CY3001-Networks and Cyber Security-II

Project Proposal

Implementation of PFSense for Network Security

Group Members:

- Ayan Mohammad Zakriya K224728
- Sami-ur-Rehman K224673

Project Description

This project focuses on deploying PFSense as a firewall and security gateway within a virtualized environment to enhance network security. The goal is to implement a dedicated security solution that provides firewall rules, access control, and packet analysis without relying on third-party networking devices such as ISP-provided routers that integrate multiple functions (routing, Wi-Fi, switching, and security). By utilizing PFSense, we aim to achieve complete control over network security from our end.

Why PFSense?

PFSense is an open-source firewall and router software based on FreeBSD. It provides enterprise-level security features, including:

- **Firewall and NAT**: Implements advanced firewall rules for traffic filtering and protection.
- **Intrusion Detection and Prevention**: Uses Snort or Suricata to detect malicious activity.
- **VPN Support**: Secure remote access through OpenVPN and IPSec.
- **Traffic Shaping**: Prioritizes bandwidth allocation for critical applications.
- **Logging and Monitoring**: Provides detailed logs and reports on network activity.
- **Access Control and VLAN Management**: Restricts and segments network traffic efficiently.

Implementation Plan

Our PFSense deployment will be set up in a **virtual machine (VM)**, connected to a modem that provides internet access. This setup will allow us to manage security independently of ISP-provided routers, which typically handle routing, access point services (Wi-Fi), switching, and firewall controls together.

How It Works:

- The PFSense VM will act as a security gateway between the modem and internal network.
- It will enforce strict firewall policies to control inbound and outbound traffic.
- Intrusion detection and packet analysis will be configured to monitor potential threats.
- VPN and remote access configurations will be set up for secure connections.
- Network segmentation will be implemented using VLANs for enhanced security.

Functional Features

1. **Firewall Deployment**: Enforces access control and packet filtering to block unauthorized traffic.
2. **Intrusion Detection & Prevention**: Uses Snort/Suricata for real-time threat detection.
3. **Access Control & VPN Support**: Implements secure remote access and network segmentation.
4. **Traffic Analysis & Monitoring**: Captures and analyzes network activity for security insights.
5. **Custom Security Policies**: Implements rules tailored to specific security needs.

Plan of Work (5 Weeks)

Week 1:

- Research and finalize PFSense architecture.
- Set up a virtualized testing environment.

Week 2:

- Deploy PFSense VM and connect it to the modem.
- Configure firewall rules and NAT settings.

Week 3:

- Implement intrusion detection and packet analysis.
- Configure VPN and secure remote access.

Week 4:

- Test security policies against simulated threats.
- Optimize firewall and IDS/IPS settings.

Week 5:

- Perform final evaluations and security hardening.
- Document findings and prepare a security assessment report.

Team Contributions

Task	Ayan	Sami
PFSense Deployment	☑	☑
Firewall Rule Configuration	☑	
Intrusion Detection Setup		☑
VPN & Access Control	☑	☑
Packet Analysis & Reporting	☑	

References

- PFSense Documentation: https://www.PFsense.org/
- Snort IDS Documentation: https://www.snort.org/
- Suricata IDS Documentation: https://suricata.io/
- VPN Configuration Guide: https://docs.netgate.com/PFsense/en/latest/vpn/index.html

This implementation will ensure that network security is controlled entirely from our end, providing stronger security measures than relying on ISP routers that integrate multiple roles.