**Overall Lab Objective**

To create two logically separate networks (VLANs) for HR and IT departments using a single physical network interface on pfSense. You will then configure firewall rules to control the traffic between these networks, demonstrating effective network segmentation.

**Prerequisites & Environment Setup**

This lab requires a slightly expanded VirtualBox environment.

1. **pfSense VM:** Your existing pfSense-Firewall VM(Main PF firewall VM).
2. **Two Client VMs:** You need two separate client machines to test the segmentation.
   * Use your existing Client-VM and rename it to HR-Client.
   * **Clone** the HR-Client to create a second, identical VM and name it IT-Client. (Right-click the VM -> Clone -> Full Clone -> Give it the new name).
3. **Virtual Network Configuration:**
   * Ensure the pfSense-Firewall VM has its LAN adapters (Adapter 3 and 4) connected to the **Internal Network** named hr-net and it-net, respectively.
   * Ensure both the HR-Client and IT-Client VMs have their single network adapter connected to the **same** hr-net and it-net Internal Network, respectively. This simulates all three devices being plugged into the same physical switch.

**Lab Task 1: Creating VLANs in pfSense (HR & IT)**

**Goal:** Define the VLAN tags that pfSense will use to separate traffic.

1. Log into your pfSense web interface as the admin user.
2. Navigate to **Interfaces > Assignments**.
3. Click on the **VLANs** tab.
4. Click the **+ Add** button to create your first VLAN.
   * **Parent Interface:** Select your LAN interface (e.g., em1). This is the physical port the tagged traffic will travel on.
   * **VLAN Tag:** 10. This is the unique ID for the HR network.
   * **Description:** HR Network.
   * Click **Save**.
5. Click **+ Add** again to create the second VLAN.
   * **Parent Interface:** Select the same LAN interface (e.g., em1).
   * **VLAN Tag:** 20. The unique ID for the IT network.
   * **Description:** IT Network.
   * Click **Save**.

You have now defined the VLANs, but they don't do anything until they are assigned and configured.

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.

**Lab Task 2: Interface Assignments and Configuration**

**Goal:** Turn the virtual VLANs into usable pfSense interfaces with IP addresses.

1. Navigate back to **Interfaces > Assignments**.
2. Under **Available network ports**, you will now see your two new VLANs.
3. Click the **+ Add** button next to VLAN 10 on em1 to create a new interface called OPT1.
4. Click the **+ Add** button next to VLAN 20 on em1 to create another new interface called OPT2.

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. Now, let's configure OPT1 for the HR department. Click on the OPT1 name.
   * Check the box for **Enable interface**.
   * Change the **Description** to HR.
   * Set **IPv4 Configuration Type** to Static IPv4.
   * Under **Static IPv4 Configuration**, set the **IPv4 Address** to 192.168.10.1 and the subnet mask to /24.
   * Click **Save**, and then **Apply Changes**.

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. Next, configure OPT2 for the IT department. Go back to **Interfaces > Assignments** and click on OPT2.
   * Check the box for **Enable interface**.
   * Change the **Description** to IT.
   * Set **IPv4 Configuration Type** to Static IPv4.
   * Set the **IPv4 Address** to 192.168.20.1 with a /24 subnet mask.
   * Click **Save**, and then **Apply Changes**.

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.

**Lab Task 3: DHCP Setup per VLAN**

**Goal:** Configure pfSense to automatically assign IP addresses to devices on both the HR and IT networks.

1. Navigate to **Services > DHCP Server**.

A screenshot of a computer

AI-generated content may be incorrect.

1. You will now see tabs for your new interfaces: **HR** and **IT**.

A screenshot of a computer

AI-generated content may be incorrect.



1. Click on the **HR** tab.
   * Check the box for **Enable DHCP server on HR interface**.
   * Set the **Range** of IP addresses to issue, for example, from 192.168.10.100 to 192.168.10.200.
   * Click **Save**.

A screenshot of a computer

AI-generated content may be incorrect.



A screenshot of a computer

AI-generated content may be incorrect.



1. Now click on the **IT** tab.
   * Check the box for **Enable DHCP server on IT interface**.
   * Set the **Range** from 192.168.20.100 to 192.168.20.200.
   * Click **Save**.

A screenshot of a computer

AI-generated content may be incorrect.



**Lab Task 4: Firewall Rule Configuration for Inter-VLAN Restrictions**

**Goal:** Implement the core security policy: IT can access the HR network, but HR cannot access the IT network.

1. First, we need to give both networks internet access.
   * Navigate to **Firewall > Rules**.

A screenshot of a computer

AI-generated content may be incorrect.



* + Click the **HR** tab. Click **+ Add**.

A screenshot of a computer

AI-generated content may be incorrect.



* + Create a rule that allows traffic from HR net to any destination. This is a basic "allow out" rule. Click **Save**.

A screenshot of a computer

AI-generated content may be incorrect.



* + Click the **IT** tab. Click **+ Add**.
  + Create a similar rule allowing traffic from IT net to any destination. Click **Save**.

A screenshot of a computer

AI-generated content may be incorrect.



A screenshot of a computer

AI-generated content may be incorrect.

1. Now, create the specific inter-VLAN rule.
   * While on the **IT** tab, click **+ Add** to create a new rule.
   * **Action:** Pass
   * **Interface:** IT
   * **Protocol:** any
   * **Source:** IT net
   * **Destination:** Select Single host or alias and type HR net.
   * **Description:** Allow IT to access HR network.
   * Click **Save**, then **Apply Changes**.

A screenshot of a computer

AI-generated content may be incorrect.



A screenshot of a computer

AI-generated content may be incorrect.



**Important:** We do **NOT** need to create a block rule on the HR interface. By default, pfSense blocks all traffic between interfaces unless a "Pass" rule specifically allows it. Since we never created a rule allowing HR to talk to IT, that traffic is already blocked.

**Lab Task 5: Testing Segmentation with Ping and Access Attempts**

**Goal:** Verify that your firewall rules are working exactly as intended.

1. **Start both client VMs:** Power on HR-Client and IT-Client.
2. **Check IP Addresses:**
   * On HR-Client, open a terminal and type ip a. It should have an IP address in the 192.168.10.x range.

A screenshot of a computer screen

AI-generated content may be incorrect.

* + On IT-Client, do the same. It should have an IP in the 192.168.20.x range.

A screenshot of a computer screen

AI-generated content may be incorrect.

1. **Perform the Tests from HR-Client:**
   * In the terminal, test internet access: ping 8.8.8.8. This **should succeed**.

A screenshot of a computer

AI-generated content may be incorrect.

1. **Perform the Tests from IT-Client:**
   * In the terminal, test internet access: ping 8.8.8.8. This **should succeed**.

A computer screen with numbers and letters

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

* + Now, attempt to access the HR network: ping 192.168.10.100 (the HR-Client's IP). This **should SUCCEED**.

A screenshot of a computer

AI-generated content may be incorrect.

**Conclusion:** If your tests produce these results, you have successfully created VLANs, assigned them to interfaces, provided DHCP, and implemented an asymmetrical firewall policy to achieve network segmentation and also tested the segmentation with ping and access attempts.