ANSIBLE

Threat Surface Analysis & Network Segmentation Strategy

Generated: October 24, 2025 at 04:56 PM  
Classification: CONFIDENTIAL - Security Analysis  
Distribution: Security Team, Architecture Team, Compliance

# Table of Contents

1. Executive Threat Summary

2. Attack Surface Analysis

3. Attack Paths & Lateral Movement Risks

4. Tier-Based Threat Assessment

5. Comprehensive Segmentation Strategy

5.1 Tier-Based Segmentation

5.2 Data Privacy Zones

5.3 External Customer Impact Zones

5.4 Single Point of Failure Analysis

5.5 Compliance-Based Segmentation

5.6 Micro-Segmentation Recommendations

6. Firewall Rules & Access Control Lists

7. Remediation Recommendations

# Executive Threat Summary

This document presents a comprehensive security analysis of the ANSIBLE application,

identifying attack surfaces, threat vectors, and providing detailed micro-segmentation strategies.

## Critical Security Metrics

|  |  |
| --- | --- |
| Total Attack Paths Identified | 8793 |
| Exposed Network Nodes | 256 |
| Critical Assets at Risk | 8793 |
| Average Attack Distance (hops) | 5.79 |
| High Threat Nodes | 512 |

# Attack Surface Analysis

## External Exposure

**CRITICAL FINDING:** 8 flows to external/internet destinations detected.

|  |  |  |  |
| --- | --- | --- | --- |
| Destination IP | Port | Protocol | Risk Level |
| 172.16.1.50 | 1433.0 | TCP | LOW |
| 10.164.92.180 | nan | UDP | LOW |
| 172.16.1.51 | 8080.0 | TCP | MEDIUM |
| 172.16.1.52 | 8080.0 | TCP | MEDIUM |
| 1.0.0.1 | 8080.0 | TCP | MEDIUM |
| 172.16.1.52 | 80.0 | TCP | MEDIUM |
| 172.16.1.51 | 5432.0 | TCP | LOW |
| 172.16.1.50 | 443.0 | TCP | MEDIUM |

# Attack Paths & Lateral Movement Risks

Identified 100 potential attack paths that could allow lateral movement from Web tier to sensitive Database tier.

## High-Risk Attack Paths (Top 10)

**Attack Path #1: [HIGH]**

* Source: 10.164.105.112 (WEB)
* Target: 10.164.116.109 (DATABASE)
* Path Length: 2 hops
* Attack Vector: External → Database (SQL Injection, Data Exfiltration)

**Attack Path #2: [HIGH]**

* Source: 10.164.105.41 (WEB)
* Target: 10.164.116.237 (DATABASE)
* Path Length: 2 hops
* Attack Vector: External → Database (SQL Injection, Data Exfiltration)

**Attack Path #3: [HIGH]**

* Source: 10.164.105.203 (WEB)
* Target: 10.164.116.238 (DATABASE)
* Path Length: 2 hops
* Attack Vector: External → Database (SQL Injection, Data Exfiltration)

**Attack Path #4: [HIGH]**

* Source: 10.164.105.74 (WEB)
* Target: 10.164.116.216 (DATABASE)
* Path Length: 2 hops
* Attack Vector: External → Database (SQL Injection, Data Exfiltration)

# Comprehensive Segmentation Strategy

This section provides extensive segmentation and micro-segmentation recommendations based on multiple security criteria.

## 5.1 Tier-Based Segmentation

**DMZ / Web Tier [HIGH]**

|  |  |
| --- | --- |
| Allowed Inbound | Internet (80/443), Load Balancer |
| Allowed Outbound | Application Tier only |
| Explicit Denies | Direct database access, SSH from internet |
| Purpose | Public-facing web servers |

**Application Tier [HIGH]**

|  |  |
| --- | --- |
| Allowed Inbound | Web Tier only |
| Allowed Outbound | Database Tier, External APIs |
| Explicit Denies | Internet access (except whitelisted APIs) |
| Purpose | Business logic and API servers |

**Database Tier [CRITICAL]**

|  |  |
| --- | --- |
| Allowed Inbound | Application Tier only |
| Allowed Outbound | None (data should not egress) |
| Explicit Denies | All other access, especially from Web Tier |
| Purpose | Data persistence and storage |

## 5.2 Data Privacy Zones

Segmentation based on data classification and privacy requirements:

|  |  |  |  |
| --- | --- | --- | --- |
| Zone | Data Type | Criticality | Compliance |
| PII Zone | Personally Identifiable Information | CRITICAL | GDPR, CCPA |
| PHI Zone | Protected Health Information | CRITICAL | HIPAA |
| PCI Zone | Payment Card Industry Data | CRITICAL | PCI-DSS |
| Confidential Zone | Business confidential data | HIGH | Internal Policy |
| Public Zone | Public-facing non-sensitive data | LOW | None |

## 5.3 External Customer Impact Zones

Segmentation based on customer-facing impact and business criticality:

|  |  |  |  |
| --- | --- | --- | --- |
| Impact Tier | Description | Priority | Recovery Objectives |
| Tier 0 - Customer Critical | Direct customer-facing services | CRITICAL | RTO: 15 min, RPO: 0 |
| Tier 1 - Customer Support | Customer support systems | HIGH | RTO: 1 hour, RPO: 15 min |
| Tier 2 - Internal Operations | Internal business systems | MEDIUM | RTO: 4 hours, RPO: 1 hour |
| Tier 3 - Non-Critical | Development/test systems | LOW | RTO: 24 hours, RPO: 4 hours |

## 5.4 Single Point of Failure Analysis

Identified single points of failure requiring redundancy and segmentation:

|  |  |  |  |
| --- | --- | --- | --- |
| Tier | Server Count | SPOF Risk | Recommendation |
| App | 4 | LOW | Verify load balancer configuration |
| Database | 5 | LOW | Verify load balancer configuration |
| Web | 3 | LOW | Verify load balancer configuration |

## 5.5 Compliance-Based Segmentation

Segmentation strategies aligned with regulatory compliance requirements:

**PCI-DSS - Payment Card Data**

* Requirements: Segment cardholder data environment (CDE) from rest of network, implement strong access controls

**HIPAA - Healthcare Data**

* Requirements: Segregate PHI systems, implement audit logging, encrypt data in transit and at rest

**SOX - Financial Systems**

* Requirements: Separate financial reporting systems, implement change controls and audit trails

**GDPR - EU Personal Data**

* Requirements: Data residency controls, right to deletion capabilities, breach notification systems

**NIST 800-53 - Federal Systems**

* Requirements: Boundary protection, least privilege access, continuous monitoring

## 5.6 Micro-Segmentation Recommendations

Detailed micro-segmentation strategies for enhanced security:

1. Application-Level Segmentation

Isolate each application into its own VLAN/subnet

1. Process-Level Segmentation

Use containers/namespaces to isolate individual processes

1. User-Based Segmentation

Segment based on user roles (admin, developer, end-user)

1. Time-Based Segmentation

Restrict access during off-hours, maintenance windows

1. Geo-Based Segmentation

Segment based on geographic location, data residency

1. Device-Based Segmentation

Separate mobile, desktop, server, IoT devices

1. Zero Trust Segmentation

Implement identity-based, least-privilege micro-perimeters

# Remediation Recommendations

## Priority 1 - Immediate Actions

1. 1. Block all direct Web-to-Database connections
2. 2. Implement network-based intrusion detection (IDS/IPS)
3. 3. Enable logging on all firewall rules and network flows

## Priority 2 - Short Term (30 days)

1. 1. Deploy micro-segmentation for database tier
2. 2. Implement application-aware firewall rules
3. 3. Conduct penetration testing on attack paths

## Priority 3 - Long Term (90 days)

1. 1. Migrate to Zero Trust Architecture
2. 2. Implement Software-Defined Perimeter (SDP)
3. 3. Deploy behavioral analytics and anomaly detection