

# FreeBSD Network Security Exercise

## Networks and Systems Security II (CSE354/554)

### Table of Contents

- 1. Lab Overview
- 2. Virtual Machine Setup
  - VM Specifications
  - Network Topology
- 3. Task 1: Firewall & NAT Configuration
  - Step 1: Assign Static IP Addresses
  - Step 2: Enable IP Forwarding on VM2
  - Step 3: Configure PF Firewall Rules
  - Step 4: Test NAT & Connectivity
- 4. Task 2: Web Server & ACL Configuration
  - Step 1: Install & Configure Nginx
  - Step 2: Set File Permissions with `setuid`
  - Step 3: Apply Linux ACLs
- 5. Validation & Screenshots
- 6. Troubleshooting
- 7. References

### Lab Overview

This lab configures a **FreeBSD-based firewall (VM2)** to perform **bidirectional NAT** and traffic filtering using `pf`, while **VM3** hosts a web server with strict file permissions enforced by **ACLs**. Key objectives:

- 1. Isolate VM1 (client) and VM3 (server) into separate subnets.
- 2. Route traffic through VM2 (firewall) with NAT.
- 3. Restrict VM3’s web server to ports 80/443.
- 4. Use Linux ACLs to control access to the web directory.

### Virtual Machine Setup

#### VM Specifications

VM	Role	OS	RAM	CPU	Interfaces
VM1	Client	FreeBSD 14	1GB	1	<code>iface1</code> # em0 (LAN)
VM2	Firewall/NAT	FreeBSD 14	1GB	1	<code>iface1</code> # em0, <code>iface2</code> # em1
VM3	Web Server	Linux/FreeBSD	1GB	1	<code>iface2</code> # em1, <code>em1</code> (WAN)

## Network Topology

```
[VM1: 10.0.1.10]
|
├─ (iface1: # em0 10.0.1.1)
|
[VM2: Firewall/NAT]
|
├─ (iface2: # em1 10.0.2.1)
|   └─ [VM3: 10.0.2.10]
|       └─ [External: 192.168.8.150]
```

- **Subnet 1:** `10.0.1.0/24` (VM1 ↔ VM2)
- **Subnet 2:** `10.0.2.0/24` (VM2 ↔ VM3)
- **External:** `192.168.8.0/24` (VM3's internet access)

---

## Task 1: Firewall & NAT Configuration

### Step 1: Assign Static IP Addresses

#### On VM1 (Client):

```
ifconfig iface1 # em0inet 10.0.1.10 netmask 255.255.255.0
route add default 10.0.1.1 # Set VM2 as gateway
```

#### On VM2 (Firewall):

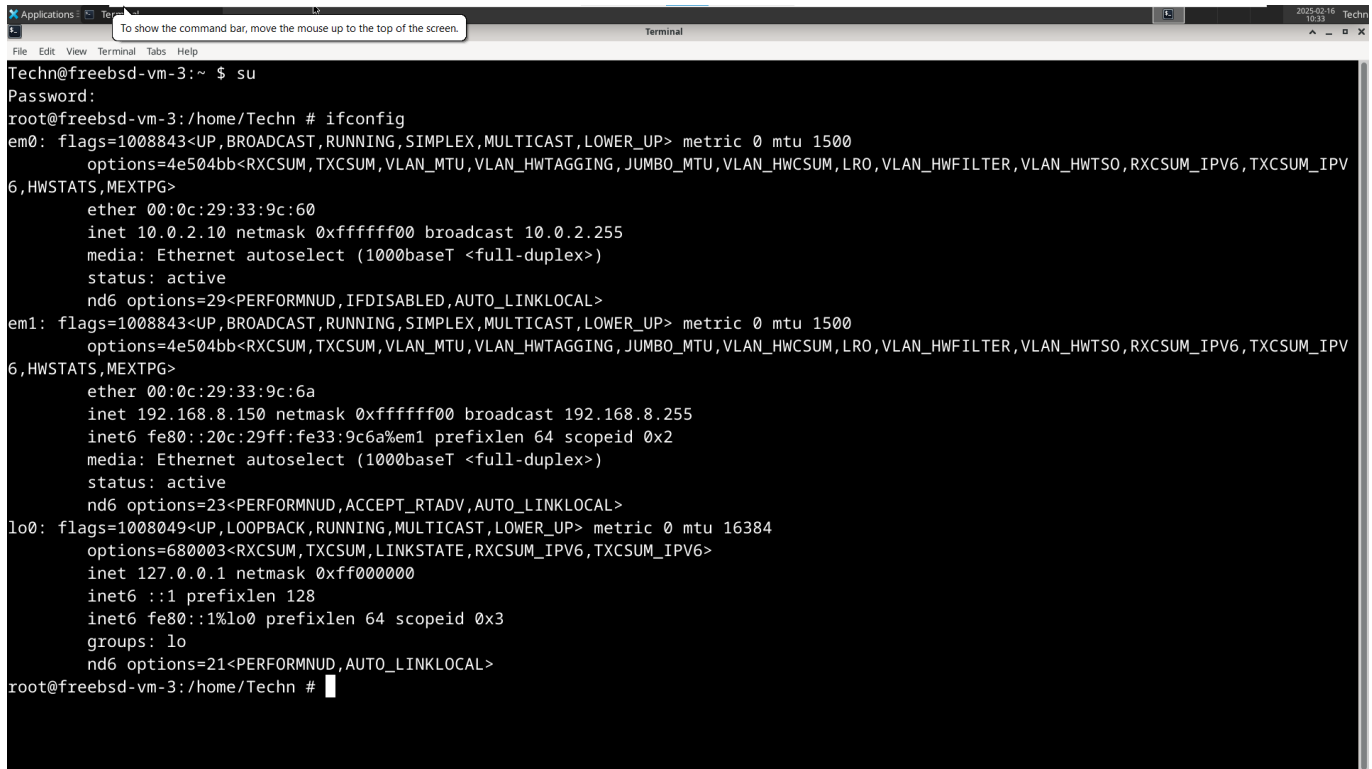
```
ifconfig iface1 # em0inet 10.0.1.1 netmask 255.255.255.0
ifconfig iface2 # em1inet 10.0.2.1 netmask 255.255.255.0
```

#### On VM3 (Server):

```
ifconfig iface2 # em1inet 10.0.2.10 netmask 255.255.255.0
ifconfig em1 inet 192.168.8.150 netmask 255.255.255.0
route add default 192.168.8.1 # External gateway
```

```
technogenius@freebsd-vm-1:/ $ su
Password:
root@freebsd-vm-1:/ # ifconfig
em0: flags=1008843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST,LOWER_UP> metric 0 mtu 1500
    options=4e504bb<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, JUMBO_MTU, VLAN_HWCSUM, LRO, VLAN_HWFILTER, VLAN_HWTSO, RXCSUM_IPV6, TXCSUM_IPV6, HWSTATS, MEXTPG>
    ether 00:0c:29:f8:e9:0e
    inet 10.0.1.10 netmask 0xffffffff broadcast 10.0.1.255
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
    nd6 options=29<PERFORMNUD, IFDISABLED, AUTO_LINKLOCAL>
em1: flags=1008843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST,LOWER_UP> metric 0 mtu 1500
    options=4e504bb<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, JUMBO_MTU, VLAN_HWCSUM, LRO, VLAN_HWFILTER, VLAN_HWTSO, RXCSUM_IPV6, TXCSUM_IPV6, HWSTATS, MEXTPG>
    ether 00:0c:29:f8:e9:18
    inet 192.168.8.148 netmask 0xffffffff broadcast 192.168.8.255
    inet6 fe80::20c:29ff:fe65:2fe6%em1 prefixlen 64 scopeid 0x2
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
    nd6 options=23<PERFORMNUD, ACCEPT_RTADV, AUTO_LINKLOCAL>
lo0: flags=1008049<UP, LOOPBACK, RUNNING, MULTICAST, LOWER_UP> metric 0 mtu 16384
    options=680003<RXCSUM, TXCSUM, LINKSTATE, RXCSUM_IPV6, TXCSUM_IPV6>
    inet 127.0.0.1 netmask 0xff000000
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
    groups: lo
    nd6 options=21<PERFORMNUD, AUTO_LINKLOCAL>
root@freebsd-vm-1:/ #
```

```
Techg@freebsd-vm-2:/ $ su
Password:
root@freebsd-vm-2:/ # ifconfig
em0: flags=1008843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST,LOWER_UP> metric 0 mtu 1500
    options=4e504bb<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, JUMBO_MTU, VLAN_HWCSUM, LRO, VLAN_HWFILTER, VLAN_HWTSO, RXCSUM_IPV6, TXCSUM_IPV6, HWSTATS, MEXTPG>
    ether 00:0c:29:65:2f:d2
    inet 10.0.1.1 netmask 0xffffffff broadcast 10.0.1.255
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
    nd6 options=29<PERFORMNUD, IFDISABLED, AUTO_LINKLOCAL>
em1: flags=1008843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST,LOWER_UP> metric 0 mtu 1500
    options=4e504bb<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, JUMBO_MTU, VLAN_HWCSUM, LRO, VLAN_HWFILTER, VLAN_HWTSO, RXCSUM_IPV6, TXCSUM_IPV6, HWSTATS, MEXTPG>
    ether 00:0c:29:65:2f:dc
    inet 10.0.2.1 netmask 0xffffffff broadcast 10.0.2.255
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
    nd6 options=29<PERFORMNUD, IFDISABLED, AUTO_LINKLOCAL>
em2: flags=1008843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST,LOWER_UP> metric 0 mtu 1500
    options=4e504bb<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, JUMBO_MTU, VLAN_HWCSUM, LRO, VLAN_HWFILTER, VLAN_HWTSO, RXCSUM_IPV6, TXCSUM_IPV6, HWSTATS, MEXTPG>
    ether 00:0c:29:65:2f:e6
    inet 192.168.8.149 netmask 0xffffffff broadcast 192.168.8.255
    inet6 fe80::20c:29ff:fe65:2fe6%em2 prefixlen 64 scopeid 0x3
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
    nd6 options=23<PERFORMNUD, ACCEPT_RTADV, AUTO_LINKLOCAL>
lo0: flags=1008049<UP, LOOPBACK, RUNNING, MULTICAST, LOWER_UP> metric 0 mtu 16384
    options=680003<RXCSUM, TXCSUM, LINKSTATE, RXCSUM_IPV6, TXCSUM_IPV6>
    inet 127.0.0.1 netmask 0xff000000
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x4
    groups: lo
    nd6 options=21<PERFORMNUD, AUTO_LINKLOCAL>
pflog0: flags=1000141<UP, RUNNING, PROMISC, LOWER_UP> metric 0 mtu 33152
    options=0
    groups: pflog
root@freebsd-vm-2:/ #
```



```
Techn@freebsd-vm-3:~ $ su
Password:
root@freebsd-vm-3:/home/Techn # ifconfig
em0: flags=1008843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST,LOWER_UP> metric 0 mtu 1500
    options=4e504bb<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, JUMBO_MTU, VLAN_HWCSUM, LRO, VLAN_HWFILTER, VLAN_HWTSO, RXCSUM_IPV6, TXCSUM_IPV6, HWSTATS, MEXTPG>
    ether 00:0c:29:33:9c:60
    inet 10.0.2.10 netmask 0xffffffff broadcast 10.0.2.255
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
    nd6 options=29<PERFORMNUD, IFDISABLED, AUTO_LINKLOCAL>
em1: flags=1008843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST,LOWER_UP> metric 0 mtu 1500
    options=4e504bb<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, JUMBO_MTU, VLAN_HWCSUM, LRO, VLAN_HWFILTER, VLAN_HWTSO, RXCSUM_IPV6, TXCSUM_IPV6, HWSTATS, MEXTPG>
    ether 00:0c:29:33:9c:6a
    inet 192.168.8.150 netmask 0xffffffff broadcast 192.168.8.255
    inet6 fe80::20c:29ff:fe33:9c6a%em1 prefixlen 64 scopeid 0x2
    media: Ethernet autoselect (1000baseT <full-duplex>)
    status: active
    nd6 options=23<PERFORMNUD, ACCEPT_RTADV, AUTO_LINKLOCAL>
lo0: flags=1008049<UP,LOOPBACK,RUNNING,MULTICAST,LOWER_UP> metric 0 mtu 16384
    options=680003<RXCSUM, TXCSUM, LINKSTATE, RXCSUM_IPV6, TXCSUM_IPV6>
    inet 127.0.0.1 netmask 0xff000000
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
    groups: lo
    nd6 options=21<PERFORMNUD, AUTO_LINKLOCAL>
root@freebsd-vm-3:/home/Techn #
```

## Step 2: Enable IP Forwarding on VM2

Enable packet forwarding to allow VM2 to route traffic:

```
sysctl net.inet.ip.forwarding=1
echo 'net.inet.ip.forwarding=1' >> /etc/sysctl.conf # Persist on reboot
```

### Verify:

```
sysctl net.inet.ip.forwarding # Should return "1"
```

```

^[ (escape) menu ^y search prompt ^k delete line ^p prev li ^g prev page
^o ascii code ^x search ^l undelete line ^n next li ^v next page
^u end of file ^a begin of line ^w delete word ^b back 1 char ^z next word
^t top of text ^e end of line ^r restore word ^f forward char
^c command ^d delete char ^j undelete char ESC-Enter: exit
=====line 1 col 0 lines from top 1 =====
hostname="freebsd-vm-2"
ifconfig_em0="inet 10.0.1.1 netmask 255.255.255.0"
ifconfig_em1="inet 10.0.2.1 netmask 255.255.255.0"
gateway_enable="YES"
ifconfig_em2="DHCP"
ifconfig_em2_ipv6="inet6 accept_rtadv"
sshd_enable="YES"
ntpd_enable="YES"
ntpd_sync_on_start="YES"
moused_nondefault_enable="NO"
# Set dumpdev to "AUTO" to enable crash dumps, "NO" to disable
dumpdev="AUTO"
zfs_enable="YES"
dbus_enable="YES"
sddm_enable="YES"
pf_enable="YES"
pflog_enable="YES"
pflog_logfile="/var/log/pflog"

file "/etc/rc.conf", 19 lines

^t top of text ^e end of line ^r restore word ^f forward char
^c command ^d delete char ^j undelete char ESC-Enter: exit
=====line 1 col 0 lines from top 1 =====
ext_if="em1" # External interface (connected to NAT/Internet)
int_if="em0" # Internal LAN interface
localnet="{ 10.0.1.0/24, 10.0.2.0/24 }" # Use curly brackets for multiple networks

# 1. NAT must come first
nat on $ext_if from $localnet to any -> ($ext_if)

# 2. Allow ICMP (ping)
pass in quick on $int_if inet proto icmp from any to any keep state
pass out quick on $int_if inet proto icmp from any to any keep state
pass in quick on $ext_if inet proto icmp from any to any keep state
pass out quick on $ext_if inet proto icmp from any to any keep state

# 3. Allow all outgoing traffic
pass out on $ext_if from any to any keep state

# 4. Allow internal network traffic
pass in on $int_if from $localnet to any keep state
pass out on $int_if from any to $localnet keep state

block in on $ext_if proto tcp from any to any port 22
block out on $ext_if proto tcp from any to any port 22

root@freebsd-vm-2:/ # sysctl net.inet.ip.forwarding
net.inet.ip.forwarding: 1
root@freebsd-vm-2:/ #

```

### Step 3: Configure PF Firewall Rules

Edit `/etc/pf.conf` on VM2:

```

# Define interfaces
ext_if = "iface2" # em1
int_if = "iface1" # em0
localnet = "{ 10.0.1.0/24, 10.0.2.0/24 }"

# NAT Configuration
nat on $ext_if from $localnet to any -> ($ext_if) # Outbound NAT

```

```
nat on $int_if from any to $ext_if -> ($int_if)    # Inbound NAT

# Traffic Rules
block all    # Default deny

# Allow internal traffic
pass in quick on $int_if from $localnet to any
pass out quick on $ext_if from any to $localnet

# Allow HTTP/HTTPS from external networks
pass in on $ext_if proto tcp from any to any port { 80, 443 }
pass out on $ext_if proto tcp from any to any port { 80, 443 }

# Block SSH (Port 22)
block in quick on $ext_if proto tcp from any to any port 22
```

**Activate Rules:**

```
pfctl -f /etc/pf.conf    # Load rules
pfctl -s rules            # Verify rules (screenshot this!)
```

**Step 4: Test NAT & Connectivity****From VM1:**

```
ping 10.0.2.10    # Should succeed
traceroute 10.0.2.10    # Traffic must route through VM2 (10.0.1.1 → 10.0.2.1)
```

```

root@freebsd-vm-2:/ # ping 10.0.1.10
PING 10.0.1.10 (10.0.1.10): 56 data bytes
64 bytes from 10.0.1.10: icmp_seq=0 ttl=64 time=0.532 ms
64 bytes from 10.0.1.10: icmp_seq=1 ttl=64 time=0.716 ms
64 bytes from 10.0.1.10: icmp_seq=2 ttl=64 time=1.568 ms
64 bytes from 10.0.1.10: icmp_seq=3 ttl=64 time=1.397 ms
64 bytes from 10.0.1.10: icmp_seq=4 ttl=64 time=0.806 ms
^C
--- 10.0.1.10 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.532/1.004/1.568/0.404 ms
root@freebsd-vm-2:/ # ping 10.0.2.10
PING 10.0.2.10 (10.0.2.10): 56 data bytes
64 bytes from 10.0.2.10: icmp_seq=0 ttl=64 time=0.821 ms
64 bytes from 10.0.2.10: icmp_seq=1 ttl=64 time=0.682 ms
64 bytes from 10.0.2.10: icmp_seq=2 ttl=64 time=0.738 ms
64 bytes from 10.0.2.10: icmp_seq=3 ttl=64 time=1.939 ms
64 bytes from 10.0.2.10: icmp_seq=4 ttl=64 time=11.822 ms
64 bytes from 10.0.2.10: icmp_seq=5 ttl=64 time=0.577 ms
64 bytes from 10.0.2.10: icmp_seq=6 ttl=64 time=0.829 ms
^C
--- 10.0.2.10 ping statistics ---
7 packets transmitted, 7 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.577/2.487/11.822/3.835 ms
root@freebsd-vm-2:/ #

root@freebsd-vm-1:/ # ping 10.0.1.1
PING 10.0.1.1 (10.0.1.1): 56 data bytes
64 bytes from 10.0.1.1: icmp_seq=0 ttl=64 time=0.875 ms
64 bytes from 10.0.1.1: icmp_seq=1 ttl=64 time=0.722 ms
64 bytes from 10.0.1.1: icmp_seq=2 ttl=64 time=0.856 ms
64 bytes from 10.0.1.1: icmp_seq=3 ttl=64 time=1.292 ms
^C
--- 10.0.1.1 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.722/0.936/1.292/0.213 ms
root@freebsd-vm-1:/ # ping 10.0.2.10
PING 10.0.2.10 (10.0.2.10): 56 data bytes
64 bytes from 10.0.2.10: icmp_seq=0 ttl=63 time=1.018 ms
64 bytes from 10.0.2.10: icmp_seq=1 ttl=63 time=1.423 ms
64 bytes from 10.0.2.10: icmp_seq=2 ttl=63 time=1.294 ms
64 bytes from 10.0.2.10: icmp_seq=3 ttl=63 time=2.573 ms
^C
--- 10.0.2.10 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.018/1.577/2.573/0.593 ms
root@freebsd-vm-1:/ # traceroute 10.0.2.10
su: traceroute: not found
root@freebsd-vm-1:/ # traceroute 10.0.2.10
traceroute to 10.0.2.10 (10.0.2.10), 64 hops max, 40 byte packets
 1 192.168.8.149 (192.168.8.149) 0.952 ms 0.607 ms 0.628 ms
 2 10.0.2.10 (10.0.2.10) 1.850 ms 1.031 ms 0.838 ms
root@freebsd-vm-1:/ #

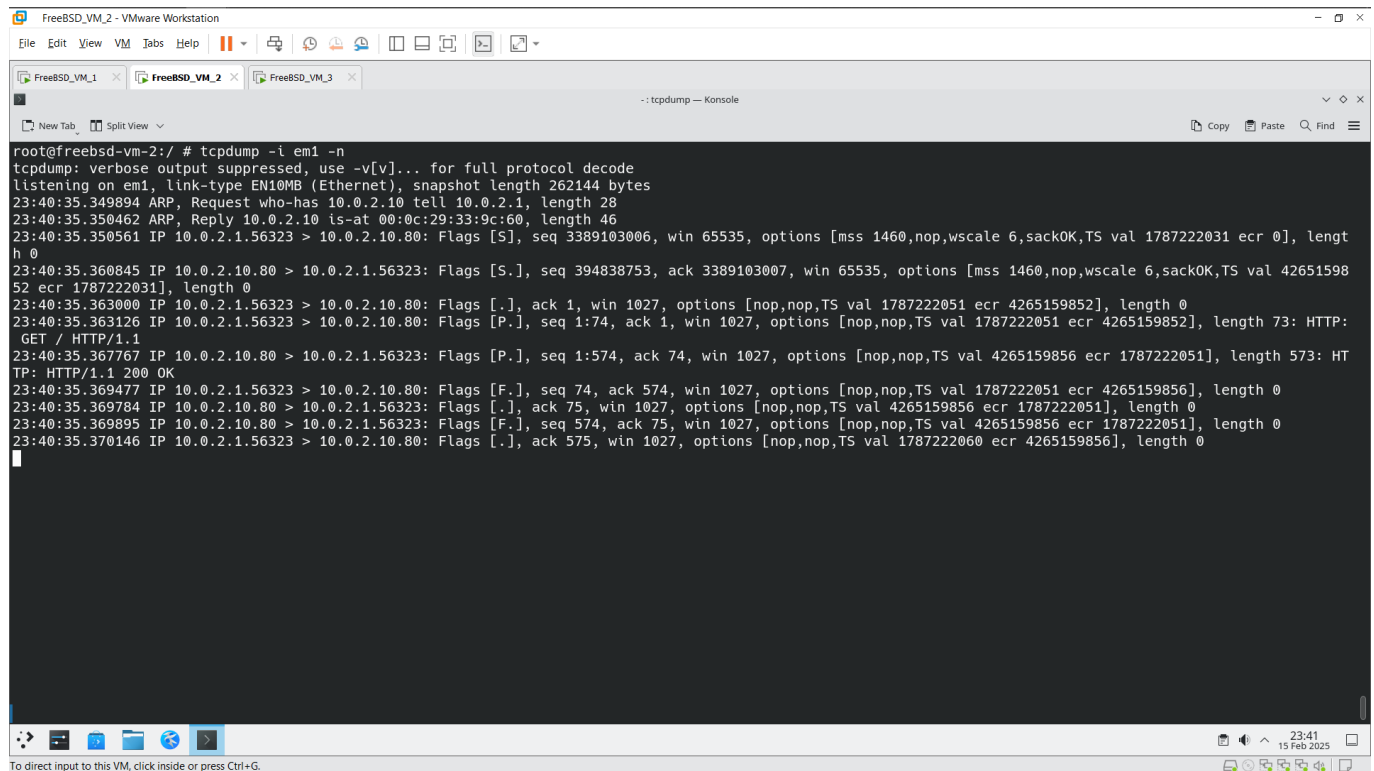
```

## Capture NAT Traffic:

On VM2, run:

```
tcpdump -i iface2 # em1-n port 80 # Observe NAT translation
```

- **Expected Result:** Requests from VM1 (10.0.1.10) appear as coming from VM2 (10.0.2.1).



```
FreeBSD_VM_2 - VMware Workstation
File Edit View VM Tabs Help
FreeBSD_VM_1 x FreeBSD_VM_2 x FreeBSD_VM_3 x
- : tcpdump - Konsole
New Tab Split View
root@freebsd-vm-2:/ # tcpdump -i em1 -n
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on em1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
23:40:35.349894 ARP, Request who-has 10.0.2.10 tell 10.0.2.1, length 28
23:40:35.350462 ARP, Reply 10.0.2.10 is-at 00:0c:29:33:9c:60, length 46
23:40:35.350561 IP 10.0.2.1.56323 > 10.0.2.10.80: Flags [S], seq 3389103006, win 65535, options [mss 1460,nop,wscale 6,sackOK,TS val 1787222031 ecr 0], length 0
23:40:35.360845 IP 10.0.2.10.80 > 10.0.2.1.56323: Flags [S.], seq 394838753, ack 3389103007, win 65535, options [mss 1460,nop,wscale 6,sackOK,TS val 4265159852 ecr 1787222031], length 0
23:40:35.363000 IP 10.0.2.1.56323 > 10.0.2.10.80: Flags [.] , ack 1, win 1027, options [nop,nop,TS val 1787222051 ecr 4265159852], length 0
23:40:35.363126 IP 10.0.2.1.56323 > 10.0.2.10.80: Flags [P.], seq 1:74, ack 1, win 1027, options [nop,nop,TS val 1787222051 ecr 4265159852], length 73: HTTP: GET / HTTP/1.1
23:40:35.367767 IP 10.0.2.10.80 > 10.0.2.1.56323: Flags [P.], seq 1:574, ack 74, win 1027, options [nop,nop,TS val 4265159856 ecr 1787222051], length 573: HTTP: HTTP/1.1 200 OK
23:40:35.369477 IP 10.0.2.1.56323 > 10.0.2.10.80: Flags [F.], seq 74, ack 574, win 1027, options [nop,nop,TS val 1787222051 ecr 4265159856], length 0
23:40:35.369784 IP 10.0.2.10.80 > 10.0.2.1.56323: Flags [.] , ack 75, win 1027, options [nop,nop,TS val 4265159856 ecr 1787222051], length 0
23:40:35.369895 IP 10.0.2.10.80 > 10.0.2.1.56323: Flags [F.], seq 574, ack 75, win 1027, options [nop,nop,TS val 4265159856 ecr 1787222051], length 0
23:40:35.370146 IP 10.0.2.1.56323 > 10.0.2.10.80: Flags [.] , ack 575, win 1027, options [nop,nop,TS val 1787222060 ecr 4265159856], length 0
```

## Task 2: Web Server & ACL Configuration

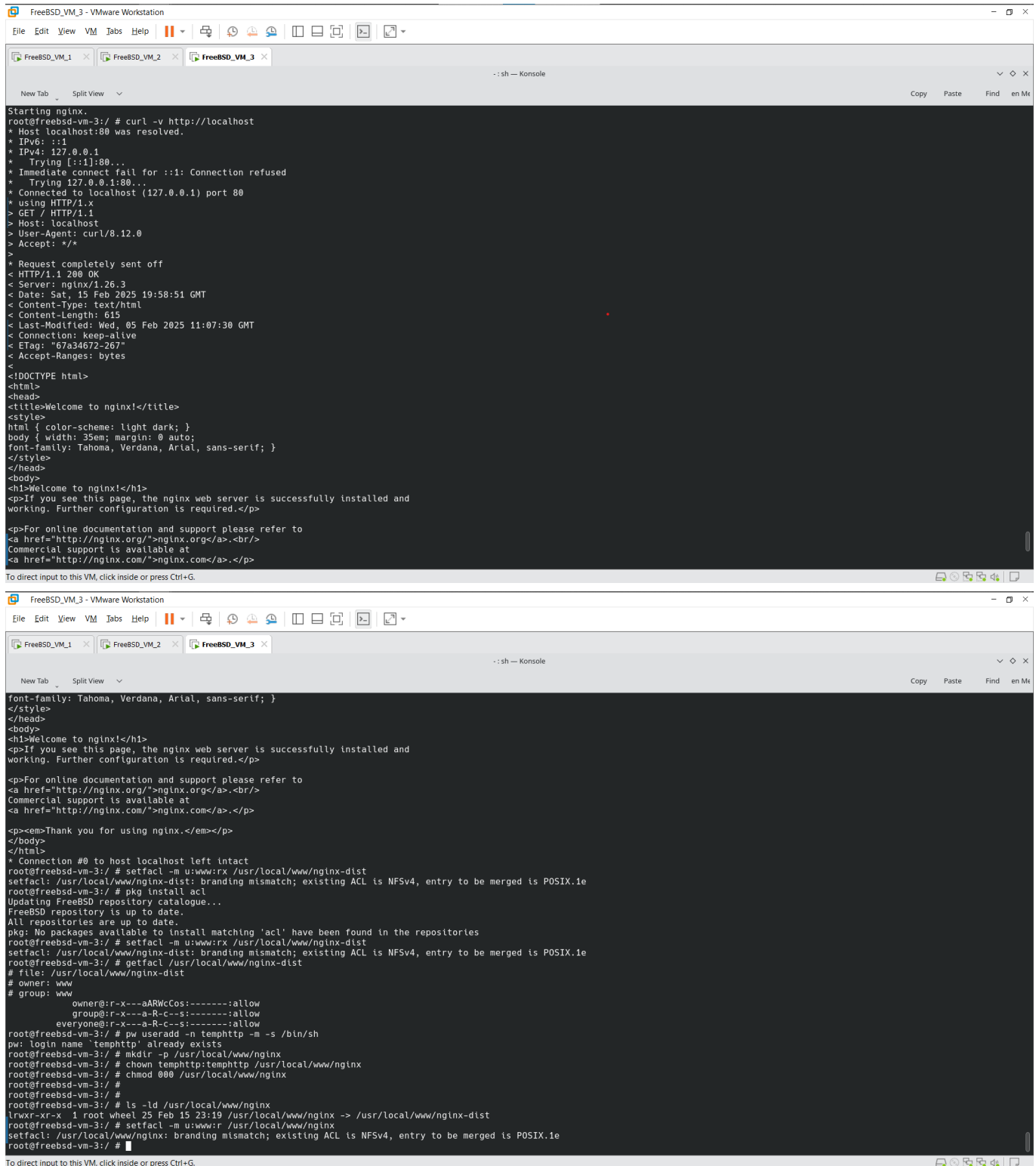
### Step 1: Install & Configure Nginx

#### On VM3:

```
# Install Nginx (Linux example)
sudo apt update && sudo apt install nginx
sudo systemctl start nginx

# Create web directory
sudo mkdir -p /usr/local/www/nginx
```





```

FreeBSD_VM_3 - VMware Workstation
File Edit View VM Tabs Help
FreeBSD_VM_1 x FreeBSD_VM_2 x FreeBSD_VM_3 x
-- sh -- Konsole
New Tab Split View
Copy Paste Find en Me

Starting nginx.
root@freebsd-vm-3:/ # curl -v http://localhost
* Host localhost:80 was resolved.
* IPv6: ::1
* IPv4: 127.0.0.1
* Trying [::1]:80...
* Immediate connect fail for ::1: Connection refused
* Trying 127.0.0.1:80...
* Connected to localhost (127.0.0.1) port 80
* using HTTP/1.x
> GET / HTTP/1.1
> Host: localhost
> User-Agent: curl/8.12.0
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Server: nginx/1.26.3
< Date: Sat, 15 Feb 2025 19:58:51 GMT
< Content-Type: text/html
< Content-Length: 615
< Last-Modified: Wed, 05 Feb 2025 11:07:30 GMT
< Connection: keep-alive
< ETag: "67a34672-267"
< Accept-Ranges: bytes
<
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
* Connection #0 to host localhost left intact
root@freebsd-vm-3:/ # setfacl -m u:www:rx /usr/local/www/nginx-dist
setfacl: /usr/local/www/nginx-dist: branding mismatch; existing ACL is NFSv4, entry to be merged is POSIX.1e
root@freebsd-vm-3:/ # pkg install acl
Updating FreeBSD repository catalogue...
FreeBSD repository is up to date.
All repositories are up to date.
pkg: No packages available to install matching 'acl' have been found in the repositories
root@freebsd-vm-3:/ # setfacl -m u:www:rx /usr/local/www/nginx-dist
setfacl: /usr/local/www/nginx-dist: branding mismatch; existing ACL is NFSv4, entry to be merged is POSIX.1e
root@freebsd-vm-3:/ # getfacl /usr/local/www/nginx-dist
# file: /usr/local/www/nginx-dist
# owner: www
# group: www
owner::r-x---aARwCcos:-----:allow
group::r-x---a-R-c--s:-----:allow
everyone::r-x---a-R-c--s:-----:allow
root@freebsd-vm-3:/ # pw useradd -n templttp -m -s /bin/sh
pw: login name 'templttp' already exists
root@freebsd-vm-3:/ # mkdir -p /usr/local/www/nginx
root@freebsd-vm-3:/ # chown templttp:templttp /usr/local/www/nginx
root@freebsd-vm-3:/ # chmod 0700 /usr/local/www/nginx
root@freebsd-vm-3:/ # ls -ld /usr/local/www/nginx
lrwxr-xr-x 1 root wheel 25 Feb 15 23:10 /usr/local/www/nginx -> /usr/local/www/nginx-dist
root@freebsd-vm-3:/ # setfacl -m u:www:r /usr/local/www/nginx
setfacl: /usr/local/www/nginx: branding mismatch; existing ACL is NFSv4, entry to be merged is POSIX.1e
root@freebsd-vm-3:/ #
To direct input to this VM, click inside or press Ctrl+G.

```

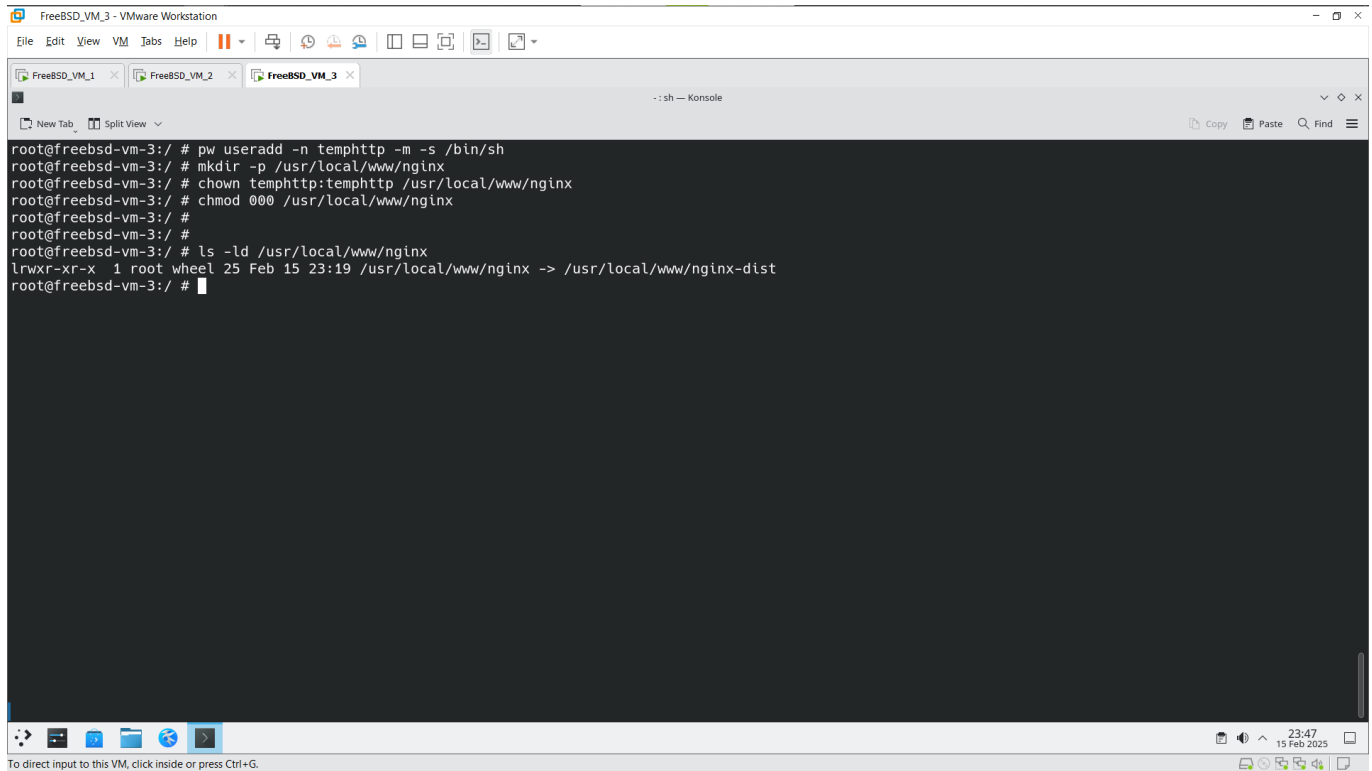
## Step 2: Set File Permissions with **setuid**

### Create User **templttp**:

```

sudo useradd templttp
sudo chown -R templttp:templttp /usr/local/www/nginx
sudo chmod 0700 /usr/local/www/nginx # Deny all except owner

```



```
FreeBSD_VM_3 - VMware Workstation
File Edit View VM Tabs Help
FreeBSD_VM_1 x FreeBSD_VM_2 x FreeBSD_VM_3 x
-- sh -- Konsole
New Tab Split View
root@freebsd-vm-3:/ # pw useradd -n temphttp -m -s /bin/sh
root@freebsd-vm-3:/ # mkdir -p /usr/local/www/nginx
root@freebsd-vm-3:/ # chown temphttp:temphttp /usr/local/www/nginx
root@freebsd-vm-3:/ # chmod 000 /usr/local/www/nginx
root@freebsd-vm-3:/ #
root@freebsd-vm-3:/ #
root@freebsd-vm-3:/ # ls -ld /usr/local/www/nginx
lrwxr-xr-x 1 root wheel 25 Feb 15 23:19 /usr/local/www/nginx -> /usr/local/www/nginx-dist
root@freebsd-vm-3:/ #
```

### Attempt Access via Nginx:

```
curl http://10.0.2.10/nginx # Should fail (403 Forbidden)
```

### Step 3: Apply Linux ACLs

Grant read access to the **www-data** user/group (Nginx):

```
sudo setfacl -m u:www-data:r-x /usr/local/www/nginx
sudo getfacl /usr/local/www/nginx # Verify ACLs (screenshot this!)
```

### Retest Access:

```
curl http://10.0.2.10/nginx # Should now succeed
```

---

## Validation & Screenshots

Include the following in your report:

1. **VM2's Routing Table:** `netstat -rn`
  2. **PF Rules:** `pfctl -s rules`
  3. **NAT Verification:** `tcpdump` output showing translated IPs.
  4. **ACL Configuration:** `getfacl /usr/local/www/nginx`
-

# Troubleshooting

Issue	Solution
PF not loading	<code>kldload pf; service pf restart</code>
VM3 cannot reach the internet	Verify default route: <code>route -n get default</code>
Connection timeout on port 80	Check firewall rules: <code>pfctl -s rules</code>

## References

- 1. [FreeBSD PF Handbook](#)
- 2. [Linux ACL Guide](#)