Small Office Network Setup with a pfSense Firewall with Snort for Network Security

Objective:

To create a simulated corporate office network environment that mirrors a small-scale business setup, complete with multiple user workstations, a central server, and enhanced network security. This environment includes a pfSense firewall with Snort for real-time intrusion detection, enabling the implementation and management of essential IT infrastructure and security practices.

A diagram of a computer network

Description automatically generated

Equipment Used (hardware/software):

* Alienware M15 R1
  + Nvidia 1060 GPU
  + 8th Gen Intel Core i7
  + 16 GB Ram
  + 1Tb HDD
  + 500 Gb SSD
  + Windows 10 Operating System
* VirtualBox
  + pfSense iso file
  + Windows Server 2022 iso file
  + Windows 10 iso file

Steps:

**Step 1: Create and Configure pfSense Virtual Machine**

1. **Create the pfSense Virtual Machine**
2. **Set network adapters for pfSense**
   * **Adapter 1:** Set to NAT
   * **Adapter 2:** Set to Internal Network. Name it “intnet” (This will connect Windows Virtual Machines to the LAN)
3. **Install pfSense**
   * Boot the pfSense Virtual Machine with the installation ISO
   * Follow on screen instructions to complete installation
   * Configure WAN on Adapter 1 and LAN on Adapter 2
   * Enable DHCP on the LAN interface to assign Ips to connected devices

**Step 2: Create the Windows Server Virtual Machine**

1. **Create the Windows Server Virtual Machine**
2. **Set network adapters for Windows Server**
   * **Adapter 1:** Set to Internal Network(“intnet”).
3. **Install and Configure Windows Server**
   * Install Windows Server on the Virtual Machine
   * After installation, go to network connections(win + r -> ncpa.cpl) and configure the internet adapter with a static IP on the pfsense LAN subnet (I used 192.168.1.101)
   * Set Preferred DNS to point to itself(192.168.1.101) and secondary DNS to the pfSense(192.168.1.1)
4. **Install Active Directory Domain Services**
   * Promote the Windows Server to a Domain Controller with Active Directory
   * Create new forest and continue with Domain Controller Options

**Step 3: Create the Windows 10 Virtual Machine**

1. **Create the Windows 10 Virtual Machine**
2. **Set network adapters for Windows Server**
   * **Adapter 1:** Set to Internal Network(“intnet”).
3. **Install and Configure Windows 10**
   * Boot and install Windows 10
   * Ensure the internal network adapter connects to pfSense
   * Set DNS to point to the Windows Server IP address to enable domain joining
4. **Join Windows 10 to the Domain**
   * Go to System Properties > Change Properties > Network ID to join the domain created by the Windows Server.
   * Reboot as required.

**Step 4: Install and Configure Snort on pfSense**

1. **Access the pfSense Web Interfaces**
   * Open a browser on the Windows Server and go to <http://192.168.1.1> (pfSense LAN IP)
   * Log in with the pfSense admin credentials
2. **Install Snort**
   * In pfSense, go to System > Package Manager > Available Packages
   * Find Snort and Install it
3. **Configure Snort**
   * After installation, go to Services > Snort
   * Add the LAN interface for Snort to monitor
   * Configure Settings and set rules, I selected the “Emerging Threats” rule
   * Enable logging and set up alerts to monitor network traffic

**Step 5: Test Network Connectivity**

1. **Verify Network Connectivity**
   * On the Windows 10 and Windows Server Virtual Machines, test connectivity by pinging the pfSense
   * Check internet connectivity on both Windows Machine
2. **Test Firewall and Snort connectivity**
   * Configure firewall rules on pfSense to control traffic between WAN and LAN
   * Run network scans from Windows 10 to verify that snort detects and suspicious activities
3. **Verify Domain and DNS Configuration**
   * Create and configure new users using Active Directory on Server
   * Log into each domain profile to ensure network policies are in place from Windows Server

Summary:

Through this project, I learned how to set up and manage a secure virtual network environment, simulating a corporate office with multiple users, a Windows Server, and enhanced network security using pfSense with Snort. I gained hands-on experience with configuring firewalls, managing user permissions with Active Directory, and monitoring network traffic for threats. This project deepened my understanding of network segmentation, security best practices, and the essential tools used to secure and maintain IT infrastructure in a business setting.