Project 1: pfSense Multi-VLAN Deployment & Configuration

Complete Implementation Guide

Executive Summary

Project Challenge: Optimize pfSense firewall configuration on MAC-MINI hardware for Management network (192.168.10.0/24) while maintaining operational flexibility for cybersecurity lab activities and attack simulation capabilities.

Solution Implemented: Comprehensive firewall rule assessment, traffic classification implementation, and redundant rule elimination resulted in a 17% reduction in rule complexity (6→5 rules) while enhancing security visibility through targeted logging.

Key Outcomes: Successfully maintained penetration testing capabilities with proper attack attribution, preserved administrative access to distributed security tools across network segments, and established baseline configuration for future SIEM integration.

Technical Skills Demonstrated: pfSense administration, firewall rule hierarchy optimization, traffic logging implementation, network segmentation validation, security policy development balancing operational requirements with security controls.

Business Value: Establishes production-ready network security foundation supporting both operational flexibility and security monitoring requirements essential for enterprise cybersecurity environments.

Table of Contents

Project Overview

This document provides a comprehensive guide for assessing and optimizing pfSense firewall configuration on MAC-MINI hardware as part of Week 1 of the cybersecurity home lab project series. The project focuses on establishing baseline security policies for the Management network segment while maintaining operational flexibility for lab activities.

What is pfSense?

pfSense is an open-source firewall and router platform that provides:

- **Stateful packet filtering**: Advanced firewall capabilities with rule-based traffic control
- **Network Address Translation (NAT)**: Port forwarding and outbound address translation
- **VPN services**: Site-to-site and remote access VPN capabilities
- **Traffic shaping**: Quality of Service (QoS) and bandwidth management
- **High availability**: Failover and load balancing features

Network Architecture Diagram

```
Internet → Router (192.168.2.0/24)
   ↓
MAC-MINI pfSense (WAN: 192.168.2.229, LAN: 192.168.10.1/24)
   ↓
Managed Switch (192.168.10.2) → Management Network (192.168.10.0/24)
   ├── Kali Linux (192.168.10.20) - Attack Platform
   ├── DVWA WebServer (192.168.10.20) - Vulnerability Testing
   └── Administrative Workstations

Cross-Network Access:
Management Network → pfSense VM → Internal Network (192.168.30.0/24)
   ├── OpenCTI (192.168.30.60:8080) - Threat Intelligence
   ├── ELK Stack - Log Analysis
   ├── Wazuh - SIEM Platform
   └── Additional Security Tools
```

Scope and Objectives

Project Scope

This project focuses on:

- Assessing existing pfSense configuration on MAC-MINI hardware
- Implementing baseline firewall policies for Management network (192.168.10.0/24)

- Documenting traffic patterns for administrative and attack simulation activities
- Establishing security controls while maintaining lab operational requirements
- Preparing foundation for advanced network security monitoring

Network Architecture Context:

- **MAC-MINI pfSense**: Primary firewall managing Management network (192.168.10.0/24)
- **pfSense VM**: Secondary firewall managing Internal network (192.168.30.0/24) and User-LAN (192.168.40.0/24)
- **Managed Switch**: VLAN segmentation at Layer 2 (192.168.10.2)

Objectives

Primary Objectives:

- Document current firewall configuration and security posture
- Implement documented rules for legitimate administrative traffic
- Maintain attack simulation capabilities for penetration testing
- Establish logging framework for future security analysis
- Validate network segmentation and access controls

Learning Outcomes:

- Understanding pfSense rule hierarchy and processing order
- Hands-on experience with firewall policy development
- Network security documentation best practices
- Traffic pattern analysis and logging implementation
- Balance between security and operational requirements

Prerequisites

Infrastructure Requirements

Hardware Requirements:

- **MAC-MINI**: pfSense 2.8.0 installation with dual network interfaces
- **Managed Switch**: VLAN-capable switch at 192.168.10.2
- **Network Access**: Administrative access to pfSense web interface at 192.168.10.1

Network Architecture:

- **WAN Interface (em0)**: DHCP connection to upstream router

- **LAN Interface (em1)**: Static IP 192.168.10.1/24 serving Management network
- **Management Network Devices**: Kali attack box (192.168.10.20), DVWA server, administrative workstations

Software Requirements

pfSense Version: 2.8.0 release

Access Requirements:

- Web browser with HTTPS support
- Administrative credentials for pfSense interface
- SSH access capability (optional for advanced troubleshooting)

Lab Environment Context

Connected Systems:

- **Kali Linux** (192.168.10.20): Penetration testing platform
- **DVWA WebServer**: Web application security testing platform
- **MAC Attack-box**: Additional security testing system

Cross-Network Dependencies:

- Access to Internal network tools (OpenCTI at 192.168.30.60)
- Administrative access to distributed security tools
- Attack simulation capabilities across network segments

Implementation Steps

Phase 1: Current Configuration Assessment

The first phase involves comprehensive assessment of existing pfSense deployment and security posture.

Step 1.1: Interface Configuration Review

Access pfSense web interface and document current setup:

```bash
# Access pfSense WebGUI
https://192.168.10.1
```

Interface Documentation:

- **WAN (em0)**: DHCP client configuration with RFC 1918 and bogon blocking enabled
- **LAN (em1)**: Static IPv4 192.168.10.1/24 configuration

Security Features Verified:

- Private network blocking: Enabled on WAN
- Bogon network blocking: Enabled on WAN
- Anti-lockout rule: Active on LAN interface

Step 1.2: Firewall Rules Analysis

WAN Interface Rules:

```
Priority 1: Block RFC 1918 networks (0/3.71 MiB processed)
Priority 2: Block bogon networks (0/1.58 MiB processed)
Default: No pass rules configured (implicit deny all)
```

LAN Interface Rules (Pre-Optimization):

```
Priority 1: Anti-Lockout Rule (1/1.76 MiB processed)
Priority 2: SSH to OpenCTI (192.168.30.60:22) - UNUSED
Priority 3: EasyRule OpenCTI access (192.168.10.50 → 192.168.30.60:8080) - UNUSED
Priority 4: General OpenCTI access (192.168.10.0/24 → 192.168.30.60:8080) - UNUSED
Priority 5: Default allow LAN to any (57/2.41 GiB processed)
Priority 6: Default allow LAN IPv6 to any
```

Phase 2: Security Policy Implementation

Step 2.1: Documented Rule Creation

Implement specific rules for traffic classification and operational documentation:

Rule 1: Kali Attack Traffic Documentation

- **Action**: Pass
- **Protocol**: Any
- **Source**: 192.168.10.20 (Kali system)
- **Destination**: Any
- **Purpose**: Document and log penetration testing activities

Rule 2: Management Web Services Access

- **Action**: Pass

- **Protocol**: TCP
- **Source**: 192.168.10.0/24
- **Destination**: 192.168.30.0/24
- **Ports**: 80, 443 (HTTP/HTTPS)
- **Purpose**: Administrative access to internal security tools

Step 2.2: Default Allow Rule Optimization

Logging Enhancement:

- Enable packet logging on "Default allow LAN to any" rule
- Purpose: Traffic pattern analysis for future rule refinement
- Benefit: Operational visibility without restricting functionality

Phase 3: Rule Cleanup and Optimization

Step 3.1: Redundant Rule Removal

Rules Removed:

1. **SSH to OpenCTI** (192.168.10.0/24 → 192.168.30.60:22)
2. **EasyRule OpenCTI** (192.168.10.50 → 192.168.30.60:8080)
3. **General OpenCTI access** (192.168.10.0/24 → 192.168.30.60:8080)

Justification: Default allow rule covers all removed functionality while new documented rules provide better traffic classification.

Step 3.2: Final Rule Order

Optimized LAN Interface Rules:

```
Priority 1: Anti-Lockout Rule (System protection)
Priority 2: Kali attack traffic documentation (192.168.10.20 → Any)
Priority 3: Management web services (192.168.10.0/24 → 192.168.30.0/24:80,443)
Priority 4: Default allow LAN to any (Fallback with logging enabled)
Priority 5: Default allow LAN IPv6 to any
```

Traffic Flow Diagram

```
Kali Attack Traffic (192.168.10.20):
[Kali] → [pfSense Rule 2] → [Logging] → [Any Destination] → [Attack Attribution]

Administrative Traffic (192.168.10.0/24):
[Admin Workstation] → [pfSense Rule 3] → [Logging] → [192.168.30.0/24:80,443] → [Security Tools]
```

General Traffic:
[Any LAN Device] → [pfSense Rule 4] → [Enhanced Logging] → [Any Destination] → [Pattern Analysis]

Testing and Validation

Phase 4: Connectivity Verification

Step 4.1: Administrative Access Testing

Test Cases:

1. **pfSense Web Interface**: Verify continued access to https://192.168.10.1
2. **OpenCTI Access**: Confirm connectivity to 192.168.30.60:8080
3. **SSH Connectivity**: Validate SSH access to internal systems
4. **Web Services**: Test HTTP/HTTPS access to internal management tools

Step 4.2: Attack Simulation Validation

Kali System Testing:

1. **Network Scanning**: Verify nmap functionality across network segments
2. **Web Application Testing**: Confirm access to DVWA and internal targets
3. **Tool Functionality**: Validate penetration testing tool connectivity

Phase 5: Logging Verification

Step 5.1: Traffic Pattern Analysis

Logging Validation:

- Navigate to **Status** → **System Logs** → **Firewall**
- Verify rule-specific logging for documented traffic patterns
- Confirm default rule logging captures miscellaneous traffic

Expected Log Entries:

- Kali attack traffic: Rule-specific attribution
- Administrative web access: Documented management activity
- General traffic: Default rule with detailed packet information

---

Troubleshooting

Common Issues and Solutions

Issue 1: Rule Order Problems

Symptoms:

- Traffic not matching expected rules
- Unintended rule processing order

Solution:

```bash
# Verify rule order in pfSense GUI
# Navigate: Firewall → Rules → LAN → Check rule sequence
# Drag rules to correct order if needed
# Apply changes and test connectivity
```

Issue 2: Logging Not Functioning

Symptoms:

- No log entries appearing for configured rules
- Missing traffic pattern data

Troubleshooting Steps:

```bash
# Check log settings
# Navigate: Status → System Logs → Settings → Verify log retention
# Clear logs and regenerate test traffic
# Verify rule logging checkbox enabled
```

Issue 3: Connectivity Loss After Changes

Symptoms:

- Loss of administrative access
- Service interruption

Recovery:

```bash
```

```
# Anti-lockout rule should prevent total lockout
# Access pfSense console directly if needed
# Restore configuration backup if available
# Verify default allow rule not accidentally disabled
```

Results and Outcomes

Project Success Metrics

The successful implementation of this project is demonstrated by the following results:

Functional Verification

System Status Confirmation:

- pfSense Management Network: **Operational** at 192.168.10.1
- Administrative Access: **Maintained** through optimized rules
- Attack Simulation Capability: **Preserved** with documented attribution
- Cross-Network Connectivity: **Verified** for management tools

Security Posture Improvements

Rule Optimization Results:

```
Before: 6 LAN rules (3 redundant, 1 undocumented)
After: 5 LAN rules (0 redundant, all documented)

Traffic Classification:
- Kali attack traffic: Specifically logged and attributed
- Administrative access: Documented and monitored
- General traffic: Logged for future analysis
- Security: Maintained flexibility with controlled visibility
```

Operational Benefits

Documentation Improvements:

- Clear traffic categorization for security analysis
- Elimination of redundant rules reducing complexity
- Enhanced logging for future optimization decisions
- Maintained lab functionality while improving visibility

Key Performance Indicators

Implementation Metrics:

- **Configuration Time**: 2 hours including analysis and testing
- **Rule Optimization**: 17% reduction in total rules (6→5)
- **Redundancy Elimination**: 100% removal of duplicate functionality
- **Logging Enhancement**: 100% coverage of significant traffic patterns

Security Metrics:

- **Access Control**: Maintained appropriate lab permissions
- **Traffic Visibility**: Enhanced through targeted logging
- **Attack Attribution**: Improved through Kali-specific rule documentation
- **Administrative Oversight**: Documented management traffic patterns

Network Architecture Validation

Segmentation Verification:

- Management Network (192.168.10.0/24): Properly isolated with controlled access
- Cross-Segment Access: Documented and monitored
- Attack Simulation: Maintained capabilities with proper attribution
- Security Tools Integration: Verified connectivity to OpenCTI and other platforms

---

Conclusion

Project Summary

This implementation successfully optimized the pfSense firewall configuration for the Management network while maintaining operational requirements for the cybersecurity lab environment. The project established a foundation for advanced security monitoring by implementing documented traffic classification and enhanced logging capabilities.

Technical Accomplishments:

- Assessed and documented existing pfSense 2.8.0 configuration
- Implemented traffic classification rules for operational visibility
- Eliminated redundant firewall rules while maintaining functionality
- Enhanced logging capabilities for future security analysis
- Validated network segmentation and cross-segment access controls

Laboratory Benefits:

- Maintained penetration testing capabilities with proper attribution
- Preserved administrative access to distributed security tools
- Established baseline for future firewall policy refinement
- Created foundation for advanced traffic analysis and monitoring

Skills & Career Relevance

This project demonstrates competencies directly aligned with network security and firewall administration roles:

Technical Skills Developed:

Firewall Administration

- pfSense configuration and optimization
- Rule hierarchy analysis and optimization
- Traffic logging and analysis implementation
- Network segmentation validation

Security Policy Development

- Risk-based rule design balancing security and operations
- Traffic classification for security monitoring
- Documentation standards for firewall policies
- Operational requirement analysis

Professional Competencies:

- Configuration assessment and optimization
- Security documentation best practices
- Change management in production-like environments
- Systematic troubleshooting approach

Career Path Alignment

Entry Level (0-2 years): Security Analyst

- Log analysis and traffic pattern recognition
- Basic firewall rule interpretation and documentation
- Security tool integration and monitoring
- Incident detection and escalation procedures

Mid Level (2-5 years): Network Security Engineer

- Firewall policy development and optimization
- Traffic analysis and security monitoring architecture
- Network segmentation design and validation
- Security control implementation and maintenance

Senior Level (5+ years): Security Architect

- Enterprise security policy framework design
- Multi-platform security integration strategies
- Risk assessment and security posture optimization
- Strategic security technology evaluation and implementation

Lessons Learned

Configuration Management:

- Always maintain operational requirements while improving security
- Document traffic patterns before making policy changes
- Use specific rules for attribution rather than relying solely on default policies
- Enable logging strategically for future analysis without overwhelming storage

Lab Operations:

- Balance security best practices with operational flexibility
- Maintain attack simulation capabilities for realistic testing
- Document all configuration changes for future reference
- Test connectivity thoroughly after policy modifications

Future Implementation Roadmap

Immediate Actions (0-2 weeks):

- Review NAT configuration for DVWA server exposure requirements
- Assess port forwarding needs for external access to lab services
- Validate outbound NAT policies for internal systems
- Implement enhanced firewall logging and monitoring

Intermediate Enhancements (2-3 months):

- Implement traffic analysis based on collected log data
- Refine rules based on observed traffic patterns
- Consider additional network segmentation as lab grows

- Develop automated rule optimization procedures

Long-term Integration (3-6 months):

- Integrate with SIEM for automated policy violation detection
- Implement advanced threat detection rule correlation
- Develop enterprise-grade security policy templates
- Create automated compliance reporting frameworks

Enterprise Value Proposition

This project demonstrates the ability to translate lab-based firewall administration into enterprise security policy design, with emphasis on scalability, compliance, and integration into SIEM ecosystems. The implementation showcases practical network security skills while maintaining operational requirements essential for production cybersecurity environments.

Key Value Drivers:

- **Operational Flexibility**: Maintains functionality while improving security visibility
- **Security Monitoring**: Enhanced logging for traffic pattern analysis and threat detection
- **Attack Attribution**: Clear documentation of security testing activities for compliance
- **Policy Foundation**: Baseline configuration supporting future enterprise security enhancements
- **Documentation Standards**: Professional approach to configuration management and change control

The successful implementation establishes a production-ready network security foundation supporting both operational efficiency and comprehensive security monitoring requirements.

References

Documentation Resources

1. **pfSense Official Documentation**: https://docs.netgate.com/pfsense/
2. **pfSense Firewall Rules Guide**: https://docs.netgate.com/pfsense/en/latest/firewall/
3. **Network Security Best Practices**: NIST SP 800-41 Rev 1
4. **Firewall Policy Development**: SANS Network Security Guidelines

Technical Standards

1. **RFC 1918**: Address Allocation for Private Internets
2. **RFC 3330**: Special-Use IPv4 Addresses
3. **NIST Cybersecurity Framework**: Network Security Guidelines

4. **CIS Controls**: Network Monitoring and Defense

Lab Architecture Resources

1. **pfSense Home Lab Setup**: Community best practices
2. **Network Segmentation Design**: Security architecture principles
3. **Logging and Monitoring**: SIEM integration preparation
4. **Attack Simulation**: Ethical hacking lab configuration

Document Version: 1.0
Last Updated: September 24, 2025
Author: Prageeth Panicker
Status: Implemented and Validated

This document serves as both an implementation guide and a reference for cybersecurity professionals setting up network security infrastructure in lab environments. The methodologies and configurations presented have been tested and can be adapted for production deployments with appropriate additional security hardening measures.