NETWORK SECURITY PROJECT

Professional Security Documentation & Implementation

Amr Khaled Saad

Ahmed Mahmoud Mohamed

Youssef Hosseny Mohamed

Youssef Wageh Moawa

Overview | General Attacks & Vulnerabilities | Network Attacks | Core Security Controls | FortiGate Configuration | NAT & Firewall Policies

PROJECT OVERVIEW

This comprehensive network security project documents critical security threats, vulnerabilities, and implementation strategies for enterprise network protection. Our approach combines theoretical knowledge with practical FortiGate firewall configuration to create a robust security posture.

Key Objectives

- Identify and analyze common security threats and attack vectors
- Implement defense-in-depth strategies across all network layers
- Configure FortiGate firewall with secure policies and NAT rules
- Establish comprehensive monitoring and incident response capabilities
- Ensure compliance with security best practices and standards
- Create a scalable and maintainable security architecture

GENERAL ATTACKS & VULNERABILITIES

Social Engineering & Phishing ▲

Threat

What it is: Manipulating users to divulge sensitive information or perform malicious actions through deceptive communications.

Mitigation: Security awareness training, phishing simulations, email security (DMARC/DKIM/SPF), URL filtering, blocking risky attachments

Security Benefit: Reduces human vulnerability to social engineering attacks by 70-80% through education and technical controls.

Ransomware ▲

Threat

What it is: Malicious software that encrypts data and demands payment for decryption, causing operational disruption.

Mitigation: Offline encrypted backups, immediate patching, restrict/secure RDP, use VPN or Zero-Trust for admin access

Security Benefit: Enables rapid recovery without paying ransom, minimizes downtime and financial impact.

Web Application Attacks (SQL Injection, XSS) ▲

Threat

What it is: Exploiting vulnerabilities in web applications to steal data, execute malicious code, or compromise systems.

Mitigation: Input validation, parameterized queries, WAF rules, regular code reviews

Security Benefit: Protects sensitive data and prevents unauthorized access to backend systems.

Supply-Chain Attacks ▲

Threat

What it is: Compromising trusted third-

Weak or Reused Passwords ▲

Threat

What it is: Using easily guessable or

Unpatched Software & Firmware ▲

Threat

What it is: Running outdated systems with

party vendors or software to infiltrate target organizations.

Mitigation: Vendor security assessments, trusted update sources, strict third-party monitoring

Security Benefit: Reduces risk from compromised dependencies and maintains trust in software supply chain.

previously compromised passwords across multiple accounts.

Mitigation: Enforce MFA, strong password policies, password managers

Security Benefit: Prevents credential-based attacks and reduces account compromise by 99%.

known vulnerabilities that attackers can exploit.

Mitigation: Patch management program, CVE risk prioritization, immediate fixes for critical vulnerabilities

Security Benefit: Closes security gaps before exploitation, maintaining system integrity.

Lack of Encryption ▲

Threat

What it is: Transmitting or storing sensitive data without proper encryption, exposing it to interception.

Mitigation: Enforce TLS 1.2/1.3, full-disk encryption, encrypted backups, secure key lifecycle management

Security Benefit: Protects data confidentiality in transit and at rest, ensuring compliance.

NETWORK ATTACKS

Distributed Denial of Service (DDoS) ▲

Network Threat

Description: Overwhelming network resources with traffic to disrupt service availability.

Mitigation Strategy: CDN protection, DDoS scrubbing services, rate limiting, geo-blocking, scalable cloud resources

Network Spoofing ▲

Network Threat

Description: Forging network packets to impersonate legitimate sources and bypass security controls.

Mitigation Strategy: Depends on spoofing type (DNS/ARP/TLS), use secure protocols and validation mechanisms

ARP Spoofing ▲

Network Threat

Description: Sending fake ARP messages to associate attacker's MAC with legitimate IP addresses.

Mitigation Strategy: Dynamic ARP Inspection, 802.1X, NAC, static ARP entries

Man-in-the-Middle (MitM) ▲

Network Threat

Description: Intercepting communications between two parties to eavesdrop or alter data.

Mitigation Strategy: Enforce TLS 1.2/1.3, HSTS, VPN on untrusted networks, wireless intrusion detection (WIDS)

DNS Spoofing ▲

Network Threat

Description: Corrupting DNS responses to redirect users to malicious websites.

Mitigation Strategy: DNSSEC, trusted DNS providers, enforce HTTPS, anomaly monitoring

Unsecured Networks (Open or Poorly Segmented Wi-Fi) ▲

Network Threat

Description: Exposing network traffic through unencrypted or improperly segmented wireless networks.

Mitigation Strategy: Network segmentation, traffic isolation, strong Wi-Fi encryption

Misconfigured Firewalls ▲

Network Threat

Description: Improperly configured firewall rules that allow unauthorized access or expose services.

Mitigation Strategy: Regular rule reviews,

remove unused ports/services, secure management interfaces

CORE SECURITY CONTROLS

Identity & Access Management (IAM) ▲

Security Control

Overview: MFA everywhere, least-privilege access, centralized SSO/IdP

Implementation: Implement multi-factor authentication across all systems, enforce role-based access control (RBAC), and utilize single sign-on for centralized authentication management.

Patch & Vulnerability Management ▲

Security Control

Overview: Asset inventory, CVE prioritization, immediate patching for critical issues

Implementation: Maintain comprehensive asset inventory, prioritize vulnerabilities based on CVSS scores and exploitability, and establish rapid response procedures for critical patches.

Monitoring & Detection (SIEM / EDR / IDS / IPS) ▲

Security Control

Overview: Log correlation, anomaly detection, fast alerts and response

Implementation: Deploy Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and network intrusion detection/prevention systems for comprehensive threat visibility.

Encryption & Key Management ▲

Security Control

Overview: TLS 1.2/1.3, full-disk encryption, encrypted backups, secure key lifecycle processes

Implementation: Enforce modern encryption standards, implement Hardware Security Modules (HSMs) for key storage, and establish proper key rotation policies.

Backup & Disaster Recovery (DR) ▲

Security Control

Overview: Offline encrypted backups, regular recovery testing, business continuity planning

Implementation: Implement 3-2-1 backup strategy (3 copies, 2 different media, 1 offsite), test recovery procedures quarterly, and maintain detailed disaster recovery documentation.

Incident Response & Security Resilience ▲

Security Control

Overview: Documented IR plan, defined roles, continuous threat awareness and readiness

Implementation: Establish incident response team with clear roles and responsibilities, conduct regular tabletop exercises, and maintain threat intelligence feeds for proactive defense.

FORTIGATE CONFIGURATION STEPS

1 Initial Access & Password Security

Action: Logged into FortiGate using DHCP-assigned IP 192.168.1.10

Why: Verify device connectivity and begin secure configuration

Security Benefit: Protects against unauthorized login and reconnaissance

2 Initial IP Discovery and WAN Configuration

Action: Configured Port 1 (WAN) in DHCP mode

Why: Ensure valid IP for network access without static assignment

Security Benefit: Reduces IP spoofing and attack surface

3 Assigning the Hostname

Action: Changed hostname to NTL_Fortinet

Why: Improve device identification in logs and audits

Security Benefit: System hardening and prevents targeting confusion

4 Creating a New Administrator Account

Action: Created super_admin account NTI with strong password

Why: Default accounts are common attack targets

Security Benefit: Mitigates credential attacks and brute-force attempts

5 Configuring the LAN Interface

Action: Configured Port 2 (LAN) with 172.16.0.1/24, DHCP server 172.16.0.2-254

Why: Secure internal network management and automation

Security Benefit: HTTPS protects against MitM, DHCP prevents conflicts

6 Testing the Internal DHCP Server

Action: Verified internal device received IP 172.16.0.2

Why: Validate internal network readiness

Security Benefit: Prevents DHCP failures and confirms stability

7 Configuring LAN_2 Interface (Port3)

Action: LAN_2 (Port3) was configured with IP 172.16.2.1/24 and DHCP enabled for the 172.16.2.x network.

Why: To create a second internal network segment for testing routing and inter-LAN communication.

Security Benefit: Allows network segmentation, which is essential for limiting lateral movement in case of internal compromise.

8 Testing LAN_2 DHCP

Action: A client automatically obtained the IP 172.16.2.2 from the DHCP server.

Why: To verify the correct configuration of DHCP services on the second LAN.

Security Benefit: Confirms reliability of the second internal segment and ensures readiness for multi-LAN communication.

9 Creating LAN-to-LAN Firewall Policies

Action: Two firewall policies were created: - PC1_PING_PC2 (LAN_1 → LAN_2) - PC2_PING_PC1 (LAN_2 → LAN_1) Services were restricted to PING only.

Why: To enable controlled communication between LANs for testing routing functionality.

Security Benefit: Limits unnecessary exposure between networks and prevents unauthorized traffic, following least-privilege principles.

10 Testing LAN-to-LAN Communication

Action: Clients successfully pinged: - LAN_1 gateway: 172.16.0.1 - LAN_2 client: 172.16.2.2

Why: To verify routing, connectivity, and firewall policy functionality.

Security Benefit: Ensures the firewall enforces controlled, reliable communication between segmented networks while preventing unintended access.

NAT & FIREWALL POLICIES

1 Virtual Machine Network Configuration

Configuration: FortiGate with VMnet2 (LAN) and VMnet1 (WAN), hosts segmented accordingly

Security Benefit: Enables firewall functionality, safeguards internal systems

2 Static Route Configuration

Configuration: Default route 0.0.0.0/0 via 192.168.1.1 on WAN

Security Benefit: Enforces all traffic through firewall for policy enforcement

3 Source NAT (SNAT) Policy

Configuration: Translates internal IPs to WAN interface for Internet access

Security Benefit: Hides internal addresses, enables secure external access

4 Destination NAT (DNAT) / Port Forwarding

Configuration: VIP mapping WAN 192.168.1.10:80 to internal server 10.0.0.2:80

Security Benefit: Permits selective inbound traffic with translation

5 Verification of NAT Policies

Configuration: Confirmed SNAT and DNAT functionality through testing

Security Benefit: Ensures policy-led access in both directions

Developed by: Amr Khaled Saad, Ahmed Mahmoud Mohamed, Youssef Hosseny Mohamed, Youssef Wageh Moawa