IPTABLES Hands-On Lab

CSE468/598 Computer Network Security

This lab will guide you through the basic configuration of iptables rules based on network as shown in fig.1.

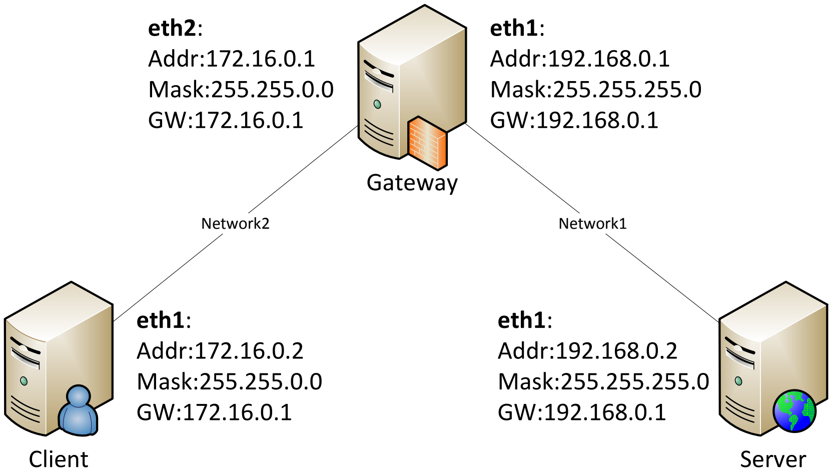

Figure 1: Network Topology

1 Initial Setup to Allow SSH

1.1 Create rc.firewall File

Connect to your Gateway VM via SSH. After you get sudo privilege, type:

```
vim rc.firewall
```

1.2 Create File Content

Switch to insert mode by tapping i key. Insert contents:

```
#!/bin/bash
#####################################################
# Initial Setup (Do NOT change!)
#####################################################

LAN_0_IFACE="eth0"
```

```
LAN_1_IP="192.168.0.1"
LAN_1_IP_RANGE="192.168.0.0/24"
LAN_1_BCAST_ADDRESS="192.168.0.255"
LAN_1_IFACE="eth1"

LAN_2_IP="172.16.0.1"
LAN_2_IP_RANGE="172.16.0.0/16"
LAN_2_BCAST_ADDRESS="172.16.0.255"
LAN_2_IFACE="eth2"

WEB_SERVER_IP="192.168.0.2"

LO_IFACE="lo"
LO_IP="127.0.0.1"

echo "1" > /proc/sys/net/ipv4/ip_forward

IPTABLES="/sbin/iptables"

$IPTABLES -F
$IPTABLES -F -t nat

$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP

$IPTABLES -A INPUT -i $LO_IFACE -j ACCEPT
$IPTABLES -A OUTPUT -o $LO_IFACE -j ACCEPT

$IPTABLES -A INPUT -p tcp --sport 80 -j ACCEPT
$IPTABLES -A OUTPUT -p tcp --dport 80 -j ACCEPT

$IPTABLES -A INPUT -p TCP --dport 22 -j ACCEPT
$IPTABLES -A OUTPUT -p TCP --sport 22 -j ACCEPT
```

Warning: Do not change this part in the future or you may lose SSH connection to the VM. The rules for port 80 also allow `apt-get` on the VM.

1.3 Apply Firewall Rules

Save the file, and exit `vim` by pressing `ESC` then type `:wq`. After that, type command in shell:

```
chmod a+x rc.firewall
./rc.firewall
```

The initial iptables rules only allow incoming and outgoing traffics on port 22 (SSH).
Test: Open a VNC connection to your Gateway VM, see if it connects.

2 Allow VNC Access to VM

Reopen the rc.firewall file by typing:

```
vim rc.firewall
```

Then, append the following lines by the end:

```
#####################################################
# Allow VNC
#####################################################

$IPTABLES -A INPUT -p TCP --dport 5901 -j ACCEPT
$IPTABLES -A OUTPUT -p TCP --sport 5901 -j ACCEPT
```

Save and apply rules.
The first line will allow incoming traffic to local port 5901. The second line will allow outgoing traffic from local port 5901.
Test: Open a VNC connection to your Gateway VM, see if it connects.

3 Allow DNS Lookup

DNS uses UDP protocol for domain name lookup on port 53. The current iptables rules disallow DNS traffics.
Test: Open a SSH connection to Server or Client VM, then do `nslookup www`, any response?
Append the following lines to rc.firewall:

```
#####################################################
# Allow DNS
#####################################################

$IPTABLES -A INPUT -p udp --dport 53 -j ACCEPT
$IPTABLES -A OUTPUT -p udp --sport 53 -j ACCEPT
```

Save and apply rules.
Test: After applying the rules, try `nslookup www` again.

4 Allow Ping on Gateway

The Internet Control Message Protocol (ICMP) has many messages that are identified by a "type" field. You need to use 0 and 8 ICMP code types. Eight (8) is for echo-request. Zero (0) is for echo-reply. Ping is disabled by iptales rules for now.
Test: Try to ping Server from Gateway, and ping Gateway from Server. Will they work?

4.1 Allow Incoming Ping Request on Gateway

Append the following rules.

```
######################################################
# Allow Incoming Ping
######################################################

$IPTABLES -A INPUT -p ICMP -s 0/0 --icmp-type 8 -j ACCEPT
$IPTABLES -A OUTPUT -p icmp --icmp-type 0 -j ACCEPT
```

Test: After applying the rules, try to ping Server from Gateway, and ping Gateway from Server. Which one will (not) work?

4.2 Allow Outgoing Ping Request on Gateway

```
######################################################
# Allow outgoing Ping
######################################################

$IPTABLES -A INPUT -p ICMP -s 0/0 --icmp-type 0 -j ACCEPT
$IPTABLES -A OUTPUT -p ICMP --icmp-type 8 -j ACCEPT
```

Test: After applying the rules, try to ping Server from Gateway, and ping Gateway from Server.

5 Allow Ping between Server & Client

Test: Can you ping Client's IP/DomainName from Server VM? Can you do it from Client to Server?
According to fig.1, to allow Server to ping Client, ICMP packets must be forwarded correctly on Gateway:
- ICMP8 needs to be forwarded from Server side to Client side.
- ICMP0 needs to be forwarded from Client side to Server side.

5.1 Allow Server to Ping Client

Append the following lines to rc.firewall:

```
######################################################
# Allow Server to Ping Client
######################################################

$IPTABLES -A FORWARD -p icmp --icmp-type 8 -i $LAN_1_IFACE -o
    $LAN_2_IFACE -j ACCEPT
$IPTABLES -A FORWARD -p icmp --icmp-type 0 -i $LAN_2_IFACE -o
    $LAN_1_IFACE -j ACCEPT
```

These lines will allow ICMP8 to be forwarded from eth1 (Server side) to eth2 (Client side), then allow ICMP0 to be forwarded from eth2 to eth1.
Test: Try to ping Client VM from Server VM.

5.2 Allow Client to Ping Server

Append the following lines to rc.firewall:

```
######################################################
# Allow Client to Ping Server
######################################################

$IPTABLES -A FORWARD -p icmp --icmp-type 8 -i $LAN_2_IFACE -o
    $LAN_1_IFACE -j ACCEPT
$IPTABLES -A FORWARD -p icmp --icmp-type 0 -i $LAN_1_IFACE -o
    $LAN_2_IFACE -j ACCEPT
```

These lines will allow ICMP8 to be forwarded from eth2 (Client side) to eth1 (Server side), then allow ICMP0 to be forwarded from eth1 to eth2.
Test: Try to ping Server VM from Client VM.

6 Web Access from Client to Server via Gateway

There are 2 ways of allowing web access from Client to Server:
• Use Gateway to forward web request from Client to Server, then forward Server response to Client.
• Use Gateway as a NAT, hiding Server from Client and only publishing its port 80 to Client. Internally routing all web request to Server.
Test: VNC to Server and Client, open Firefox on Client, can you access Server's website?

6.1 Use FORWARD to Allow Web Access

Append the rules.

```
######################################################
# Use FORWARD to Allow Web Access
######################################################

$IPTABLES -A FORWARD -p tcp -i $LAN_2_IFACE -o $LAN_1_IFACE --dport 80
     -j ACCEPT
$IPTABLES -A FORWARD -p tcp -i $LAN_1_IFACE -o $LAN_2_IFACE --sport 80
     -j ACCEPT
```

Save and apply rules.
Test: In Client's Firefox, type Server's address. View the results.

6.2 Use NAT to Allow Web Access

Append the rules.

```
#####################################################
# Use FORWARD to Allow Web Access
#####################################################

$IPTABLES -t nat -A PREROUTING -p tcp -i $LAN_2_IFACE --dport 80 -j
    DNAT --to-destination $WEB_SERVER_IP:80
$IPTABLES -t nat -A POSTROUTING -p tcp -d $WEB_SERVER_IP --dport 80 -j
     MASQUERADE
```

Save and apply rules.
Test: In Client's Firefox, instead of typing Server's address, type Gateway's address in the URL bar. View the results.