Tim Casey | NS-10-LS | May 7, 2020

Network Security

Final Project – Secure Your Network



# Describe the Network Environment for this Lab

This Final Lab’s virtual Network consists of 1 Firewall on a Bridged Network connection to an outside network with some host PCs and an Internal Network with a set of hosts.

The Firewall is a pfSense Linux-based appliance.

WAN-side devices include the Host PC (Windows 10) and a Kali Linux VM.

LAN-side devices include a NagiosXI Linux-based log monitor, an Ubuntu Linux VM that is also the LAN’s Apache Web Server, and a Debian Linux host.

### Host Network on WAN side of Firewall

The Firewall’s WAN connection is on a Bridged Network Adapter setting. It receives an IP address (192.168.1.160/24) from the Host Network’s DHCP Server.

The Host PC (Win-10) also receives an IP address (192.168.1.96/24) from the Host Network’s DCHP Server.

The Host Network’s Default Gateway is set as the ISP-supplied Modem with an address of 192.168.1.254.

### Internal Network on LAN side of Firewall

The Firewall’s LAN connection is on an Internal Network “TestNet” Adapter setting. It receives a static IP address (172.16.77.1/24) for use in the Internal LAN Network.

The Nagios XI log monitor (Linux-Centos appliance) is configured with a static IP address (172.16.77.110/24) for use in the Internal LAN Network.

The Ubuntu Linux VM and Apache Web Server is configured with a static IP address (172.16.77.104/24) for use in the Internal LAN Network.

The Debian Linux VM is configured with a static IP address (172.16.77.105/24) for use in the Internal LAN Network.

The Internal LAN Network’s Default Gateway is set as the pfSense Firewall with an address of 172.16.77.1.

## Validate the network environment

Test PING from each host to each other host, including the Default Gateways.

## task 1 – Block Unwanted Traffic

Test PING from the Debian host on the LAN to external destinations on the WAN, including 4.2.2.2 and 8.8.8.8

In pfSense, create a LAN Firewall Rule to block address 8.8.8.8 destination from any LAN source.

A screenshot of a cell phone

Description automatically generated A screenshot of a cell phone

Description automatically generated

Apply the blocking firewall rule, then try to ping to address 8.8.8.8 from the Debian host and the Ubuntu host.

A screenshot of a computer

Description automatically generated

The Rule will block the hosts from reaching address 8.8.8.8 if the rule is written correctly and applied properly within pfSense.

Test PING to address 8.8.8.8 from the Ubuntu Host.

A screenshot of a computer

Description automatically generated

If the firewall rule is applied correctly, the PING to address 8.8.8.8 will fail.

Test PING to address 8.8.8.8 from Debian Host.

A screenshot of a computer

Description automatically generated

If the firewall rule is applied correctly, the PING to address 8.8.8.8 will fail.

Confirm that both LAn hosts are blocked from reaching address 8.8.8.8 via ping request

A screenshot of a computer screen

Description automatically generated

## task 2 – permit limited access to lan services from the host pc on the wan network via firewall rules

Confirm Apache2 Web Server access (172.16.77.104) from the Ubuntu Linux host on the LAN from a Firefox browser. Success will display the Apache2 Default page.

Confirm Apache2 Web Server access (172.16.77.104) from the Debian Linux host on the LAN from a Firefox browser. Success will display the Apache2 Default page.

Attempt Apache2 Web Server access (172.16.77.104) from the Remote Win10 host on the WAN from a Firefox browser. The Host PC should **NOT** be able to reach the Apache2 Default page.

A screenshot of a computer

Description automatically generated

The goal is to use the Firewall Rules feature in pfSense to create some NAT Firewall Rules to PERMIT specific access from the WAN through the Firewall to specific LAN services.

### Permit HOST on WAN to access the Apache2 Web Server on LAN

NAT Firewall Rule to permit only the Host PC’s address (192.168.1.96) on the WAN interface (192.168.1.160) as the SOURCE to redirect to the LAN interface as the DESTINATION to the Apache2 Web Server’s browser address (172.16.77.104) for standard HTTP traffic.

To further limit access, assign the destination port a specific port number (8080).

A screenshot of a cell phone

Description automatically generated

### CONFIRM that HOST on WAN can access the Apache2 Web Server on LAN

NAT Firewall Rule to permit only the Host PC’s address (192.168.1.96) on the WAN interface (192.168.1.160) as the SOURCE to redirect to the LAN interface as the DESTINATION to the Apache2 Web Server’s browser address (172.16.77.104) for standard HTTP traffic.

To further limit access, assign the destination port a specific port number (8080).

A screenshot of a social media post

Description automatically generated

### Permit HOST on WAN to access the Nagios Log Monitor on LAN

NAT Firewall Rule to permit only the Host PC’s address (192.168.1.96) on the WAN interface (192.168.1.160) as the SOURCE to redirect to the LAN interface as the DESTINATION to the Nagios Log Monitor’s browser address (172.16.77.110) for standard HTTP traffic.

To limit access, assign the destination port a specific port number (8989).

A screenshot of a cell phone

Description automatically generated

### CONFIRM that HOST on WAN can access the Nagios Log Monitor on LAN

NAT Firewall Rule to permit only the Host PC’s address (192.168.1.96) on the WAN interface (192.168.1.160) as the SOURCE to redirect to the LAN interface as the DESTINATION to the Nagios Log Monitor’s browser address (172.16.77.110) for standard HTTP traffic.

To limit access, assign the destination port a specific port number (8989).

A screenshot of a computer

Description automatically generated

### Permit HOST on WAN to access the pfSense Firewall on LAN

NAT Firewall Rule to permit only the Host PC’s address (192.168.1.96) on the WAN interface (192.168.1.160) as the SOURCE to redirect to the LAN interface as the DESTINATION to the pfSense Firewall’s browser address (172.16.77.1) for standard HTTP traffic.

To limit access, assign the destination port a specific port number (9090).

A screenshot of a computer

Description automatically generated

### CONFIRM that HOST on WAN can access the pfSense Firewall on LAN

NAT Firewall Rule to permit only the Host PC’s address (192.168.1.96) on the WAN interface (192.168.1.160) as the SOURCE to redirect to the LAN interface as the DESTINATION to the pfSense Firewall’s browser address (172.16.77.1) for standard HTTP traffic.

To limit access, assign the destination port a specific port number (9090).

A screenshot of a social media post

Description automatically generated

Apply all 3 NAT Forwarding rules on the pfSense Firewall.

A screenshot of a computer

Description automatically generated

## task 3 – gather logs for monitoring in nagios

Enable SNMP service in the pfSense Firewall so that logs of certain services may be sent to the monitoring appliance in Nagios on the LAN interface.

Enable the Nagios Monitoring appliance to receive logs from the pfSense firewall via SNMP.

A screenshot of a computer

Description automatically generated

### CONFIRM that Nagios Monitoring on LAN is receiving logs from the pfSense Firewall on LAN

A screenshot of a computer

Description automatically generated

## task 4 – install a vpn solution to grant host pc access to the lan services

Enable VPN service in the pfSense Firewall so that VPN Clients outside of the LAN may have access to the services on the LAN interface.

A screenshot of a computer screen

Description automatically generated

A screenshot of a cell phone

Description automatically generated