**Lab Exercise: Configuring and Managing Firewall Rules in pfSense to Control Network Traffic**

This lab will guide you through the process of installing pfSense in a VirtualBox environment and then configuring various firewall rules to control network traffic.

**Estimated Time:** 2-3 hours.

**Part 1: Installing pfSense in VirtualBox**

**Objective:** Set up a virtualized pfSense firewall.

**Requirements:**

* VirtualBox is installed on your host machine.
* <https://youtu.be/s3BM4dgn_Is> can be used to watch the installation process if necessary
* pfSense CE (Community Edition) ISO image downloaded from the official pfSense website. (Already provided by trainer, need not download)
* <https://youtu.be/Y-Dj8lHmXy8> can be used to watch the installation process of pfSense if any necessary.

**Steps:**

1. **Create a New Virtual Machine in VirtualBox:**
   * Open VirtualBox.
   * Click "New" to create a new VM.
   * **Name:** pfSense-Firewall
   * **Type:** BSD
   * **Version:** FreeBSD (64-bit)
   * Click "Next."
   * A screenshot of a computer

     AI-generated content may be incorrect.



1. **Memory Allocation:**
   * Allocate 8192 MB (8 GB) of RAM. You can give more if your host machine allows.
   * And 4 CPU
   * Click "Next."
   * A screenshot of a computer

     AI-generated content may be incorrect.
2. **Hard Disk:**
   * Select "Create a virtual hard disk now."
   * Click "Create."
   * **Hard disk file type:** VDI (VirtualBox Disk Image)
   * Click "Next."
   * **Storage on physical hard disk:** Dynamically allocated (This saves space on your host).
   * Click "Next."
   * **File location and size:**
     + Choose a location.
     + Set the size to 16 GB.
   * Click "Create."
   * A screenshot of a computer

     AI-generated content may be incorrect.



1. **Configure Network Adapters:**
   * With your pfSense-Firewall VM selected, click "Settings" -> "Network."
   * **Adapter 1 (WAN Interface):**
     + Enable Network Adapter.
     + **Attached to:** Bridge Adapter (This allows pfSense to access the internet).
     + Click "OK."
     + A screenshot of a computer

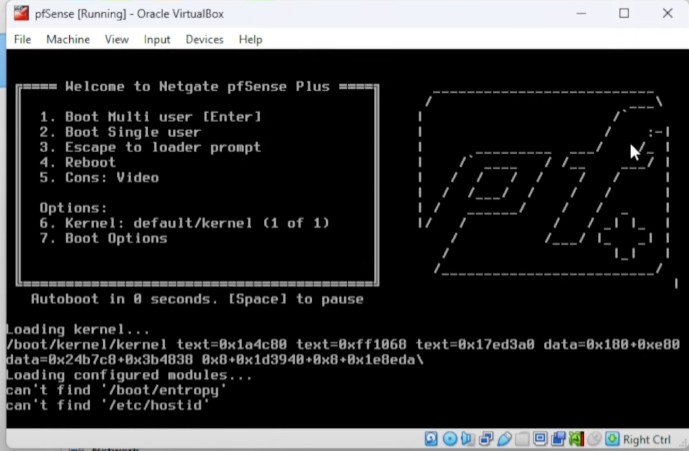
       AI-generated content may be incorrect.
   * **Adapter 2 (LAN Interface):**
     + Go to "Adapter 2."
     + Enable Network Adapter.
     + **Attached to:** Internal - Network
     + **Name:** Lan-network (This creates an isolated network for your internal VMs).
     + Click "OK."
     + A screenshot of a computer

       AI-generated content may be incorrect.



1. **Start the pfSense VM and install:**

Follow the images to install Pfsense on the VirtualBox.

****

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A computer screen with a blue and white screen

AI-generated content may be incorrect.**

**A computer screen with a blue background

AI-generated content may be incorrect.**

**A computer screen with a blue background

AI-generated content may be incorrect.**

**A computer screen with a blue screen

AI-generated content may be incorrect.**



em0, em1 are WAN and LAN adapters of Pfsense. Recheck the MAC address assigned during the installation from the virtual box setting. When em0 is asked to select, select the right mac address by checking with virtual box mac address.

**A computer screen with a blue and white screen

AI-generated content may be incorrect.**

**A computer screen with a message

AI-generated content may be incorrect.**



Choose the LAN address correctly.

**A computer screen with a blue and white screen

AI-generated content may be incorrect.**

**A computer screen shot of a computer

AI-generated content may be incorrect.**

**A computer screen with a message

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A computer screen with a blue and white screen

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A computer screen with a blue background

AI-generated content may be incorrect.**

**A computer screen with white text

AI-generated content may be incorrect.**

**Remove ISO after Installation:**

* + Before the VM reboots completely, go to "Devices" -> "Optical Drives" -> "Remove disk from virtual drive" (or force unmount if prompted). This ensures it boots from the hard drive.
  + If it reboots into the installer, power off the VM, remove the ISO from "Settings" -> "Storage," and then start it again.
  + A screenshot of a computer

    AI-generated content may be incorrect.
  + A screenshot of a computer

    AI-generated content may be incorrect.
  + Delete the Controller: IDE ISO file and let the SATA be the primary booting option.

A screenshot of a computer

AI-generated content may be incorrect.



Once Pfsense is installed, the above screen will open.

* + The console will display the WAN IP (from NAT, probably DHCP) and the LAN IP (default 192.168.1.1).
  + **Note down the LAN IP address.** This is how you will access the web interface.

**Part 2: pfSense Dashboard and Navigation Basics**

**Objective:** Access the pfSense web interface and familiarize yourself with the dashboard.

**Steps:**

1. **Set up a Client VM (Optional but Recommended):**
   * Create another Virtual Machine (e.g., Windows 10, Ubuntu Desktop) in VirtualBox.
   * **Name:** Client-PC
   * **Network Settings:** Set its network adapter to "Internal Network" and the **Name** to Lan-network (the same internal network as pfSense's LAN interface).
   * Start this Client-PC VM.
   * It should receive an IP address from pfSense's DHCP server (in the 192.168.1.x range).
   * **Verify Connectivity:** Try to ping 192.168.1.1 (pfSense LAN IP) from your Client-PC.
2. **Access the pfSense Web Interface:**
   * From your Client-PC (or your host machine if you configure its network to access the internal network), open a web browser.
   * Navigate to https://192.168.1.1 (the pfSense LAN IP).
   * You'll likely get a certificate warning; accept it and proceed.
   * **Login:**
     + **Username:** admin
     + **Password:** pfsense
     + A screenshot of a login screen

       AI-generated content may be incorrect.
3. **Initial Setup Wizard:**
   * The wizard will guide you through basic configuration and let the default setting be as it is, rather than making any changes.
   * Follow the images.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Provide the new password.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

This is how the final Dashboard would look like with all the details.

1. **Dashboard Overview:**
   * After the wizard, you'll be on the pfSense dashboard.
   * Familiarize yourself with the widgets: System Information, Interfaces, Gateways, DNS Servers, Firewall Logs, etc.
   * **Navigation:** Explore the main menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics.

**Following images give a picture of all the available options in the navigation pane.**

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Part 3: Creating and Managing Firewall Rules (Allow, Deny, Block)**

**Objective:** Learn how to create, edit, and apply firewall rules.

**Steps:**

1. **Understand Default Rules:**
   * Navigate to Firewall -> Rules.
   * Select the LAN tab.
   * Observe the default rules. There's usually a "Default allow LAN to any rule" that permits all traffic from the LAN to the WAN.

A screenshot of a computer

AI-generated content may be incorrect.

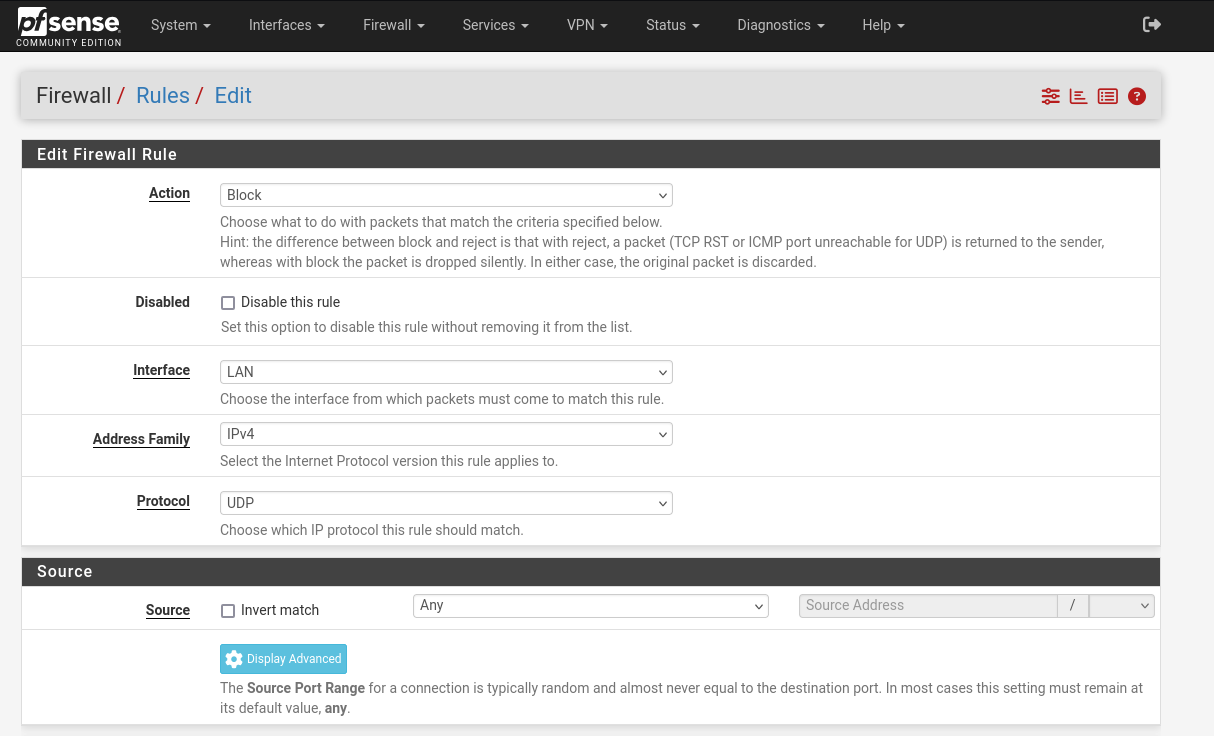
A screenshot of a computer

AI-generated content may be incorrect.

1. **Create a "Block DNS" Rule (and observe the impact):**
   * **Purpose:** To demonstrate how a block DNS rule works.
   * On the LAN tab, click the "Add" button (the one with the plus sign at the top of the rule list).
   * **Action:** Block
   * **Interface:** LAN
   * **Family Address:** IPv4
   * **Protocol:** UDP
   * **Source:** LAN subnet
   * **Destination:** Any
   * **Destination Port:** 53
   * **Description:** Block all DNS from LAN
   * Click "Save."
   * Click "Apply Changes" at the top.
   * **Test:** From your Client-PC VM, try to nslookup google.com or browse to any google.com. It should fail.

A screenshot of a computer

AI-generated content may be incorrect.

Follow the image to set the rule

A screenshot of a computer

AI-generated content may be incorrect.

And click on save.

A screenshot of a computer

AI-generated content may be incorrect.



Click on apply change and go to the terminal and browser to test the rules, results should as in the images shown below.

A screenshot of a computer

AI-generated content may be incorrect.

Nslookup failing but curl command working.

A screenshot of a computer

AI-generated content may be incorrect.

Failing to load in the browser when searched by Google.com

1. **Create an "Allow ALL" Rule:**
   * **Purpose:** To allow traffic
   * On the LAN tab, click the "Add" button (the one with the plus sign at the top of the rule list).
   * **Action:** Pass
   * **Interface:** LAN
   * **Address Family:** IPv4
   * **Protocol:** \*
   * **Source:** LAN net
   * **Destination:** Any
   * **Description:** Allow traffic
   * Click "Save."
   * **Reorder Rule:** Click the arrow icon next to the "Allow traffic" rule and drag it **above** the "Block DNS" rule. Rules are processed from top to bottom.
   * Click "Apply Changes."
   * **Test:** test from the terminal with nslookup command and also browse in the browser.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Disable/Delete Rules:**
   * You can disable a rule by clicking the toggle icon next to it.
   * You can delete a rule by clicking the trash can icon.
   * **Action:** Delete the "Block all outbound from LAN" rule and the "Allow DNS traffic" rule for now, so you can start fresh.
   * Click "Apply Changes."
   * **Test:** From your Client-PC VM, verify that you can access the internet again.

**Part 4: ICMP, TCP, UDP Filtering Examples (Block ICMP, Allow HTTPS)**

**Objective:** Implement more specific filtering based on common protocols.

**Steps:**

1. **Block ICMP (Ping) from LAN:**
   * On the LAN tab, click "Add."
   * **Action:** Block
   * **Interface:** LAN
   * **Address Family:** IPv4
   * **Protocol:** ICMP
   * **ICMP Type:** Any (or you can select specific types like echo request for outbound pings)
   * **Source:** LAN net
   * **Destination:** Any
   * **Description:** Block outbound ICMP from LAN
   * Click "Save."
   * Click "Apply Changes."
   * **Test:** From your Client-PC, try to ping 8.8.8.8 or google.com. It should now fail.
   * Verify that web browsing still works (because the default allow rule is still there, and the ICMP block only affects ping).
   * Rules will only work when “apply changes” is clicked every time the rule is modified.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer error

AI-generated content may be incorrect.

1. **Allow HTTPS (Port 443) Only:**
   * **Purpose:** To secure the network by only allowing essential web traffic.
   * On the LAN tab, click "Add" (at the top).
   * **Action:** Pass
   * **Interface:** LAN
   * **Address Family:** IPv4
   * **Protocol:** TCP
   * **Source:** LAN net
   * **Destination:** Any
   * **Destination Port Range:**
     + **From:** HTTPS (Port 443)
     + **To:** HTTPS (Port 443)
   * **Description:** Allow outbound HTTPS
   * Click "Save."
   * **Add a Block HTTP Rule Below HTTPS:**
     + Click "Add" again (this time, use the plus sign at the **bottom** of the rule list or ensure it's below your HTTPS rule).
     + **Action:** Block
     + **Interface:** LAN
     + **Address Family:** IPv4
     + **Protocol:** TCP
     + **Source:** LAN net
     + **Destination:** Any
     + **Destination Port:** from 80 to 80
     + **Description:** Block HTTP outbound traffic
     + Click "Save."
   * **Reorder Rules:** Ensure your Block outbound HTTP from LAN rule, Allow outbound HTTPS rule are in the correct order. The Allow HTTPS should be above the Block HTTP outbound traffic. This allows only HTTPS traffic. Click "Apply Changes."
   * **Test:**
     + Try to browse an HTTPS website (e.g., https://google.com). It should work.
     + Try to browse an HTTP website (e.g., http://example.com - if you can find one, it's becoming rare). It should fail.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

While processing the above rules, we have seen that rules should be in order of execution, and also pfSense implies rules in a top-down approach. Rule processing order and priority will be based on the requirements of execution. Firewall rule order and priority are crucial because the firewall processes rules sequentially, stopping at the first matching rule to apply its action. This means more specific rules, or those with higher priority, should be listed first to control traffic effectively, as a broad "deny all" rule placed first will block all subsequent rules, including any "allow" rules. Prioritization ensures that security policies are applied in a predictable and intended manner, preventing unintended access or blocking of traffic.

**Part 5: Log Analysis and Monitoring of Blocked Packets**

**Steps:**

1. **Access Firewall Logs:**
   * In the pfSense web interface, navigate to Status -> System Logs -> Firewall.

A screenshot of a computer

AI-generated content may be incorrect.

* + This page displays real-time firewall log entries of the firewall as shown in the image below.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Filter Logs:**
   * You can use the "Filter" options at the top to narrow down results.
   * **Action:** Filter by "Block" to see only blocked traffic.
   * **Interface:** Filter by "LAN" to see traffic originating from your LAN.
   * **Source IP:** You can filter by your Client-PC's IP address.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Monitoring the firewall**

A screenshot of a computer

AI-generated content may be incorrect.

**A screenshot of a computer

AI-generated content may be incorrect.**

Setting the above parameters as shown in the figure will fetch a graph showing the A screen shot of a computer

AI-generated content may be incorrect.

Data summary as shown belowA screenshot of a computer

AI-generated content may be incorrect.

**This ends the first Pfsense lab and we shall move to next lab session.**