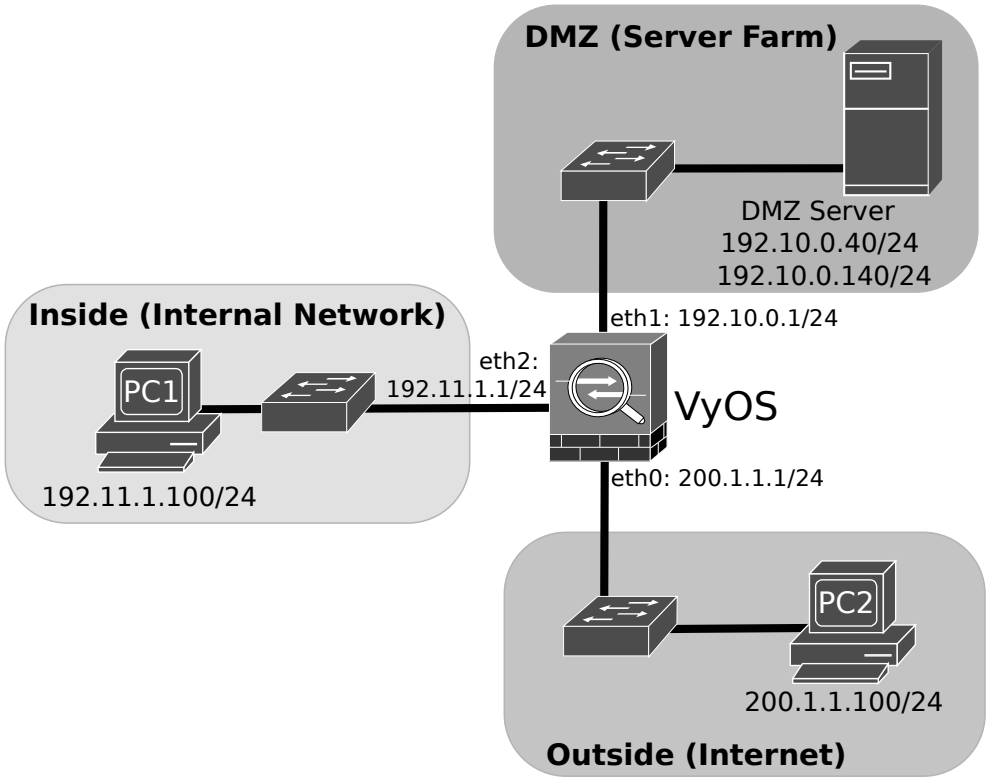
Laboratory Guide

VyOS/Firewalls Deployment

Linux (VyOS) Firewall Deployment

1. Configure the network depicted in the following figure using GNS3. Configure PCs and Server addresses and gateways.



2. Configure the firewall using the following commands. To enter into configuration mode:

```
configure
```

To configure the interfaces IP addresses:

```
set interfaces ethernet eth0 address 200.1.1.1/24
set interfaces ethernet eth1 address 192.10.0.1/24
set interfaces ethernet eth2 address 192.11.1.1/24
commit
```

Test the full connectivity between all network equipments. Note: the firewall has a blank configuration, so by default it allows all traffic and performs all routing mechanisms.

3. Start by defining the network security zones:

```
set zone-policy zone INSIDE description "Inside (Internal Network)"
set zone-policy zone INSIDE interface eth2
set zone-policy zone DMZ description "DMZ (Server Farm)"
set zone-policy zone DMZ interface eth1
set zone-policy zone OUTSIDE description "Outside (Internet)"
set zone-policy zone OUTSIDE interface eth0
commit
```

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

```
show zone-policy
show firewall
```

Test the full (or lack of) connectivity between all network equipments (and IP addresses).

4. Configure the firewalls rules to allow the Inside equipments to ping all Outside equipments:

```
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 description "Accept ICMP Echo Request"
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 action accept
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 protocol icmp
set firewall name FROM-INSIDE-TO-OUTSIDE rule 10 icmp type 8
set firewall name TO-INSIDE rule 10 description "Accept Established-Related Connections"
set firewall name TO-INSIDE rule 10 action accept
set firewall name TO-INSIDE rule 10 state established enable
set firewall name TO-INSIDE rule 10 state related enable
set zone-policy zone INSIDE from OUTSIDE firewall name TO-INSIDE
set zone-policy zone OUTSIDE from INSIDE firewall name FROM-INSIDE-TO-OUTSIDE
```

Verify the correct configuration:

```
show zone-policy
show firewall
```

Commit the new configurations and re-verify the configurations:

```
commit
```

Test the implemented rules, pinging from PC1 the Internet Router.

5. Configure the firewalls rules to allow the Inside equipment to ping all DMZ (network 192.10.0.0/24) equipment:

```
set firewall name FROM-INSIDE-TO-DMZ rule 10 description "Accept ICMP Echo Request"
set firewall name FROM-INSIDE-TO-DMZ rule 10 action accept
set firewall name FROM-INSIDE-TO-DMZ rule 10 protocol icmp
set firewall name FROM-INSIDE-TO-DMZ rule 10 icmp type 8
set firewall name FROM-INSIDE-TO-DMZ rule 10 destination address 192.10.0.0/24
set zone-policy zone INSIDE from DMZ firewall name TO-INSIDE
set zone-policy zone DMZ from INSIDE firewall name FROM-INSIDE-TO-DMZ
```

Verify the correct configuration:

```
show zone-policy
show firewall
```

Commit the new configurations and re-verify the configurations:

```
commit
```

Test the implemented rules, pinging from PC1 the DMZ Server (192.10.0.40 and 192.10.0.41).

6. Configure the firewalls rules to allow the Outside equipment to ping the DMZ Server (IP address 192.10.0.40) equipment:

```
set firewall name FROM-OUTSIDE-TO-DMZ rule 10 description "Accept ICMP Echo Request"
set firewall name FROM-OUTSIDE-TO-DMZ rule 10 action accept
set firewall name FROM-OUTSIDE-TO-DMZ rule 10 protocol icmp
set firewall name FROM-OUTSIDE-TO-DMZ rule 10 icmp type 8
set firewall name FROM-OUTSIDE-TO-DMZ rule 10 destination address 192.10.0.40
set firewall name FROM-DMZ-TO-OUTSIDE rule 10 description "Accept ICMP Echo Request"
set firewall name FROM-DMZ-TO-OUTSIDE rule 10 action accept
set firewall name FROM-DMZ-TO-OUTSIDE rule 10 state established enable
set firewall name FROM-DMZ-TO-OUTSIDE rule 10 state related enable
set zone-policy zone OUTSIDE from DMZ firewall name FROM-DMZ-TO-OUTSIDE
set zone-policy zone DMZ from OUTSIDE firewall name FROM-OUTSIDE-TO-DMZ
```

Verify the correct configuration:

```
show zone-policy
show firewall
```

Commit the new configurations and re-verify the configurations:

```
commit
```

Test the implemented rules, pinging from the PC2 the DMZ Server (192.10.0.40 and 192.10.0.140).

7. Exit the firewall configuration mode (`exit`) and analyze the underlying IPTables Chains (`iptables -L`) that were created.