: ESX VM Guest (1 vCPU, 4GB RAM)

Storage: 40GB (inc swap)

emp\_core\_c3560g-48ts\_2

Host Name: emp\_core\_c3560g-48ts\_2

IP Address: 10.1.1.244

Hardware: Cisco Switch 3560G-48ts

VLans: 1, 3, 4, 5, 6, 101, 666

**Installation**

The connections to and from the APEagers Ltd Qld/Nt networks are monitored, controlled and routed through an Open BSD PF firewall. The firewall is build with the OpenBSD 4.5 release. The following information is a break down on how the firewall is installed and configured, as well as information on some custom scripts for monitoring and debugging.

**Firewall Hardware**

Name: bne-obfw45.apeagers.com.au

OS: Open BSD 4.5

IP Addresses:

vic0 - 165.228.157.90/28 (External)

vic0 - 203.38.61.192/28 (External Aliases)

vic1 - 10.1.1.253 (Internal)

vic2 - 172.20.3.33 (DMZ)

vic3 - 10.40.1.34 (B2B)

**Firewall OS Installation**

The following information is a basic guide on how to install Open BSD on your chosen platform. For further information, go to the link which as a more in-depth step-by-step guide on how to install OpenBSD on your chosen platform.

Boot from OpenBSD cdrom

Select "i" to install once the kernel has booted

Terminal type TW200 or default

"none" when prompted to select a keyboard encoding table

Proceed with install "yes"

Root hard drive to use is the default "sd0"

"no" when prompted whether to use the entire disk. \*\* IMPORTANT \*\* edit MBR manually!!!

Issue the following commands for creating the MBR: "reinit", "write", "update", "quit" - \*\*\* IMPORTANT \*\*\* In this order every time

Disk label creation: p to view partition, d to delete partition, a to add partitions.

Add partition of size 37.7G, FS Type "4.2 BSD" and a mount point of /

Add partition of size 2300M, FS type "swap"

w to write, q to quit

Proceed with setting file system "y"

System hostname is the unqualified (no apeagers.com.au suffix) name which will be the same for all interfaces.

Configure network, "Y"

BNS name is the complete DNS suffix (i.e. apeagers.com.au)

Initialise external interface and select external IP address, netmask and symbolic hostname.

Initialise internal interface and select internal IP address, netmask and symbolic hostname.

Initialise DMZ interface and select DMZ IP address, netmask and symbolic hostname.

Initialise B2B interface and select B2B IP address, netmask and symbolic hostname.

Enter and confirm the root account password. This password should be a difficult string to remember as you will never need to log into the box as root. We ill setup a privileged user account later on.

Ensure the sets which you wish to install are selected (base32.tgz, etc32.tgz, misc32.tgz, comp32.tgz, man32.tgz, and bsd) and remove any others with a command such as -game\*. Once complete type "done" and answer "y" to continue with installation.

"n" to extract more sets and "n" when prompted whether we will be using the x windows system.

Select the "Australia/Brisbane" time zone

Once the installation has been completed, type halt to stop the server and press any key to reboot

\*\*\* IMPORTANT \*\*\* Ensure you remove the installation disk from the server before rebooting.

**Firewall Configuration**

\*\* These steps need to be done with the "root" account from the console \*\*

**Add a normal user account for monitoring and logging**

Issue the command adduser

Enter the following details to setup user default environments:

- default shell "ksh"

- default home "/home"

- copy dotfiles from /etc/skel "yes"

- send mesage to user "no"

- prompt for password "yes"

- default encryption "auto"

When you add the new user be sure to add the user to the group "wheel" if you intend for them to have "su" rights. \*\*\* NOT NECESSARY \*\*\*

**Edit /etc/sudoers**

In order to log into the firewall and obtain root privileges, we use a package called sudo. This allows us to log in as a normal user, and then issue the command "sudo <command>", which will allow us to run whatever <command> is as root.

Add the following entry in /etc/sudoers

<username> ALL=(ALL) ALL

you will find an entry in this file for root already. You may wish to copy this line and alter the entry from root to <username>.

**Edit /etc/sysctl.conf**

Enable the firewall to forward IP packets by uncommenting:

net.inet.ip.forwarding=1 #..... blah

Ensure that nobody can capture pages going to the swap by uncommenting:

vm.swapencrypt.enable=1 #...... blah

**Edit /etc/rc.conf**

Enable PF firewall by changing pf=NO to "pf=YES"

Turn off all services as absolutely no services apart from PF should be running on the firewall. To do this, simply change yES variables to "NO"

Point the pf\_rules variable to where the PF configuration file will reside. Currently APEagers Ltd uses a naming scheme which incorporates the company name. IE "pf\_rules=/etc/apeagers.conf"

**Edit/Create /etc/apeagers.conf**

The PF firewall and NAT is completely configured through the use of a .conf file, which is pointed to via the variable in /etc/rc.conf. A complete copy of the rules used by this firewall is included.

The general rules are as follows (in English):

- Block all incoming traffic by default and only allow the traffic which is necessary for the business

- Explicitly block any private address spaces with a quick rule

- Pass all internal traffic out by default and only deny the traffic which is undesirable to the business.

To block traffic you can simply follow this format:

block <in> [log] on <interface> all

To allow NAT use the following format:

nat on <interface> from <source ip> to <dest ip> -> <interface>

To redirect specific traffic to an internal/alternate server user the following:

rdr on <interface> from <source ip> to <dest ip> -> <server ip>

\*\* This may be more complicated due to protocols and ports needed for this redirect \*\*

**Create /usr/bin/monitor-pf**

Create a script which will allow you to quickly monitor the output of the state table to the console or terminal. The script should read:

#!/bin/ksh

clear

tcpdump -n -e -ttt -i pflog0

Remember to chmod 755 the file so that all users can execute it.

**Create /usr/bin/grep-pf**

Create a script which will allow you to quickly grep the output of the blocked packets to the console or terminal. The script should read:

#!/bin/ksh

clear

tcpdump -n -e -ttt -r /var/log/pflog | grep "block in on vic0"

Remember to chmod 755 the file so that you can execute it.

\*\* THIS should be changed to simply grep for command line option 1, AND replaced with blocked-pf \*\*

#!/bin/ksh

clear

if [ $1 -n ]; then

echo "usage: grep-pf <what to grep>"

else

tcpdump -n -e -ttt -r /var/log/pflog | grep $1

fi

**Create restart-pf**

Create a script which will allow you to quickly flush NAT and redirect rule tables, as well as restart the NAT and firewall services. The script should read:

#!/bin/ksh

clear

pfctl -F nat

pfctl -N -f /etc/apeagers.conf

pfctl -s nat

pfctl -F rules

pfctl -R -f /etc/apeagers.conf

pfctl -s rules

Again, chmod 755 this script (although this may have to be run as root???)

**Hostfiles**

Hostfiles contain the definitions for the network cards and any aliases they have within the network if any. These files should at least be partially correct if you setup the network correctly at installation.

**Edit/Verify /etc/hostname.vic0**

Should appear as:

inet 165.228.157.90 255.255.255.252 NONE

#203.38.61.192/28 Subnet

inet alias 203.38.61.193 255.255.255.240 NONE

inet alias 203.38.61.194 255.255.255.240 NONE

inet alias 203.38.61.195 255.255.255.240 NONE

inet alias 203.38.61.196 255.255.255.240 NONE

inet alias 203.38.61.197 255.255.255.240 NONE

inet alias 203.38.61.198 255.255.255.240 NONE

inet alias 203.38.61.199 255.255.255.240 NONE

inet alias 203.38.61.200 255.255.255.240 NONE

inet alias 203.38.61.201 255.255.255.240 NONE

inet alias 203.38.61.202 255.255.255.240 NONE

inet alias 203.38.61.203 255.255.255.240 NONE

inet alias 203.38.61.204 255.255.255.240 NONE

inet alias 203.38.61.205 255.255.255.240 NONE

inet alias 203.38.61.206 255.255.255.240 NONE

**Edit/Verify /etc/hostname.vic1**

Should appear as:

inet 10.1.1.253 255.255.0.0 NONE

**Edit/Verify /etc/hostname.vic2**

Should appear as:

inet 172.20.3.33 255.255.255.224 NONE

**Edit/Verify /etc/hostname.vic3**

Should appear as:

inet 10.40.1.34 255.255.255.224 NONE

**Edit /etc/resolv.conf**

Should appear as:

lookup file bind

nameserver 10.1.1.43

**Edit /etc/rc.local**

This file contains all the routes for the firewall. This must be filled in with routes to all dealership locations, manufacturer locations (ie B2B destinations),

Examine appendix for the exact file used.

**Edit /etc/mail/relay-domains**

This file contains all the domains for APEagers. This file will be edited every time there is an additional domain added to APEagers. If this file does not have an entry for a domain the firewall will fail to accept and relay the mail message to the MX server.

Examine appendix for the current file used (at the time of this publication).

**Edit /etc/apeagers.conf**

As explained before this file contains all the rules for the firewall's NATs, blocks and redirects.

Examine appendix for the exact file used.

**Edit /etc/mail/access**

Examine appendix for the exact file used.

**Switch configuration**

As noted earlier the firewall will generally from now on be a virtual machine located in an ESX infrastructure. To compensate for the 4 network cards, we use 4 separate VLan, 1 for internal, 3 for DMS, 5 for B2B and 666 for External. Each of these are handled with a different virtual switch inside the ESX Host. The guest Firewall connects each virtual NIC to matching switches. These switches in turn have individual Interface ports to the real world (which may also have to be configured via the server interface). The external interfaces must be known and patched accordingly to the correct vlans denoted on the core switch used.

Examine appendix for the exact ports used on qld-esx1.

Examine appendix for the setup used on emp\_core\_3560g-48ts\_2

**Ongoing System Administration**

**OS Version**

It is important to note that this document is based upon 4.5. At the time of writing this document, the current version of OpenBSD is 4.7. The configuration items explained in this document, will not work on this more recent release, due to a complete rework of the pf system. However, the rules laid out here are useful as a guide for this new system.

**Warning: / was not properly un-mounted**

Should the system be incorrectly rebooted or power cycled, the root file system may be marked dirty. In some cases the OS will drop to a shell after a core dump and may be unable to clean the FS. Issue a manual fsck and clean appropriately. Reboot to a clean FS.

**System Backup Procedure**

At the time of writing this manual, it is advised that a new machine be created if the former existing firewall is corrupted or fails. Creation time should be around 15min, with practice. Following and using Michael's backup scripts, will greatly reduce down time and editing times.

Backup and Restore no longer relies upon ESX backup infrastructure. You are encouraged to have a standby firewall built at all times.

*Michael's Backup script*

This script will copy all the relevant files to a consolidated position on the firewall and will then proceed to take ownership of the files and copy them to a backup server within the APEagers Network.

*Michael's Restore Script*

On a backup server mentioned above in "Backup Script", perform restore to new firewall. Once files have been copied to new firewall, execute restore script on new firewall, which will copy consolidated files back to relevant positions.

Restart pf should be done, but it may be easier/simpler to reboot firewall with "shutdown -r now"

Examine Appendix for the details of these scripts.

**Appendix A - /etc/rc.local**

The following is a copy of the current file at the time of writing this document.

#############################

# AP Eagers Local Config

# 2010-07-30

# Author: Michael Spence

#############################

echo -n 'starting local daemons:'

# Default routes internal

route -n add -net 10.10.0.0/16 10.1.1.254

route -n add -net 10.11.0.0/16 10.1.1.254

route -n add -net 10.12.0.0/16 10.1.1.254

route -n add -net 10.13.0.0/16 10.1.1.254

route -n add -net 10.14.0.0/16 10.1.1.254

route -n add -net 10.15.0.0/16 10.1.1.254

route -n add -net 10.16.0.0/16 10.1.1.254

route -n add -net 10.17.0.0/16 10.1.1.254

route -n add -net 10.18.0.0/16 10.1.1.254

route -n add -net 10.19.0.0/16 10.1.1.254

route -n add -net 10.2.0.0/16 10.1.1.254

route -n add -net 10.22.0.0/16 10.1.1.254

route -n add -net 10.23.0.0/16 10.1.1.254

route -n add -net 10.24.0.0/16 10.1.1.254

route -n add -net 10.25.0.0/16 10.1.1.254

route -n add -net 10.26.0.0/16 10.1.1.254

route -n add -net 10.27.0.0/16 10.1.1.254

route -n add -net 10.28.0.0/16 10.1.1.254

route -n add -net 10.29.0.0/16 10.1.1.254

route -n add -net 10.32.0.0/16 10.1.1.254

route -n add -net 10.33.0.0/16 10.1.1.254

route -n add -net 10.34.0.0/16 10.1.1.254

route -n add -net 10.35.0.0/16 10.1.1.254

route -n add -net 10.36.0.0/16 10.1.1.254

route -n add -net 10.37.0.0/16 10.1.1.254

route -n add -net 10.5.0.0/16 10.1.1.254

route -n add -net 10.50.0.0/16 10.1.1.254

route -n add -net 10.51.0.0/16 10.1.1.254

route -n add -net 10.52.0.0/16 10.1.1.254

route -n add -net 10.6.0.0/16 10.1.1.254

route -n add -net 10.7.0.0/16 10.1.1.254

route -n add -net 10.8.0.0/16 10.1.1.254

# Audi Routes

route -n add -net 10.112.192.0/24 10.1.1.240

#route -n add -net 10.112.192.0/24 10.1.1.250

route -n add -net 10.112.230.0/24 10.1.1.240

route -n add -host 10.112.230.8 10.1.1.240

#route -n add -net 10.112.230.0/24 10.1.1.250

route -n add -net 10.166.145.0/24 10.1.1.240

# Test Autogrid Route

route -n add 19.110.66.48 10.40.1.39

# Autogrid Routes Old

route -n add 19.197.2.93 10.40.1.39

route -n add 19.197.2.171 10.40.1.39

route -n add 19.197.2.183 10.40.1.39

route -n add 19.197.6.35 10.40.1.39

route -n add -net 136.8.159.0/24 10.40.1.39

route -n add -net 136.9.242.0/24 10.40.1.39

route -n add -net 136.9.246.0/24 10.40.1.39

route -n add -net 136.9.249.0/24 10.40.1.39

route -n add -net 136.9.252.0/24 10.40.1.39

route -n add -net 136.130.208.0/24 10.40.1.39

route -n add -net 192.28.103.0/24 10.40.1.39

route -n add 193.129.10.228 10.40.1.39

# Autogrid Routes New

#route -n add 19.197.2.93 10.1.1.246

#route -n add 19.197.2.171 10.1.1.246

#route -n add 19.197.2.183 10.1.1.246

#route -n add 19.197.6.35 10.1.1.246

#route -n add -net 136.8.159.0/24 10.1.1.246

#route -n add -net 136.9.242.0/24 10.1.1.246

#route -n add -net 136.9.246.0/24 10.1.1.246

#route -n add -net 136.9.249.0/24 10.1.1.246

#route -n add -net 136.9.252.0/24 10.1.1.246

#route -n add -net 136.130.208.0/24 10.1.1.246

#route -n add -net 192.28.103.0/24 10.1.1.246

#route -n add 193.129.10.228 10.1.1.246

# Bill Buckles LAN

route -n add -net 172.17.150.0/24 10.1.1.254

route -n add -net 172.17.158.0/24 10.1.1.254

route -n add -net 192.168.1.0/24 10.1.1.254

route -n add -net 192.168.5.0/24 10.1.1.254

route -n add -net 192.168.6.0/24 10.1.1.254

# Dealerlink Routes

route -n add -net 10.20.0.0/16 10.40.1.33

route -n add -net 10.21.0.0/16 10.40.1.33

route -n add -net 10.30.0.0/16 10.40.1.33

route -n add -net 10.31.0.0/16 10.40.1.33

route -n add -net 10.40.3.0/24 10.40.1.33

route -n add -net 10.40.5.0/24 10.40.1.33

route -n add -net 10.40.6.0/24 10.40.1.33

route -n add -net 10.40.7.0/24 10.40.1.33

route -n add -net 10.40.9.0/24 10.40.1.33

route -n add -net 10.41.0.0/16 10.40.1.33

route -n add -net 10.81.7.0/24 10.40.1.33

route -n add -net 10.81.12.0/24 10.40.1.33

route -n add -net 10.81.34.0/24 10.40.1.33

route -n add -net 10.81.51.0/24 10.40.1.33

route -n add -net 10.81.60.0/24 10.40.1.33

route -n add -net 10.81.80.0/24 10.40.1.33

route -n add -net 10.81.105.0/24 10.40.1.33

route -n add -net 10.81.114.0/24 10.40.1.33

route -n add -net 10.81.122.0/24 10.40.1.33

route -n add -net 10.81.127.0/24 10.40.1.33

route -n add -net 10.81.137.0/24 10.40.1.33

route -n add -net 10.81.142.0/24 10.40.1.33

route -n add -net 10.81.168.0/24 10.40.1.33

route -n add -net 10.81.174.0/24 10.40.1.33

route -n add -net 10.81.205.0/24 10.40.1.33

route -n add -net 10.81.241.0/24 10.40.1.33

route -n add -net 10.82.6.0/24 10.40.1.33

route -n add -net 10.85.41.0/24 10.40.1.33

route -n add -net 10.100.12.0/24 10.40.1.33

route -n add -net 100.100.150.0/24 10.40.1.33

route -n add 122.122.125.5 10.40.1.33

route -n add 122.122.125.30 10.40.1.33

route -n add 172.20.3.66 10.40.1.33

route -n add 172.20.3.98 10.40.1.33

route -n add 172.20.3.132 10.40.1.33

route -n add 172.20.3.162 10.40.1.33

route -n add 172.20.3.194 10.40.1.33

route -n add 172.20.4.34 10.40.1.33

route -n add 192.168.0.5 10.40.1.33

route -n add -net 192.168.3.0/24 10.40.1.33

route -n add -net 192.168.24.0/24 10.40.1.33

route -n add -net 192.168.30.0/24 10.40.1.33

route -n add -net 203.13.244.0/24 10.40.1.33

route -n add -net 203.23.31.0/24 10.40.1.33

route -n add -net 203.25.41.0/24 10.40.1.33

route -n add -net 203.25.42.0/24 10.40.1.33

route -n add 203.53.30.232 10.40.1.33

route -n add 203.166.118.195 10.40.1.33

# Klosters LAN

route -n add -net 172.17.104.0/22 10.1.1.254

route -n add -net 172.17.8.0/24 10.1.1.254

route -n add -net 172.17.48.0/24 10.1.1.254

route -n add -net 172.17.74.0/24 10.1.1.254

route -n add -net 172.17.75.0/24 10.1.1.254

route -n add -net 172.17.128.0/24 10.1.1.254

route -n add -net 172.17.208.0/24 10.1.1.254

# Management LAN

route -n add -net 192.168.248.0/24 10.1.1.239

# Mazda Routes

route -n add -net 10.3.0.0/16 10.40.1.35

route -n add -net 10.4.0.0/16 10.40.1.35

route -n add -net 136.133.248.0/24 10.40.1.35

route -n add -net 19.190.18.0/24 10.40.1.35

#route -n add -net 19.190.18.0/24 10.1.1.246

route -n add 19.197.2.141 10.40.1.35

# Porsche Routes

route -n add -net 10.61.1.0/24 10.40.1.37

route -n add 10.61.248.65 10.40.1.37

route -n add 10.61.248.66 10.40.1.37

route -n add -net 84.21.39.0/24 10.40.1.37

route -n add 84.21.52.11 10.40.1.37

route -n add 84.21.53.11 10.40.1.37

route -n add 141.36.132.85 10.40.1.37

route -n add 192.168.200.34 10.40.1.37

route -n add 193.175.6.2 10.40.1.37

route -n add 203.26.190.6 10.40.1.37

route -n add 203.26.190.226 10.40.1.37

# Subaru Inchape Routes

# route -n add -net 172.16.211.0/24 ????

# route -n add -net 172.17.132.0/24 ????

# route -n add 192.168.3.3 ????

# Toyota Routes

route -n add -net 10.9.100.0/24 10.40.1.46

route -n add -net 132.147.0.0/16 10.40.1.46

route -n add -net 150.45.0.0/16 10.40.1.46

route -n add -net 192.168.42.0/24 10.40.1.46

route -n add -net 192.168.101.0/24 10.40.1.46

route -n add -net 192.168.108.0/24 10.40.1.46

route -n add -net 192.168.109.0/24 10.40.1.46

route -n add -net 192.168.206.0/24 10.40.1.46

# VW Routes

#route -n add -net 10.112.198.0/24 10.1.1.250

route -n add -net 10.112.198.0/24 10.1.1.240

#route -n add -net 10.152.15.0/24 10.1.1.250

route -n add -net 10.152.15.0/24 10.1.1.240

#route -n add -net 172.16.61.0/24 10.1.1.250

route -n add -net 172.16.61.0/24 10.1.1.240

#route -n add 210.193.223.156 10.1.1.250

route -n add 210.193.223.156 10.1.1.240

# Start ftpproxy

ftpproxy\_flags=""

# Start squiddy

# if [ -x /usr/local/sbin/squid ]; then

# echo -n ' squid'; /usr/local/sbin/squid

# fi

echo '.'

**Appendix B - /etc/mail/relay-domains**

# $OpenBSD: relay-domains,v 1.2 2003/12/23 21:17:04 miod Exp $

#

# List of other domains to relay mail for here (one per line).

# By default, sendmail(8) will not relay for foreign domains. If the mail

# is not destined for (or sent by) a user in the local domain the message

# will be rejected. Alternately, domains may be listed in /etc/mail/access

# with the RELAY attribute instead of being enumerated here.

#

# This file is read only at startup or when sendmail(8) is sent SIGHUP.

#

13zoos.com

13zoos.com.au

1300zoos.com

1300zoos.com.au

1300zoos.net

1300zoos.net.au

20hoursale.com

20hoursale.com.au

4wdzoo.com.au

4wdzoo.net

4wdzoo.net.au

4wdzoos.com

4wdzoos.com.au

4wdzoos.net

4wdzoos.net.au

4x4zoo.com.au

4x4zoo.net.au

4x4zoo.com

4x4zoo.net

4x4zoos.com.au

4x4zoos.net.au

4x4zoos.com

4x4zoos.net

adelaidesubaru.com.au

apauctions.com.au

apbma.com.au

apeagers.com.au

apeagers.biz

apeagers.mobi

apeagers.net.au

apeagers.net

apeptc.com.au

audicentresunshinecoast.com.au

audicentredarwin.com.au

australhonda.com.au

australjaguar.com.au

australlandrover.com.au

australmotorgroup.com.au

australmotors.com.au

australnewstead.com.au

austral-porsche.com.au

australprestige.com.au

australvolkswagen.com.au

austral-volkswagen.com.au

australvolvo.com.au

australvw.com.au

autozoos.com.au

autozoos.net.au

autozoos.com

autozoos.net

bikezoo.net.au

bikezoos.com.au

bikezoos.net.au

bikezoos.com

bikezoos.net

boatzoos.com.au

boatzoos.net.au

boatzoos.com

boatzoos.net

bridgeautos.com.au

bridgetoyota.com.au

brisbanecityjaguar.com.au

brisbanecitysubaru.com.au

brisbanejaguar.com.au

brisbanemotorauctions.com.au

brisbanesubaru.com.au

calcityautos.com.au

calcityauto.com.au

caloundracityautos.com.au

caloundracitygreatwall.com.au

caloundracityholden.com.au

caloundracityhonda.com.au

caloundracitymitsubishi.com.au

caloundracitysuzuki.com.au

calcityholden.com.au

calcityhonda.com.au

calcitymitsubishi.com.au

calcitysuzuki.com.au

canberrasubaru.com.au

carzoo.net.au

carzoo.biz

carzoos.com.au

carzoos.net.au

carzoos.biz

carzoos.com

carzoos.info

carzoos.mobi

carzoos.net

ccautos.com.au

citroensunshinecoast.com.au

cityautomotive.com.au

city-automotive.com.au

citymitsubishibrisbane.com.au

citypeugeotbrisbane.com.au

dapallterrain.com

dapallterrain.com.au

darwinsubaru.com.au

discountcarsandcommercials.com.au

discountcarsdarwin.com.au

discountcarparts.net.au

eagers.com.au

eagersfleet.com.au

eagers-holden.com.au

eagersholden.com.au

eagersholden.mobi

eagershsv.com.au

eagers-kia.com.au

eagerskia.com.au

eagerskia.mobi

eagersmazda.com.au

eagersmazda.mobi

eagers-mazda.com.au

eagersmitsubishi.com.au

eagersmitsubishi.mobi

eagers-mitsubishi.com.au

eagersusedcars.com.au

financezoos.com.au

financezoos.net.au

financezoos.com

financezoos.net

fordhomedrive.com.au

fordonlineshop.com.au

grwcars.com.au

hiddenvalleyford.com.au

hobartsubaru.com.au

homedrive.com.au

homedrive.net.au

lexusofdarwin.com.au

mazdadeals.com.au

metroford.com.au

metrofordhomedrive.com.au

metropanel.com.au

metropanel.net.au

metroparts.com.au

metrotorque.com.au

moneyzoo.com.au

moneyzoo.net.au

moneyzoos.com.au

moneyzoos.net.au

moneyzoos.com

moneyzoos.net

mopedzoo.com.au

mopedzoo.net.au

mopedzoo.com

mopedzoo.net

mopedzoos.com.au

mopedzoos.net.au

mopedzoos.com

mopedzoos.net

newcastlesubaru.com.au

newsteadservice.com.au

newsteadstrip.com.au

partszoo.com.au

partszoo.net.au

partszoos.com.au

partszoos.com

partszoos.net.au

partszoos.net

perthsubaru.com.au

peugeotonjames.com.au

porschecentrebrisbane.com.au

porschecentrebrisbane.net.au

porschecentredarwin.com.au

powerzoo.com.au

powerzoo.net.au

powerzoos.com.au

powerzoos.net.au

powerzoos.com

powerzoos.net

protondarwin.com.au

qldusedcars.com.au

scooterzoo.com.au

scooterzoo.net.au

scooterzoos.com.au

scooterzoos.net.au

scooterzoos.com

scooterzoos.net

servicezoo.com.au

servicezoo.net.au

servicezoos.com.au

servicezoos.net.au

servicezoos.com

servicezoos.net

southsidehonda.com.au

southsidelandrover.com.au

southsideprestige.com.au

southsidevolvo.com.au

southsideford.com.au

southsidetoyota.com.au

strathpinetoyota.com.au

stuartmotorgroup.com.au

subarucity.com

subarucity.com.au

subarudarwin.com.au

subarutoowong.com.au

sydneysubaru.com.au

theultimatedrivingmachine.com.au

theusedcarshop.com.au

torqueford.com.au

torquegroup.com.au

torquegroup.net.au

torquehonda.com.au

torquekia.com.au

torquesubaru.com.au

torquetoyota.com.au

truckzoo.com.au

truckzoo.net.au

truckzoos.com.au

truckzoos.net.au

truckzoos.com

truckzoos.net

twentyhoursale.com

twentyhoursale.com.au

usedcarbrisbane.net

westpointsubaru.com.au

**Appendix C - /etc/apeagers.conf**

#############################

# AP Eagers Firewall Config

# 2010-07-30

# Author: Michael Spence

#############################

# Default parameters

set require-order no

set skip on lo

#++++++++++++++

# Macros START

#++++++++++++++

# Interfaces

ext\_if="vic0" # External Interface

int\_if="vic1" # Internal Interface

dms\_if="vic2" # DMS Interface

b2b\_if="vic3" # B2B Interface

# Proxy internet ports

inet\_ports="{ 80, 443 }"

# Additional Ext IP addresses

ext\_194="203.38.61.194"

#--------------

# Servers BEGIN

#--------------

ape\_ftp\_ext="203.38.61.203" # AP Eagers FTP

bne\_dax09="10.1.1.22" # bne-dax09

bne\_iis="10.1.1.9" # bne-iis

bne\_mx1="10.1.1.32" # bne-mx1

carzoos\_ftp\_ext="203.38.61.204" # Carzoos FTP

citrix\_ext="203.38.61.205" # NFuse Ext

citrix\_int="10.1.1.6" # NFuse Int

intranet\_ext="203.38.61.206" # Intranet Ext

intranet\_int="10.1.1.13" # Intranet Int

owa\_ext="203.38.61.193" # OWA Ext

proxy\_svrs="{ 10.1.254.45, 10.1.1.8, 10.1.1.18, 10.1.1.25, 10.1.1.41, 10.1.1.42, 10.1.1.48, 10.1.1.49, 10.1.1.59, 10.1.1.68, 10.1.1.69, 10.1.11.9, 10.2.254.1, 10.25.4.16, 10.34.1.68, 10.34.1.69, 10.35.1.111, 10.34.100.71, 10.40.1.51, 192.168.248.0/24 }"

vga\_juniper\_ext="10.40.1.61"

vga\_juniper\_int="10.1.1.240"

#--------------

# Servers END

#--------------

#----------------------------

# Manufacturer Networks START

#----------------------------

audi\_sites="{ 10.112.192.0/24, 10.112.230.0/24, 10.166.145.0/24, 61.88.114.35 }"

autogrid\_sites="{ 19.197.2.93, 19.197.2.171, 19.197.2.183, 19.197.6.35, 136.8.159.0/24, 136.9.242.0/24, 136.9.246.0/24, 136.9.249.0/24, 136.9.252.0/24, 136.130.208.0/24, 192.28.103.0/24, 193.129.10.228, 19.110.66.48 }"

bma\_sites="{ 210.8.199.67, 210.8.223.54 }"

capital\_finance="202.160.110.10"

citroen\_sites="{ 74.125.19.147, 81.255.178.161, 194.250.98.65, 203.210.109.237 }"

dealerlink\_sites="{ 10.20.0.0/16, 10.21.0.0/16, 10.30.0.0/16, 10.31.0.0/16, 10.40.3.0/24, 10.40.5.0/24, 10.40.6.0/24, 10.40.7.0/24, 10.40.9.0/24, 10.41.0.0/16, 10.81.7.0/24, 10.81.12.0/24, 10.81.34.0/24, 10.81.51.0/24, 10.81.60.0/24, 10.81.80.0/24, 10.81.105.0/24, 10.81.114.0/24, 10.81.122.0/24, 10.81.127.0/24, 10.81.142.0/24, 10.81.168.0/24, 10.81.174.0/24, 10.81.205.0/24, 10.81.241.0/24, 10.82.6.0/24, 10.85.41.0/24, 10.100.12.0/24, 100.100.150.0/24, 122.122.125.5, 122.122.125.30, 172.20.3.66, 172.20.3.98, 172.20.3.132, 172.20.3.162, 172.20.3.194, 172.20.4.34, 192.168.0.5, 192.168.3.0/24, 192.168.24.0/24, 192.168.30.0/24, 203.13.244.0/24, 203.23.31.0/24, 203.25.41.0/24, 203.25.42.0/24, 203.53.30.232, 203.166.118.195 }"

ford\_sites="{ 64.14.29.50, 136.1.25.105, 136.2.12.190, 136.1.241.107 }"

holden\_sites="{ 66.235.128.158, 66.235.132.121, 66.235.132.152, 72.247.49.230, 72.5.123.29, 72.247.247.88, 96.6.229.230, 148.95.0.0/16, 198.208.16.25, 198.208.16.26, 198.208.54.157, 198.208.154.157, 198.208.187.168 }"

inchape\_sites="192.168.3.3"

jaguar\_sites="{ 72.247.247.161, 72.247.247.176, 80.231.29.29, 96.6.230.123, 140.174.24.168, 140.174.24.201 }"

kia\_sites="203.53.30.232"

mazda\_sites="{ 10.3.0.0/16, 10.4.0.0/16, 19.190.18.0/24, 19.197.2.141 }"

mitsubishi\_sites="{ 159.196.36.12, 159.196.36.15, 159.196.36.16, 159.196.36.125, 202.45.13.114 }"

peugeot\_sites="203.53.30.233"

porsche\_sites="{ 10.61.1.0/24, 10.61.248.65, 10.61.248.66, 84.21.39.0/24, 84.21.52.11, 84.21.53.11, 84.21.53.14, 84.21.53.16, 141.36.132.85, 192.168.200.34, 193.175.6.2, 193.175.6.66, 203.26.190.6, 203.26.190.226 }"

toyota\_sites="{ 10.9.100.0/24, 132.147.0.0/16, 150.45.0.0/16, 192.168.42.0/24, 192.168.101.0/24, 192.168.108.0/24, 192.168.109.0/24, 192.168.206.0/24, 208.39.44.0/24, 208.39.45.0/24, 216.14.206.48 }"

volvo\_sites="136.8.154.0/24"

vw\_sites="{ 10.112.198.0/24, 10.152.15.0/24, 172.16.61.0/24, 210.193.223.156 }"

#--------------------------

# Manufacturer Networks END

#--------------------------

#-------------------------

# Proxy Bypass Sites START

#-------------------------

addresslink\_sites="210.193.214.83"

ato\_sites="203.202.41.80"

caplink\_sites="203.153.237.100"

carsales\_sites="{ 140.174.24.8, 140.174.24.80, 140.174.24.177, 140.174.24.218 }"

dais\_sites="{ 203.94.167.209, 203.9.185.207, 203.9.185.233 }"

dealerlogic\_sites="{ 203.94.176.180, 203.94.176.181 }"

fowles\_sites="{ 203.166.110.40, 203.166.110.41 }"

ibmhmc\_sites="{ 129.42.160.48, 129.42.160.50, 207.25.252.200, 207.25.252.205 }"

liberty\_sites="{ 202.45.13.114, 202.45.13.124 }"

motorone\_sites="203.35.213.102"

pickles\_sites="202.58.54.235"

stgeorge\_sites="{ 166.120.202.249, 203.16.39.136, 203.16.39.137, 203.16.39.138, 203.16.39.139, 203.23.44.136, 203.23.44.137, 203.23.44.138, 203.23.44.139 }"

suncorp\_sites="{ 203.0.222.16, 203.0.222.101, 203.110.139.190 }"

tipt\_sites="203.44.43.220"

vital\_sites="{ 202.125.164.104, 67.19.91.90 }"

#-----------------------

# Proxy Bypass Sites END

#-----------------------

#---------------------

# External Sites START

#---------------------

billbuckles\_ext="203.43.230.186"

klosters\_ext="203.38.221.86"

surfers\_ext="210.56.85.111"

surfers\_ext2="210.56.85.112"

external\_sites="{" $billbuckles\_ext $klosters\_ext $surfers\_ext $surfers\_ext2 "}"

external\_ftp\_sites="{" $billbuckles\_ext $klosters\_ext $surfers\_ext $surfers\_ext2 "}"

messagelabs="{ 62.231.131.0/24, 67.219.240.0/20, 85.158.136.0/21, 95.131.104.0/21, 117.120.16.0/21, 193.109.254.0/23, 194.106.220.0/23, 195.245.230.0/23, 216.82.240.0/20 }"

#---------------------

# External Sites END

#---------------------

# Citrix Ports

citrix\_ports="{ 80, 1494 }"

# MSN Messenger Ports

msn\_msg\_ports="{ 1493, 1542, 1863, 1963 }"

# File Sharing PTP

torrents="{ 6881, 37001, 37002, 37003, 37000 }"

p2p="{ 1214, 5000, 5555, 6346, 777, 8331, 8875, 8888, 6257, 6699 }"

cvsup="5999"

pptp="1723"

# Instant Messaging Clients

jabber="5222"

icqaim="5190"

irc="6667"

#++++++++++++++

# Macros END

#++++++++++++++

#++++++++++++++

# Ruleset BEGIN

#++++++++++++++

# Scrub

scrub in all

#--------------

# NAT/RDR BEGIN

#--------------

# Default NAT/RDR

nat on $ext\_if from !($ext\_if) -> ($ext\_if:0)

# Inchape NAT/RDR

nat on $int\_if from any to 192.168.3.3 -> $int\_if

# Audi NAT/RDR

nat on $int\_if from any to 10.112.192.0/24 -> $int\_if

nat on $int\_if from any to 10.166.145.0/24 -> $int\_if

# Redirect VW VGA Juniper

rdr on $ext\_if from 61.88.114.38 to any -> $vga\_juniper\_ext # VW VPN to Ext int of VGA Juniper

rdr on $ext\_if from 119.225.2.78 to any -> $vga\_juniper\_ext # Audi VPN to Ext int of VGA Juniper

rdr on $ext\_if from 210.48.210.1 to any -> $vga\_juniper\_ext # may no longer be in use, Ext int of VGA Juniper

# VW NAT/RDR

nat on $int\_if from any to 10.112.198.0/24 -> $int\_if

nat on $int\_if from any to 10.112.230.0/24 -> $int\_if

#no nat on $int\_if from 10.10.9.60 to 10.152.15.0/24

nat on $int\_if from any to 10.152.15.0/24 -> $int\_if

nat on $int\_if from any to 172.16.61.0/24 -> $int\_if

nat on $int\_if from any to 210.193.223.156 -> $int\_if

# Toyota NAT/RDR

nat on $int\_if from any to 10.9.100.0/24 -> $int\_if

nat on $int\_if from any to 132.147.0.0/16 -> $int\_if

nat on $int\_if from any to 150.45.0.0/16 -> $int\_if

nat on $int\_if from any to 192.168.42.0/24 -> $int\_if

nat on $int\_if from any to 192.168.101.0/24 -> $int\_if

nat on $int\_if from any to 192.168.108.0/24 -> $int\_if

nat on $int\_if from any to 192.168.109.0/24 -> $int\_if

nat on $int\_if from any to 192.168.206.0/24 -> $int\_if

# NAT for DWN ERA

nat on $b2b\_if from 172.20.3.40 to 19.190.18.11 -> $b2b\_if

#--------------

# NAT/RDR END

#--------------

# FTP Anchor

nat-anchor "ftp-proxy/\*"

rdr-anchor "ftp-proxy/\*"

rdr on $int\_if proto tcp from any to any port 21 -> 127.0.0.1 port 8021

anchor "ftp-proxy/\*"

#-------------------------

# Remote Connections BEGIN

#-------------------------

# AP Eagers FTP

rdr on $ext\_if proto tcp from $external\_ftp\_sites to $ape\_ftp\_ext port ftp -> $bne\_iis

rdr on $ext\_if proto tcp from $external\_ftp\_sites to $ape\_ftp\_ext port 49151:65535 -> $bne\_iis

# Carzoos FTP

rdr on $ext\_if proto tcp from $external\_ftp\_sites to $carzoos\_ftp\_ext port ftp -> $bne\_dax09

rdr on $ext\_if proto tcp from $external\_ftp\_sites to $carzoos\_ftp\_ext port 49152:65535 -> $bne\_dax09

# Citrix NFuse

rdr on $ext\_if proto tcp from any to $citrix\_ext port www -> $citrix\_int

rdr on $ext\_if proto tcp from any to $citrix\_ext port 1494 -> $citrix\_int

# Intranet Access

rdr on $ext\_if proto tcp from $external\_sites to $intranet\_ext port 80 -> $intranet\_int

# OWA Access

rdr on $ext\_if proto tcp from any to $owa\_ext port 80 -> $bne\_mx1 port 80

pass in log on $ext\_if proto tcp from any to $bne\_mx1 port 80

# SMTP Access

rdr on $ext\_if proto tcp from $messagelabs to any port 25 -> localhost

# VGA pass traffic to Juniper

pass in log quick on $ext\_if from 61.88.114.38 to $vga\_juniper\_ext keep state

pass in log quick on $ext\_if from 119.225.2.78 to $vga\_juniper\_ext keep state

pass in log quick on $ext\_if from 210.48.210.1 to $vga\_juniper\_ext keep state

#-------------------------

# Remote Connections END

#-------------------------

# Default deny

block in log all

# Deny Outgoing Dodgy ports

block out log quick on $ext\_if proto { tcp, udp } from any to any port $msn\_msg\_ports

block out log quick on $ext\_if proto { tcp, udp } from any to any port $torrents

block out log quick on $ext\_if proto { tcp, udp } from any to any port $p2p

block out log quick on $ext\_if proto { tcp, udp } from any to any port $cvsup

block out log quick on $ext\_if proto { tcp, udp } from any to any port $jabber

block out log quick on $ext\_if proto { tcp, udp } from any to any port $icqaim

block out log quick on $ext\_if proto { tcp, udp } from any to any port $irc

block out log quick on $ext\_if proto { tcp, udp } from any to any port $pptp

#-------------------------

# Remote Connections BEGIN

#-------------------------

# AP Eagers FTP

pass in log quick on $ext\_if proto tcp from $external\_ftp\_sites to $bne\_iis port ftp

pass in log quick on $ext\_if proto tcp from $external\_ftp\_sites to $bne\_iis port > 49151

# Carzoos FTP

pass in log quick on $ext\_if proto tcp from $external\_ftp\_sites to $bne\_dax09 port ftp

pass in log quick on $ext\_if proto tcp from $external\_ftp\_sites to $bne\_dax09 port > 49151

# Citrix NFuse

pass in log quick on $ext\_if proto tcp from any to $citrix\_int port $citrix\_ports

# email from Messagelabs

pass in quick on $ext\_if proto tcp from $messagelabs to any port 25 keep state

# Intranet Access

pass in quick on $ext\_if proto tcp from $external\_sites to $intranet\_int port www

# OWA Access

pass in quick on $ext\_if proto tcp from any to $bne\_mx1 port www

#-------------------------

# Remote Connections END

#-------------------------

# Allow all traffic out.

pass out all

# Allow all ERA traffic

pass quick on $dms\_if no state

# Allow all B2B traffic

pass quick on $b2b\_if no state

# Pass in internal traffic

pass on $int\_if no state

pass out on $int\_if from any to any keep state

# Allow sites to bypass proxy

pass in quick on $int\_if proto { tcp, udp } from any to $addresslink\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $ato\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $caplink\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $carsales\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $dais\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $dealerlogic\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $fowles\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $ibmhmc\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $liberty\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $motorone\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $pickles\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $stgeorge\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $suncorp\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $tipt\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $vital\_sites port $inet\_ports

# Allow Manufacturer web traffic to bypass proxy

pass in quick on $int\_if proto { tcp, udp } from any to $audi\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $autogrid\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $bma\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $capital\_finance port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $citroen\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $dealerlink\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $ford\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $holden\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $inchape\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $jaguar\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $kia\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $mazda\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $mitsubishi\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $peugeot\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $porsche\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $toyota\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $volvo\_sites port $inet\_ports

pass in quick on $int\_if proto { tcp, udp } from any to $vw\_sites port $inet\_ports

# Allow/Block internet traffic

pass in quick on $int\_if proto { tcp, udp } from $proxy\_svrs to any port $inet\_ports

block in on $int\_if proto { tcp, udp } from any to any port $inet\_ports

# Antispoof loopback

antispoof quick for { lo $int\_if }

# Allow DNS transfers and queries

pass in quick on $int\_if proto { tcp, udp } from any port 53 to any keep state

pass in quick on $dms\_if proto { tcp, udp } from any port 53 to any keep state

pass in quick on $b2b\_if proto { tcp, udp } from any port 53 to any keep state

pass in quick on $int\_if proto { tcp, udp } from any to any port 53 keep state

pass in quick on $dms\_if proto { tcp, udp } from any to any port 53 keep state

pass in quick on $b2b\_if proto { tcp, udp } from any to any port 53 keep state

# By default, do not permit remote connections to X11

#block in on ! lo0 proto tcp from any to any port 6000

#++++++++++++++

# Ruleset END

#++++++++++++++

**Appendix D - /etc/mail/access**

# $OpenBSD: access,v 1.1 2003/09/23 21:37:11 millert Exp $

#

# sendmail(8) access database. Rebuild by running as root:

# makemap hash /etc/mail/access < /etc/mail/access

#

# See /usr/share/sendmail/README for a description of this file

# under the "access\_db" feature.

#

Connect:67.219.240.0/20 RELAY

Connect:95.131.104.0/21 RELAY

Connect:62.231.131.0/24 RELAY

Connect:85.158.136.0/21 RELAY

Connect:193.109.254.0/23 RELAY

Connect:194.106.220.0/23 RELAY

Connect:195.245.230.0/23 RELAY

Connect:216.82.240.0/20 RELAY

Connect:117.120.16.0/21 RELAY

**Appendix E – qld-esx1 port config**

Refer to “Replacement Corporate Firewall untilising ESXi 4.1 Infrastructure” written by Timothy Walters

**Appendix F – emp\_core\_3560g-48ts\_2 configuration**

version 12.2

no service pad

service timestamps debug uptime

service timestamps log uptime

service password-encryption

!

hostname emp\_core\_c3560g\_48ts\_2

!

enable secret 5 $1$UICO$5LN2GCe0JwoEyYxEPNXX0.

enable password 7 1500030202237B7C

!

no aaa new-model

clock timezone AEST 10

ip subnet-zero

ip domain-name apeagers.com.au

ip name-server 10.1.1.43

!

no file verify auto

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

interface Port-channel1

switchport access vlan 2

switchport mode access

!

interface Port-channel2

switchport access vlan 2

switchport mode access

!

interface Port-channel3

switchport access vlan 2

switchport mode access

!

interface Port-channel4

switchport access vlan 2

switchport mode access

!

interface GigabitEthernet0/1

!

interface GigabitEthernet0/2

!

interface GigabitEthernet0/3

!

interface GigabitEthernet0/4

!

interface GigabitEthernet0/5

!

interface GigabitEthernet0/6

!

interface GigabitEthernet0/7

!

interface GigabitEthernet0/8

!

interface GigabitEthernet0/9

!

interface GigabitEthernet0/10

!

interface GigabitEthernet0/11

!

interface GigabitEthernet0/12

!

interface GigabitEthernet0/13

!

interface GigabitEthernet0/14

!

interface GigabitEthernet0/15

!

interface GigabitEthernet0/16

!

interface GigabitEthernet0/17

!

interface GigabitEthernet0/18

switchport access vlan 666

switchport mode access

!

interface GigabitEthernet0/19

switchport access vlan 666

switchport mode access

!

interface GigabitEthernet0/20

switchport access vlan 666

switchport mode access

!

interface GigabitEthernet0/21

switchport access vlan 666

switchport mode access

!

interface GigabitEthernet0/22

switchport access vlan 3

switchport mode access

!

interface GigabitEthernet0/23

switchport access vlan 3

switchport mode access

!

interface GigabitEthernet0/24

switchport access vlan 3

switchport mode access

!

interface GigabitEthernet0/25

switchport access vlan 2

switchport mode access

channel-group 1 mode active

!

interface GigabitEthernet0/26

switchport access vlan 2

switchport mode access

channel-group 1 mode active

!

interface GigabitEthernet0/27

switchport access vlan 2

switchport mode access

channel-group 2 mode active

!

interface GigabitEthernet0/28

switchport access vlan 2

switchport mode access

channel-group 2 mode active

!

interface GigabitEthernet0/29

switchport access vlan 2

switchport mode access

channel-group 4 mode active

!

interface GigabitEthernet0/30

switchport access vlan 2

switchport mode access

channel-group 4 mode active

!

interface GigabitEthernet0/31

switchport access vlan 2

switchport mode access

channel-group 4 mode active

!

interface GigabitEthernet0/32

switchport access vlan 2

switchport mode access

channel-group 4 mode active

!

interface GigabitEthernet0/33

switchport access vlan 2

switchport mode access

channel-group 3 mode active

!

interface GigabitEthernet0/34

switchport access vlan 2

switchport mode access

channel-group 3 mode active

!

interface GigabitEthernet0/35

switchport access vlan 2

switchport mode access

channel-group 3 mode active

!

interface GigabitEthernet0/36

switchport access vlan 2

switchport mode access

channel-group 3 mode active

!

interface GigabitEthernet0/37

switchport access vlan 2

switchport mode access

!

interface GigabitEthernet0/38

switchport access vlan 2

switchport mode access

!

interface GigabitEthernet0/39

switchport access vlan 2

switchport mode access

!

interface GigabitEthernet0/40

switchport access vlan 2

switchport mode access

!

interface GigabitEthernet0/41

switchport access vlan 2

switchport mode access

!

interface GigabitEthernet0/42

switchport access vlan 2

switchport mode access

!

interface GigabitEthernet0/43

switchport access vlan 2

switchport mode access

!

interface GigabitEthernet0/44

switchport access vlan 5

switchport mode access

!

interface GigabitEthernet0/45

switchport access vlan 5

switchport mode access

!

interface GigabitEthernet0/46

switchport access vlan 5

switchport mode access

!

interface GigabitEthernet0/47

description ipman

switchport trunk encapsulation dot1q

switchport mode access

!

interface GigabitEthernet0/48

description uplink

switchport trunk encapsulation dot1q

switchport mode trunk

!

interface GigabitEthernet0/49

!

interface GigabitEthernet0/50

switchport trunk encapsulation dot1q

switchport mode trunk

!

interface GigabitEthernet0/51

!

interface GigabitEthernet0/52

switchport trunk encapsulation dot1q

switchport mode trunk

!

interface Vlan1

ip address 10.1.1.244 255.255.0.0

!

ip classless

ip http server

!

snmp-server community apsnmpro RO

!

control-plane

!

line con 0

line vty 0 4

password 7 14051A050A0D7A73

no login

line vty 5 15

password 7 14051A050A0D7A73

no login

!

ntp server 10.1.1.43

end

**Appendix G – Michael’s Backup Scripts**

**backup.sh (run as su)**

#!/bin/ksh

cp /etc/rc.local data/backup/etc/.

cp /etc/apeagers.conf data/backup/etc/.

cp /etc/rc.conf data/backup/etc/.

cp /etc/resolv.conf data/backup/etc/.

cp /etc/sysctl.conf data/backup/etc/.

cp /etc/mygate data/backup/etc/.

cp /etc/hostname.vic0 data/backup/etc/.

cp /etc/hostname.vic1 data/backup/etc/.

cp /etc/hostname.vic2 data/backup/etc/.

cp /etc/hostname.vic3 data/backup/etc/.

cp /etc/mail/relay-domains data/backup/mail/.

cp /etc/mail/access data/backup/mail/.

cp /usr/bin/monitor-pf data/backup/bin/.

cp /usr/bin/grep-pf data/backup/bin/.

cp /usr/bin/restart-pf data/backup/bin/.

cp bin/backup.sh data/backup/.

chown -R mspence data/backup/\*

**backup.bat (run on windows)**

pscp -r mspence@10.1.1.253:data/backup/\* backup/.

**restore.bat (run on windows)**

pscp -r bne-obfw45/\* mspence@10.1.1.253:data/restore/.

**restore.sh (run as su)**

#!/bin/ksh

chown -R root:wheel data/restore/\*

cp data/restore/etc/rc.local /etc/.

cp data/restore/etc/apeagers.conf /etc/.

cp data/restore/etc/rc.conf /etc/.

cp data/restore/etc/resolv.conf /etc/.

cp data/restore/etc/sysctl.conf /etc/.

cp data/restore/etc/mygate /etc/.

cp data/restore/etc/hostname.vic0 /etc/.

cp data/restore/etc/hostname.vic1 /etc/.

cp data/restore/etc/hostname.vic2 /etc/.

cp data/restore/etc/hostname.vic3 /etc/.

cp data/restore/mail/relay-domains /etc/mail/.

cp data/restore/mail/access /etc/mail/.

cp data/restore/bin/monitor-pf /usr/bin/.

cp data/restore/bin/grep-pf /usr/bin/.

cp data/restore/bin/restart-pf /usr/bin/.