Comprehensive Enterprise Network Security & Infrastructure Lab

Architecture, Implementation, and Traffic Analysis

Jackson McCullough

May, 2026

Abstract

This technical report details the design, deployment, and administration of a multi-network cybersecurity lab environment. The project was engineered to simulate a modern enterprise network architecture, focusing on defense-in-depth methodologies. Core implementations include rigorous VLAN segmentation, stateful firewall rule management, Access Control List (ACL) enforcement, secure service deployment, and centralized traffic analysis utilizing Splunk as a Security Information and Event Management (SIEM) solution. The resulting infrastructure provided a robust platform for hands-on validation of enterprise network security controls, threat detection, and incident response procedures.

Contents

1 Introduction

Modern enterprise environments necessitate resilient and strictly segmented network architectures to mitigate the risk of lateral movement during a cyber intrusion. This lab was constructed to bridge theoretical networking concepts with practical, hands-on administration of security controls. The primary objective was to build a complete, multi-tiered network from the ground up, enforcing the principle of least privilege at the network layer while ensuring comprehensive visibility into intra-network and ingress/egress traffic.

By integrating network routing, firewall configurations, and endpoint log aggregation, this lab serves as a dynamic testing ground for identifying vulnerabilities and validating the effectiveness of applied countermeasures.

2 Network Architecture and Topology

To accurately replicate a corporate infrastructure, the network was divided into distinct security zones utilizing Virtual Local Area Networks (VLANs). A core Layer 3 switch facilitated inter-VLAN routing, with all traffic traversing security boundaries inspected by a centralized next-generation firewall (NGFW).

2.1 VLAN Segmentation & IP Addressing Strategy

The IP schema was designed utilizing a hierarchical Class A private IP space (`10.0.0.0/8`), subnetted to isolate broadcast domains and logical business units.

Table 1: VLAN Configuration and Subnet Allocation

VLAN ID	Zone Name	Subnet	Purpose & Security Posture
VLAN 10	Management	10.1.10.0/24	Highly restricted. Hosts hypervisor management interfaces, firewall web UI, and SIEM administration.
VLAN 20	Server Farm	10.1.20.0/24	Internal corporate servers (Active Directory, internal DNS, File Shares). No direct outbound internet access.
VLAN 30	User Endpoints	10.1.30.0/24	Simulated employee workstations. Subject to strict web filtering and egress ACLs.
VLAN 40	DMZ (External)	10.1.40.0/24	Public-facing services (Web server, external DNS proxy). Isolated from all internal VLANs.

2.2 Infrastructure Components

The virtualized infrastructure was provisioned using a Type-1 hypervisor, deploying the following core components:

- **Edge/Core Firewall:** pfSense / OPNsense virtual appliance acting as the primary gateway, NAT provider, and inter-VLAN filter.
- **Switching Structure:** Open vSwitch handling 802.1Q VLAN tagging.
- **SIEM Server:** Ubuntu Server hosting a Splunk Enterprise instance.
- **Endpoints:** Windows 10/11 VMs for the user segment and Windows Server 2022 for directory services.

3 Implementation and Configuration

3.1 Layer 2 & Layer 3 Segmentation

The foundational step involved configuring 802.1Q trunking between the virtual switch and the firewall appliance. Subinterfaces were created on the firewall to act as the default gateway for each respective VLAN. This ”router-on-a-stick” configuration ensured that no two VLANs could communicate without the traffic being explicitly evaluated by the firewall's ruleset.

```
interface GigabitEthernet0/1
 description TRUNK-TO-FIREWALL
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,40
 spanning-tree portfast trunk
```

Listing 1: Example Switch Trunk Configuration (Cisco IOS equivalent logic used in vSwitch)

3.2 Firewall Rule Management and ACL Enforcement

A default-deny policy was implemented across all interfaces. Rules were iteratively added based on the operational requirements of the simulated enterprise.

3.2.1 Access Control Policy Examples

1. **DMZ Isolation:** Traffic originating from VLAN 40 (DMZ) destined for RFC 1918 internal addresses was explicitly dropped, preventing a compromised web server from pivoting into the Server Farm (VLAN 20).

2. **DNS/NTP Restrictions:** User Endpoints (VLAN 30) were forced to utilize the internal AD DNS server. An ACL dropped all outbound UDP/TCP port 53 traffic originating from VLAN 30 endpoints that attempted to reach external DNS servers (e.g., 8.8.8.8), preventing DNS tunneling exfiltration.

3. **Management Access:** SSH (TCP 22) and HTTPS (TCP 443) access to network appliances and server infrastructure were restricted exclusively to jump boxes located in VLAN 10.

3.3 Secure Service Deployment

To emulate a hardened environment, critical network services were deployed with security best practices:

- **Active Directory (AD):** Configured with LDAP signing requirements. SMBv1 and NTLMv1 were explicitly disabled via Group Policy Objects (GPOs) to prevent Pass-the-Hash and relay attacks.
- **Web Server (DMZ):** Deployed an Nginx reverse proxy terminating TLS 1.3. Cryptographic configurations disabled legacy cipher suites
- **Secure Shell (SSH):** Linux servers were configured to reject password authentication, requiring ED25519 cryptographic keys. The `PermitRootLogin` directive was set to `no`.

4 Traffic Analysis and SIEM Integration with Splunk

A critical requirement of this lab was achieving full visibility into network flows and endpoint behaviors. Splunk Enterprise was deployed in VLAN 10 to aggregate, parse, and correlate logs.

4.1 Log Forwarding Architecture

- **Network Telemetry:** The edge firewall was configured to forward syslog events (firewall blocks, NAT translations, DHCP leases) to Splunk via UDP 514. Suricata (IDS/IPS) logs were formatted as JSON and sent over to track potential intrusion attempts.
- **Endpoint Logs:** Splunk Universal Forwarders were deployed to the Windows Server and User Endpoints. Sysmon (System Monitor) was installed on the endpoints using the SwiftOnSecurity configuration to capture process creation (Event ID 1), network connections (Event ID 3), and registry modifications (Event ID 12).

4.2 Threat Hunting and Dashboarding

Custom Splunk dashboards were built to visualize the security posture in real-time. Several Search Processing Language (SPL) queries were engineered to detect anomalous behavior.

```
index=firewall sourcetype=pfsense:filter action=blocked
| stats count by src_ip, dest_ip, dest_port
| eventstats sum(count) as total_blocks by src_ip
| where total_blocks > 100
| sort - total_blocks
| table src_ip, dest_ip, dest_port, count, total_blocks
```

Listing 2: Splunk SPL Query: Detecting Excessive Firewall Denies (Potential Port Scan)

This specific query successfully detected a simulated Nmap scan originating from a rogue internal device, flagging the source IP for rapid quarantine.

5 Testing and Validation

To validate the efficacy of the implemented controls, several penetration testing techniques were simulated:

- **Lateral Movement Simulation:** Executed an ICMP sweep and TCP port scan from a compromised User Endpoint (VLAN 30). *Result:* The firewall successfully dropped traffic destined for the Management VLAN (10). Splunk generated an alert based on the high volume of dropped packets.
- **Brute Force Attack:** Simulated an SSH dictionary attack against an internal server. *Result:* Splunk correlated the repeated failed authentication attempts in the Linux `auth.log` and triggered a high-severity alert dashboard widget.

6 Conclusion

The construction and administration of this multi-network cybersecurity lab successfully demonstrated the practical application of enterprise network security controls. By architecting isolated VLANs, rigorously enforcing ACLs, and adhering to strict firewall rule management, the attack surface of the simulated enterprise was drastically reduced. Furthermore, the deployment of secure services and the integration of Splunk for granular traffic analysis provided invaluable hands-on experience in both proactive infrastructure hardening and reactive threat detection. This project serves as a comprehensive foundation for understanding the complexities of defending modern enterprise networks against persistent cyber threats.