**2. Firewalls/DMZ**

In this lab you will configure the firewall service on a gateway router in a sample core configuration file. Download the file [ITO4137\_Module\_6\_Lab\_Task-1.imn](https://learning.monash.edu/mod/resource/view.php?id=3529409&section=11) and save it in the shared folder on the host machine (your laptop or PC). Open core and from the file menu open the downloaded core configuration from the shared folder in the VM (under /media folder starting with sf\_).

The node phoenix is the gateway router with its eth0 connected to the internal network of the organisation, the eth1 interface to the Demilitarised Zone (DMZ), and the eth2 connected to the internet. The firewall will protect the two networks: internal and DMZ against unauthorised traffic by inspecting the packets that pass through the router (or firewall).

The DMZ network is part of the organisation’s network where servers that provide services to the internet will be located. The DMZ network is separated from the internal network (or intranet) since it is possible for these servers to be compromised by an attacker and then be used to attack the rest of the network hence the firewall protects the internal network against both of the internet and DMZ. Check out [DMZ (computing)](https://en.wikipedia.org/wiki/DMZ_%28computing%29) (Wikipedia 2020) for more information.

**Firewall policy**

Open the services configuration for the firewall router (node phoenix) and select the tool icon next to the Firewall setting (in the Security column). This will open a dialogue that lets you enter firewall rules based on the iptables tool (man iptables).

Enter the following as the basis for your firewall rules:

#!/bin/sh  
# Set default policy: drop all packets   
# This means that the firewall blocks all traffic for the identified chain  
iptables -P INPUT DROP  
iptables -P OUTPUT DROP  
iptables -P FORWARD DROP

After setting up this firewall, you should not be able to reach any computer inside the DMZ or the Internal network. In fact, no traffic will be allowed to pass through, be sent from, or be delivered to the firewall.

The iptables commands use different chains for different tasks. The **INPUT** chain is for packets that have the firewall router as its destination. The **OUTPUT** chain is for packets that software on the firewall router wants to send somewhere else. The **FORWARD** chain controls the packets for which the firewall router performs routing. When a packet is passing through the firewall, entering from one interface, routed by the firewall, and then exiting from another interface, then the packet is checked against the **FORWARD** chain rules.

**External to DMZ**

Now that the system is secure (all traffic is blocked), we can start allowing traffic for individual services to pass through. We will start by allowing the servers in DMZ to be accessible to external hosts.

For the configuration to persist in core we need to use the GUI; however, as we are learning the iptables rules, it would be better to try the commands while the core configuration is running. This way we can test the rules and make sure the rules correctly match the intended traffic and then we can add the rules to the configuration via GUI.

: Keep a copy of the tested and correct rules in a text file so that you can add them to the Firewall service through GUI.

To test the policy we just configured, start the emulation and open a terminal on helios and try to visit the web server in DMZ:

 lynx 10.1.1.71

**Incoming rule**

Now we add a rule that allows TCP packets for port 80 to pass from outside to web server in DMZ. Open a terminal on phoenix and enter the following command:

iptables -A FORWARD -i eth2 -o eth1 -d 10.1.1.71 -p tcp --dport 80 -j ACCEPT

The command line arguments specify the criteria for a packet to match against and the policy to apply if the packet matches the criteria:

* -A FORWARD append the rule to the FORWARD chain.
* -i eth2 input interface must match eth2 (the interface the packet came in) when omitted will match any interface.
* -o eth1 output interface must match eth1 (the interface the packet is going out) when omitted will match any interface
* -d 10.1.1.70 destination IP address must match the specified address or address range (with subnet mask)
* -p tcp the protocol must match TCP
* --dport 80 the destination port must match 80, only if TCP or UDP is specified as protocol
* -j ACCEPT jump to ACCEPT target, the target policy to apply to the matched packet.

With this rule, a client can now send a HTTP request to the web server. However, the server response will not pass through the firewall as all traffic from within the DMZ to the outside is still blocked. You can observe this by opening a Wireshark on firewall (node phoenix) interface eth1 and another on the node Internet interface eth0. Then in the terminal on node helios enter:

lynx 10.1.1.71

**Note**: You can use tcpdump as a command line alternative to Wireshark. To do so in a separate terminal on phoenix issue tcpdump -l -i eth1 and in a terminal on internet issue tcpdump -l -i eth0 which will print a summary of captured packets in the terminal.

**Outgoing rule**

To allow the response from the server to pass through, we use the following command (on phoenix):

iptables -A FORWARD -i eth1 -o eth2 -s 10.1.1.71 -p tcp --sport 80 -j ACCEPT

Notice the changes in the input and output interfaces and -s instead of -d to specify the source IP address that must be matched and the --sport instead of --dport indicating that the source port must be 80.

Try to visit the web server from helios.

**Internal to DMZ**

Write rules that allow traffic from internal network to reach servers in DMZ: web, mail and DNS.

**Check your answer**

iptables -A FORWARD -i eth0 -o eth1 -d 10.1.1.70 -p udp --dport 53 -j ACCEPT

iptables -A FORWARD -i eth1 -o eth0 -s 10.1.1.70 -p udp --sport 53 -j ACCEPT

iptables -A FORWARD -i eth0 -o eth1 -d 10.1.1.71 -p tcp --dport 80 -j ACCEPT

iptables -A FORWARD -i eth1 -o eth0 -s 10.1.1.71 -p tcp --sport 80 -j ACCEPT

iptables -A FORWARD -i eth0 -o eth1 -d 10.1.1.72 -p tcp --dport 25 -j ACCEPT

iptables -A FORWARD -i eth1 -o eth0 -s 10.1.1.72 -p tcp --sport 25 -j ACCEPT

**Internal to external**

Now that we have opened up the DMZ, we configure the firewall to allow the clients in Internal network to access web servers outside. Try to find the correct iptables rules that would implement the following:

* Any packet from the internal network is allowed to pass to the outside network.
* Insignificant traffic from the outside toward the internal network is only accepted and allowed to pass if it is a response to a request made by a local client.

This can be achieved using only ESTABLISHED and RELATED packets to pass through in the opposite direction (from outside to Internal). This is the iptables method of Stateful Inspection. Do a research on this topic to find out how to implement these rules (man iptables-extensions).

**Check your answer**

iptables -A FORWARD -i eth0 -o eth2 -s 10.1.1.0/26 -p tcp --dport 80 -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT

iptables -A FORWARD -i eth2 -o eth0 -d 10.1.1.0/26 -p tcp --sport 80 -m state --state RELATED,ESTABLISHED -j ACCEPT

**Internal to firewall**

Write rules that allow clients in internal network to connect to SSH service on phoenix.

**Check your answer**

iptables -A INPUT -i eth0 -s 10.1.1.0/26 -p tcp --dport 22 -j ACCEPT

iptables -A OUTPUT -o eth0 -d 10.1.1.0/26 -p tcp --sport 22 -j ACCEPT