Network Security Optimization with pfSense Firewall & IDS

Introduction

In today's cybersecurity landscape, securing network infrastructure is essential to prevent unauthorized access and mitigate threats. This project demonstrates how to **optimize network security using pfSense**, a powerful open-source firewall, in combination with an **Intrusion Detection System (IDS)** like **Snort or Suricata**.

The goal is to **enhance network security** by configuring firewall rules to control traffic, setting up IDS to detect threats, and implementing logging mechanisms for analysis.

Project Objectives

✅ Set up a **pfSense firewall** to filter incoming and outgoing traffic.
✅ Implement **Intrusion Detection (IDS)** using **Snort or Suricata**.
✅ Automate **security monitoring and logging** for threat analysis.
✅ Improve **network resilience** against attacks like **brute force, malware, and unauthorized access**.

Step 1: Setting Up pfSense Firewall

1.1 Install pfSense on a Virtual Machine

To begin, download and install **pfSense** on a virtual machine.

1. Download **pfSense ISO** from pfSense Official Site.
2. Install pfSense on **VirtualBox/VMware** with at least two network interfaces (**LAN** and **WAN**).
3. Configure the **LAN** for internal traffic and the **WAN** for external access.

1.2 Configuring Firewall Rules

A firewall is essential for controlling network traffic. Follow these steps to configure **pfSense firewall rules**:

1. Navigate to **Firewall > Rules** in the pfSense Web UI.
2. Define the following **custom rules**:
    - **Allow internal traffic** for trusted devices (LAN to WAN).
    - **Block unauthorized access** to sensitive ports (e.g., SSH, RDP).
    - **Enable logging** for all blocked traffic.
3. Apply the firewall rules and monitor logs for unauthorized connection attempts.

Step 2: Configuring Intrusion Detection System (IDS)

2.1 Installing Snort or Suricata

IDS helps detect suspicious activity and prevent intrusions. Follow these steps to install **Snort (or Suricata)**:

1. Navigate to **System > Package Manager** in pfSense.
2. Install **Snort** or **Suricata** from the package list.
3. Configure IDS settings to monitor LAN traffic for potential threats.

2.2 Setting Up IDS Rules

Once the IDS is installed, define security policies to detect cyber threats.

1. Enable **Emerging Threats** rules to detect:
    - Malware infections
    - Brute-force login attempts
    - DDoS attacks
2. Configure **automatic IP blocking** to block malicious traffic.
3. Monitor **real-time alerts** under **Services > Snort/Suricata > Alerts**.

Step 3: Logging and Monitoring Network Security

3.1 Enabling pfSense Logging

1. Navigate to **Status > System Logs > Firewall**.
2. Enable **logging for blocked connections**.
3. Export logs for further security analysis.

3.2 Visualizing Threats with Dashboard

- Install **Splunk or ELK Stack** for log visualization.
- Generate reports on security events.

Step 4: Testing and Validating Security Measures

To ensure the firewall and IDS are working correctly:

✅ Perform **port scans** using nmap to test firewall blocking.
✅ Simulate **brute force attacks** with Hydra and analyze IDS alerts.
✅ Generate **malicious traffic** to verify automatic blocking.

Conclusion

By implementing **pfSense firewall rules** and an **Intrusion Detection System (IDS)**, we can significantly enhance network security. This project provides a **robust defense mechanism** against unauthorized access and cyber threats. Future improvements could include **automated security reporting** and **machine learning-based threat detection**.

References & Useful Links

- pfSense Documentation
- Snort IDS Official Guide
- Suricata Documentation
