Segurança em Redes de Comunicações

Introduction to Firewall Deployment

iptables (nf_tables)

Linux Firewall Deployment

After the first boot, check network interface names: `ip addr`

To change the keyboard layout: `loadkeys pt-latin1`

`loadkeys us`

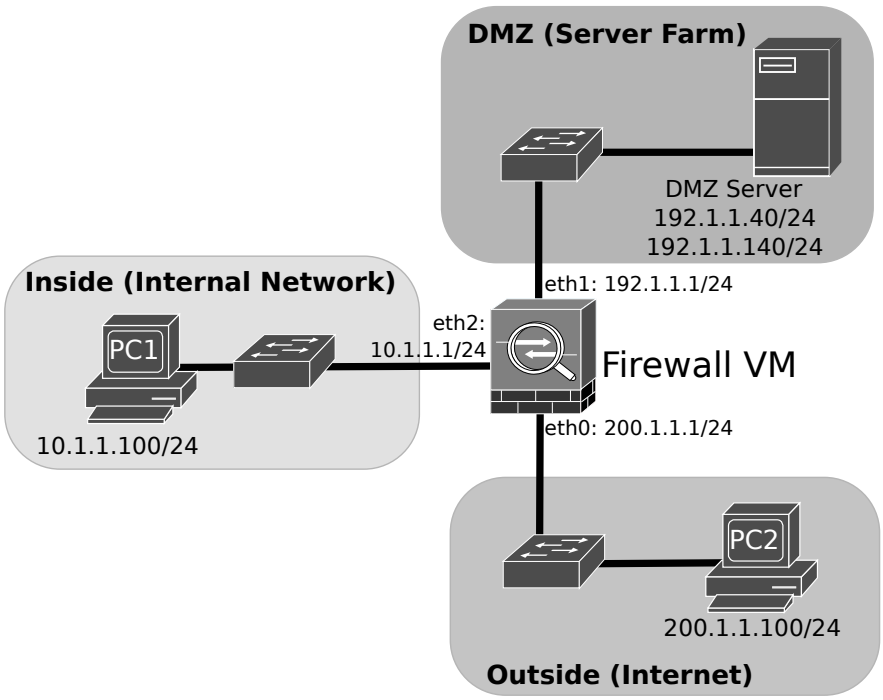
The Linux device should have the iptables and conntrackd packages installed.

For QEMU GNS3 template use the following parameters: RAM: 256M, Console type: telnet (or none with auto start console checked), HD Disk interface: ide, Network Adapters: 6, Network Name format: eth{0}.

For VirtualBox GNS3 template use the following parameters: RAM: 256M, Console type: telnet (or none with auto start console checked), Network Adapters: 6, Network Name format: eth{0}, check Network option “Allow GNS3 to use any ... adapter”.

iptables manual: https://linux.die.net/man/8/iptables

1. Configure the network depicted in the following figure using GNS3 with PC1 and PC2 as VPCS, the DMZ server as a VM Linux server (or two VPCS), and the Firewall VM is a Linux device with iptables and conntrackd installed. Configure PCs and Server addresses and gateways.



2. Configure the firewall IPv4 addresses using the following commands.

Enter into root mode:

```
# sudo su
```

Configure the interfaces IPv4 addresses, commit the configurations and exit the configuration mode:

```
# ip addr add 10.1.1.1/24 dev eth2
# ip addr add 192.1.1.1/24 dev eth1
# ip addr add 200.1.1.1/24 dev eth0
```

Enable IPv4 routing, by uncommenting the line

```
net.ipv4.ip_forward=1
```

in file /etc/sysctl.conf, and running the command:

```
# sysctl -p
```

>> Verify the configured addresses with: `# ip addr`

>> Test the full connectivity between all network equipment.

3. Configure the firewall NAT/PAT mechanisms. Assume that the network will use the IPv4 public address 192.1.0.1 to 192.1.0.10:

```
# iptables -t nat -A POSTROUTING -j SNAT -o eth0 -s 10.1.1.0/24 --to 192.1.0.1-192.1.0.10
```

Verify the applied rules:

```
# iptables -t nat -L -v
```

>> Start a capture on the link between the firewall (eth0) and the OUTSIDE switch. Ping PC2 from PC1 and verify the correct translation of the source IPv4 addresses.

>> Use the following command to verify the active NAT translations:

```
# conntrack -L -n
```

Notes:

Save iptables rules use:

```
# iptables-save > iptables.rules
```

To restore iptables rules use:

```
# iptables-restore < iptables.rules
```

To create a new chain use option: `-N <chain>`.

To delete a clompete chain use option: `-X <chain>`. Must not be referenced in other chains.

To Append a rule to the end use option `-A <chain>`.

To Insert a rule in line x, use option: `-I <chain> x`.

To delete an entry in line x, use option: `-D <chain> x`.

Examples:

```
# iptables -N ZONE-OUTSIDE
# iptables -X ZONE-OUTSIDE
# iptables -A ZONE-OUTSIDE ...
(insert in line 10) # iptables -I ZONE-OUTSIDE 10 ...
(delete line 10) # iptables -D ZONE-OUTSIDE 10 ...\
```

4. Define the network security zones:

```
# iptables -N ZONE-INSIDE
# iptables -A FORWARD -o eth2 -j ZONE-INSIDE
# iptables -N ZONE-DMZ
# iptables -A FORWARD -o eth1 -j ZONE-DMZ
# iptables -N ZONE-OUTSIDE
# iptables -A FORWARD -o eth0 -j ZONE-OUTSIDE
```

Define default policy, do nothing (RETURN) and forward packet if it originates in the same zone, drop it (DROP) otherwise:

```
#iptables -A ZONE-INSIDE -i eth2 -j RETURN
#iptables -A ZONE-INSIDE -j DROP
#iptables -A ZONE-DMZ -i eth1 -j RETURN
#iptables -A ZONE-DMZ -j DROP
#iptables -A ZONE-OUTSIDE -i eth0 -j RETURN
#iptables -A ZONE-OUTSIDE -j DROP
```

To verify the zone policies, firewall rules and statistics use the following commands:

```
# iptables -L -v
# iptables -L -v –line-numbers
# iptables -S
```

>> Test the full (or lack of) connectivity between all network equipment (and IPv4 addresses).

5. Create and configure the firewalls chains and rules to allow the Inside equipment to ping all Outside devices:

```
# iptables -N FROM-INSIDE-TO-OUTSIDE
# iptables -A FROM-INSIDE-TO-OUTSIDE -p icmp --icmp-type echo-request -j RETURN
# iptables -A FROM-INSIDE-TO-OUTSIDE -j DROP

# iptables -N TO-INSIDE
# iptables -A TO-INSIDE -m state --state RELATED,ESTABLISHED -j RETURN
# iptables -A TO-INSIDE -j DROP

# iptables -I ZONE-OUTSIDE 2 -i eth2 -j FROM-INSIDE-TO-OUTSIDE
# iptables -I ZONE-OUTSIDE 3 -i eth2 -j RETURN

# iptables -I ZONE-INSIDE 2 -j TO-INSIDE
# iptables -I ZONE-INSIDE 3 -j RETURN
```

To verify the zone policies, firewall rules and statistics use the following commands:

```
# iptables -L -v
# iptables -L -v --line-numbers
```

>> Test the implemented rules, pinging the Server and PC2 from PC1.

6. Configure the firewalls chains and rules to allow the Inside devices to ping all DMZ (network 192.1.1.0/24) devices:

```
# iptables -N FROM-INSIDE-TO-DMZ
# iptables -A FROM-INSIDE-TO-DMZ -d 192.1.1.0/24 -p icmp --icmp-type echo-request -j RETURN
# iptables -A FROM-INSIDE-TO-DMZ -j DROP

# iptables -I ZONE-DMZ 2 -i eth2 -j FROM-INSIDE-TO-DMZ
# iptables -I ZONE-DMZ 3 -i eth2 -j RETURN
```

Note: The chain TO-INSIDE was already defined before.

To verify the zone policies, firewall rules and statistics use the following commands:

```
# iptables -L -v
# iptables -L -v --line-numbers
```

>> Test the implemented rules, pinging from PC1 the Server (192.1.1.40 and 192.1.1.140).

7. Configure the firewalls chains and rules to allow the Outside devices to ping the DMZ Server (only IP address 192.1.1.40):

```
# iptables -N FROM-OUTSIDE-TO-DMZ
# iptables -A FROM-OUTSIDE-TO-DMZ -d 192.1.1.40 -p icmp --icmp-type echo-request -j RETURN
# iptables -A FROM-OUTSIDE-TO-DMZ -j DROP

# iptables -N FROM-DMZ-TO-OUTSIDE
# iptables -A FROM-DMZ-TO-OUTSIDE -m state --state RELATED,ESTABLISHED -j RETURN
# iptables -A FROM-DMZ-TO-OUTSIDE -j DROP

# iptables -I ZONE-DMZ 2 -i eth0 -j FROM-OUTSIDE-TO-DMZ
# iptables -I ZONE-DMZ 3 -i eth0 -j RETURN

# iptables -I ZONE-OUTSIDE 2 -i eth1 -j FROM-DMZ-TO-OUTSIDE
# iptables -I ZONE-OUTSIDE 3 -i eth1 -j RETURN
```

To verify the zone policies, firewall rules and statistics use the following commands:

```
# iptables -L -v
# iptables -L -v --line-numbers
```

>> Test the implemented rules, pinging from the PC2 the Server (192.1.1.40 and 192.1.1.140).

8. Add a new rule to the chain FROM-OUTSIDE-TO-DMZ to allow the Outside devices to send UDP packets to port 8080 to the DMZ Server (only IP address 192.1.1.140):

```
# iptables -I FROM-OUTSIDE-TO-DMZ 2 -d 192.1.1.140 -p udp -m udp --dport 8080 -j RETURN
```

To verify the zone policies, firewall rules and statistics use the following commands:

```
# iptables -L -v
# iptables -L -v --line-numbers
```

>> Test the implemented rules, pinging with UDP to port 8080 from the PC2 the Server (192.1.1.40 and 192.1.1.140). Use the VPCS command: `ping 192.1.1.140 -P 17 -p 8080`

>> Test the connectivity with the other server IPv4 address, with other UDP ports and test also TCP connections. For TCP pings from the VPCS use command: `ping 192.1.1.140 -P 6 -p 8080`