

Create Jail, Networking and NAT

Step 1: Enable IP Forwarding

First, you need to enable IP forwarding on your FreeBSD host. This allows the host to forward packets between the jail and the outside network.

Edit the `/etc/sysctl.conf` file and add the following line:

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

Apply the changes:

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

Step 2: Configure the Host Network Interface

You need to configure the host's network interface to allow NAT.

Identify your network interface (e.g., `em0`, `re0`, etc.) using:

```
ifconfig
```

Set up NAT using `pf` (Packet Filter). First, ensure that `pf` is enabled. Edit `/etc/rc.conf` and add:

```
pf_enable="YES"
```

Create or edit the `/etc/pf.conf` file to include NAT rules. Here's a basic example:

```
ext_if="eth0" # Replace with your external interface
jails_net="10.10.10.0/24" # Replace with your jail network

# Set the default policy
set block-policy return
set loginterface $ext_if

# Jail
nat on $ext_if from $jails_net to any -> ($ext_if)
pass in on $ext_if proto tcp from any to ($ext_if) port { 22, 80, 443 }

# Block all incoming traffic by default
block in all

# Allow incoming traffic on specific ports
pass in on $ext_if proto tcp from any to any port { 22, 80, 443 }

# Allow all outgoing traffic
pass out all
```

Load the `pf` rules:

```
sysrc pf_enable="YES"
kldload pf
pfctl -f /etc/pf.conf
pfctl -e
```

Create Classic Jails

Step 1: Enable the Jail Feature

Make sure the jail feature is enabled in your FreeBSD system. You can check this by looking for the `jail` keyword in your `/etc/rc.conf` file. If it's not there, you can add it.

```
echo 'jail_enable="YES"' >> /etc/rc.conf
```

Step 2: Create a Directory for the Jail

Create a directory where the jail's filesystem will reside. This is typically done in `/usr/jails`.

```
mkdir -p /usr/jails/website
```

Step 3: Install the Base System

You need to populate the jail directory with a FreeBSD base system. You can use the `make` command to extract the base system into the jail directory.

```
mkdir -p /usr/jails/website
mkdir /usr/jail/media
fetch https://download.freebsd.org/ftp/releases/amd64/amd64/14.2-RELEASE/base.txz -o
/usr/jails/media/14.2-RELEASE-base.txz
tar -xf /usr/jails/media/14.2-RELEASE-base.txz -C /usr/jails/website --unlink
```

Setp 4: Copy important Files & Update

```
cp /etc/resolv.conf /usr/jails/website/etc/resolv.conf
cp /etc/localtime /usr/jails/website/etc/localtime
freebsd-update -b /usr/jails/website fetch install
```

Step 5: Create Network interface for Jail

```
sysrc cloned_interfaces+="lo1"
```

Step 6: Configure the Jail in `/etc/jail.conf`:

```
website {  
    path = "/usr/jails/website";  
    sysvshm = "new";  
    host.hostname = "website.local";  
    ip4.addr = "lo1|10.10.10.100/24"; # Assign an IP from your jail network  
    allow.raw_sockets;  
    allow.socket_af;  
    allow.mount;  
    mount.devfs;  
    devfs_ruleset = 111;  
    exec.clean;  
    exec.start = "/bin/sh /etc/rc";  
    exec.stop = "/bin/sh /etc/rc.shutdown";  
}
```

Step 7: Reboot

Reboot Host

```
reboot
```

Step 8: Start the Jail

```
jail -c website
```

Now you should have a jail with networking

Destroy Jail

```
service jail stop website  
chflags -R 0 /usr/jails/website/  
rm -rf /usr/jails/website/
```

Revision #7

Created 21 January 2025 16:50:33 by tinfoil-hat

Updated 21 January 2025 17:46:54 by tinfoil-hat