OpenBSD PF Router/Firewall Plus VLAN

In this document the firewall/router runs on a dedicated physical machine. The **WAN** NIC of this machine is called **bge0** and the **LAN** NIC is called **re0**.

This machine provides Internet access for two networks: the LAN network of **192.168.0.0/24** and a VLAN network of **172.16.5.0/24**. The VLAN network is used by a wireless access point and has Internet connectivity but none to the LAN network; in other words it's a 'guest' network.

First of all we must enable packet forwarding on this firewall/router machine. Create the file in question if it doesn't already exist.

```
# vim /etc/sysctl.conf

net.inet.ip.forwarding=1
```

To enable the VLAN on the firewall/router machine, create a file something like the following but keep the **hostname** prefix.

```
# vim /etc/hostname.vlan10
```

In this file, add something like the following details.

```
172.16.5.1/24 172.16.5.255 parent re0 vnetid 10
```

Incidentally on a switch connected to the **re0** NIC, I've set a VLAN ID of 10 on one of the ports which connects the wireless access point (which has a similar configuration).

Now that you've added the configuration for the VLAN interface, restart networking by either rebooting or by using the following command.

```
# sh /etc/netstart
```

Here is the firewall/router configuration for **/etc/pf.conf** which contains the VLAN interface. There are also some other rules commmented out which just demonstrate port forwarding (**rdr-to**) , port ranges and table usage.

```
lanif = "re0"
wanif = "bge0"
localnet = $lanif:network
vlanif = "vlan10"
vlannet = $vlanif:network

set skip on lo

set block-policy drop

icmp_types = "{ echoreq, unreach, paramprob, squench, echorep }"

#table <badhosts> persist file "/etc/pftables/bad_hosts.txt"
#table <badnets> persist file "/etc/pftables/bad_networks.txt"

#block in quick log (all) on $wanif from <badhosts> to any
#block in quick log (all) on $wanif from <badnets> to any

match in all scrub (no-df random-id max-mss 1440)

match out on $wanif from $localnet to any nat-to ($wanif)

match out on $wanif from $vlannet to any nat-to ($wanif)

block in on $vlanif from $vlannet to $localnet

pass in quick on $wanif inet proto icmp all icmp-type $icmp_types
pass in on $wanif inet proto tcp from any to any port 22
#pass in on $wanif inet proto tcp from any to any port 443 rdr-to 192.168.0.22
#pass in on $wanif inet proto tcp from any to any port 21 rdr-to 192.168.0.24
#pass in on $wanif inet proto tcp from any to any port 37100:39000 \
#   rdr-to 192.168.0.24


pass out quick inet
pass in on $lanif
```

Enable the new rules by running the following command.

```
# pfctl -f /etc/pf.conf
```

Date	2022-03-25
Updated	2022-03-27
Chosen OS	OpenBSD 7.0