Zero Trust Network Architecture Implementation

CIS 3353 Group Project Plan

Project Mission Statement

Design and implement a Zero Trust Network Architecture that demonstrates the principle of "never trust, always verify" by implementing network micro-segmentation, identity-based access controls, and continuous monitoring to protect against lateral movement and insider threats in a simulated enterprise environment.

Course Modules Integration (3+ Required)

Primary Modules:

- **Architecture and Design (Modules 4, 5, 9, 11)**: Network segmentation, secure architecture principles
- **Implementation (Modules 4, 6, 7, 12)**: PKI certificates, authentication systems, encryption
- **Operations and Incident Response (Module 14)**: Continuous monitoring, logging, threat detection

Secondary Integration:

- **Threats, Attacks, and Vulnerabilities (Modules 1, 2, 3, 8)**: Lateral movement prevention, insider threats

System Architecture Overview

Core Components:

1. **pfSense Firewall/Router** - Central policy enforcement point
2. **Certificate Authority (CA)** - PKI infrastructure for device/user authentication
3. **Multiple Network Zones** - Micro-segmented VLANs
4. **SIEM/Logging Server** - Continuous monitoring and alerting
5. **Jump/Bastion Host** - Controlled administrative access
6. **Various Client Systems** - Different trust levels and roles

Network Zones:

- **Management Zone** (VLAN 10): Admin systems, CA, SIEM
- **Corporate Zone** (VLAN 20): Standard employee workstations
- **DMZ Zone** (VLAN 30): Public-facing services

- **Guest Zone** (VLAN 40): Untrusted devices
- **IoT Zone** (VLAN 50): Internet of Things devices

Sprint Planning (6 Sprints x 2 weeks each)

Sprint 1: Foundation & Network Segmentation

Goal: Establish base infrastructure and network micro-segmentation

Week 1-2 Tasks:

□ Set up pfSense VM with multiple interfaces
□ Create and configure 5 VLANs (Management, Corporate, DMZ, Guest, IoT)
□ Implement basic inter-VLAN firewall rules (default deny)
□ Deploy test VMs in each zone
□ Document network topology and IP addressing scheme
□ Create GitHub repository structure
□ Set up project wiki with network diagrams

Deliverables:

- Functional network segmentation
- Network topology documentation
- Basic firewall rule set

Sprint 2: PKI Infrastructure & Certificate-Based Authentication

Goal: Implement strong identity verification using PKI

Week 3-4 Tasks:

□ Deploy Windows Server 2019 as Certificate Authority
□ Configure certificate templates for devices, users, and services
□ Implement certificate-based authentication on pfSense
□ Set up RADIUS server for 802.1X authentication
□ Configure certificate auto-enrollment for domain devices
□ Test certificate revocation procedures
□ Document PKI hierarchy and certificate policies

Deliverables:

- Functional PKI infrastructure

- Certificate-based device authentication
- RADIUS authentication system

Sprint 3: Advanced Access Controls & Policy Enforcement

Goal: Implement granular access policies based on device trust and user identity

Week 5-6 Tasks:

□ Configure pfSense with advanced firewall rules based on certificates
□ Implement time-based access controls
□ Set up device compliance checking
□ Configure NAC (Network Access Control) policies
□ Implement application-layer filtering
□ Test policy enforcement with different device types
□ Create policy exception procedures

Deliverables:

- Granular access control policies
- Device compliance framework
- Policy enforcement testing results

Sprint 4: Continuous Monitoring & SIEM Implementation

Goal: Deploy comprehensive monitoring and threat detection

Week 7-8 Tasks:

□ Deploy Wazuh or ELK Stack for SIEM
□ Configure log collection from all network devices
□ Set up pfSense logging and monitoring
□ Implement Windows event log collection (Sysmon)
□ Create custom detection rules for Zero Trust violations
□ Build dashboards for network traffic analysis
□ Configure alerting for suspicious activities

Deliverables:

- Centralized logging and monitoring
- Zero Trust violation detection rules
- Security dashboards and alerts

Sprint 5: Advanced Threat Detection & Response

Goal: Implement automated threat response and lateral movement detection

Week 9-10 Tasks:

□ Configure behavioral analysis for anomaly detection
□ Implement automated threat response (isolate suspicious devices)
□ Set up threat intelligence feeds
□ Create incident response playbooks for Zero Trust violations
□ Test lateral movement detection capabilities
□ Implement user behavior analytics (UBA)
□ Configure threat hunting capabilities

Deliverables:

- Automated threat response system
- Lateral movement detection
- Incident response procedures

Sprint 6: Testing, Documentation & Presentation Prep

Goal: Comprehensive testing and professional documentation

Week 11-12 Tasks:

□ Conduct penetration testing to validate Zero Trust controls
□ Perform compliance assessment against Zero Trust principles
□ Complete comprehensive documentation in GitHub Wiki
□ Create demonstration scenarios for presentation
□ Prepare final project presentation
□ Conduct lessons learned session
□ Finalize project deliverables

Deliverables:

- Penetration test results
- Complete project documentation
- Final presentation
- Demo scenarios

Technical Implementation Details

Required VMs and Resources:

- **pfSense Router/Firewall**: 2GB RAM, 20GB disk
- **Windows Server 2019 (CA/RADIUS)**: 4GB RAM, 60GB disk
- **Ubuntu Server (SIEM)**: 4GB RAM, 60GB disk
- **Windows 10 (Corporate User)**: 4GB RAM, 60GB disk
- **Ubuntu Desktop (Admin Workstation)**: 4GB RAM, 40GB disk
- **Lightweight VMs for IoT simulation**: 1GB RAM each

Key Technologies:

- **pfSense**: Firewall, VPN, traffic shaping
- **Windows PKI**: Certificate Services, RADIUS
- **Wazuh/ELK**: SIEM, log analysis, threat detection
- **802.1X**: Port-based network access control
- **IPSec/SSL VPN**: Encrypted remote access
- **VLAN**: Network micro-segmentation

Zero Trust Principles Implementation:

1. Verify Explicitly

- Certificate-based device authentication
- Multi-factor authentication for users
- Device compliance checking
- Real-time risk assessment

2. Use Least Privilege Access

- Micro-segmented network zones
- Application-specific firewall rules
- Time-based access controls
- Just-in-time access for admin functions

3. Assume Breach

- Continuous monitoring and logging
- Lateral movement detection

- Behavioral analysis and anomaly detection
- Automated incident response

Risk Management & Contingency Plans

High-Risk Items:

1. **PKI Complexity**: Certificate management can be complex
   - *Mitigation*: Start with simple CA, expand gradually
   - *Backup Plan*: Use simpler authentication if PKI fails
2. **SIEM Resource Requirements**: May need significant compute resources
   - *Mitigation*: Use lightweight alternatives (Wazuh vs full ELK)
   - *Backup Plan*: Focus on pfSense logging if SIEM struggles
3. **Integration Complexity**: Multiple systems need to work together
   - *Mitigation*: Test integrations early and often
   - *Backup Plan*: Demonstrate components individually if integration fails

Success Metrics:

☐ Network traffic properly segmented and controlled
☐ Certificate-based authentication working
☐ SIEM detecting and alerting on violations
☐ Demonstration of lateral movement prevention
☐ Clear documentation of Zero Trust implementation

Demonstration Scenarios

Scenario 1: Legitimate User Access

- User with valid certificate accesses corporate resources
- Show normal traffic flow and logging

Scenario 2: Unauthorized Device

- Unknown device attempts network access
- Demonstrate blocking and alerting

Scenario 3: Compromised Device Simulation

- Simulate device compromise and lateral movement attempt
- Show detection and automated response

Scenario 4: Admin Access

- Demonstrate secure administrative access through jump host
- Show privileged access monitoring

Documentation Structure (GitHub Wiki)

Required Pages:

1. **Home**: Project overview and navigation
2. **Architecture**: Network diagrams and design decisions
3. **Implementation Guide**: Step-by-step setup instructions
4. **Configuration Files**: All configs and scripts
5. **Testing Results**: Penetration test and validation results
6. **Lessons Learned**: Challenges and solutions
7. **References**: Zero Trust frameworks and standards

Success Tips:

1. **Start Simple**: Begin with basic segmentation, add complexity gradually
2. **Document Everything**: Keep detailed notes of all configuration changes
3. **Test Continuously**: Validate each component before moving to the next
4. **Focus on Business Value**: Always relate technical controls to business security outcomes
5. **Practice Demos**: Rehearse your demonstration scenarios multiple times