Enterprise Network Segmentation Analysis

Comprehensive Assessment of Network Architecture & Segmentation Strategy

Generated: October 24, 2025  
Applications Analyzed: 145  
Total Network Flows: 11,172  
Classification: CONFIDENTIAL - Executive Summary

# Table of Contents

1. Executive Summary

2. Enterprise Network Overview

2.1 Application Portfolio Analysis

2.2 Network Flow Statistics

2.3 Infrastructure Inventory

3. Current State Assessment

3.1 Network Topology Analysis

3.2 Application Dependencies Map

3.3 External Exposure Points

4. Segmentation Analysis

4.1 Tier-Based Segmentation

4.2 Data Classification Zones

4.3 Compliance Requirements

4.4 Geographic Distribution

5. Risk Assessment

5.1 Attack Surface Analysis

5.2 Lateral Movement Risks

5.3 Single Points of Failure

6. Segmentation Recommendations

6.1 Immediate Actions (0-30 days)

6.2 Short-Term Strategy (30-90 days)

6.3 Long-Term Roadmap (90+ days)

7. Implementation Roadmap

8. Success Metrics & KPIs

# 1. Executive Summary

This document presents a comprehensive analysis of the enterprise network infrastructure, **covering 145 applications** and 11,172 network flows. The analysis identifies critical security gaps, proposes a detailed network segmentation strategy, and provides a roadmap for achieving Zero Trust Network Architecture.

## Key Findings

|  |  |
| --- | --- |
| Total Applications | 145 |
| Total Servers/Nodes | 3,436 |
| Total Network Flows | 11,172 |
| Application Dependencies | 4 |
| External Exposure Points | 59 |
| Unique Protocols | 20 |

# 2. Enterprise Network Overview

## 2.1 Application Portfolio Analysis

The enterprise network consists of 145 distinct applications, ranging from

customer-facing web services to internal business systems and data storage platforms.

### Top 20 Applications by Flow Volume

|  |  |  |
| --- | --- | --- |
| Rank | Application | Flow Count |
| 1 | I3SQL | 201 |
| 2 | DM\_CMREG | 195 |
| 3 | DSAA | 189 |
| 4 | DM\_WMAHR | 188 |
| 5 | DM\_RDOM | 183 |
| 6 | DM\_CMRDB | 178 |
| 7 | DM\_CORD | 173 |
| 8 | DNESR | 167 |
| 9 | DM\_SBADJ | 162 |
| 10 | DNCCS | 159 |
| 11 | DM\_CMDAT | 141 |
| 12 | DM\_CCRMBZ | 139 |
| 13 | DM\_BLZE | 137 |
| 14 | DM\_CMDF | 136 |
| 15 | DM\_DNCCW | 136 |
| 16 | IVR | 132 |
| 17 | DM\_LEDAT | 131 |
| 18 | CMAR | 117 |
| 19 | DM\_BAP | 116 |
| 20 | DPAPI | 116 |

## 2.2 Network Flow Statistics

|  |  |  |  |
| --- | --- | --- | --- |
| Flow Direction | Count | Percentage | Risk Level |
| Internal | 6 | 0.1% | LOW |
| Outbound (App-to-App) | 9 | 0.1% | MEDIUM |
| External (Internet) | 59 | 0.5% | HIGH |
| TOTAL | 11,172 | 100% | - |

# 3. Current State Assessment

## 3.1 Network Topology Analysis

Current network topology analysis reveals:

* [CRITICAL] 59 flows to external/internet destinations
* [HIGH] 4 application dependencies create complex attack surface
* [MEDIUM] 3,436 unique servers require segmentation

# 4. Segmentation Analysis

## 4.1 Tier-Based Segmentation

Recommended segmentation by application tier:

|  |  |  |  |
| --- | --- | --- | --- |
| Tier | Purpose | Criticality | Isolation Level |
| DMZ/Edge | Public-facing services | HIGH | Strong (VLAN + FW) |
| Web Tier | Web application servers | HIGH | Strong (VLAN + FW) |
| App Tier | Business logic | HIGH | Medium (VLAN) |
| Data Tier | Databases & storage | CRITICAL | Maximum (VLAN + FW + ACL) |
| Management | Admin & monitoring | CRITICAL | Strong (Dedicated Network) |

# 6. Segmentation Recommendations

## 6.1 Immediate Actions (0-30 days)

1. Deploy Network Access Control Lists (ACLs) to block unauthorized tier-to-tier communication
2. Implement firewall rules to restrict direct Web-to-Database connections
3. Enable comprehensive network flow logging across all applications
4. Identify and catalog all external-facing services
5. Deploy network intrusion detection systems (IDS) at tier boundaries

## 6.2 Short-Term Strategy (30-90 days)

1. Implement VLAN-based segmentation for all application tiers
2. Deploy application-aware firewall rules based on flow analysis
3. Establish micro-segmentation for database tier
4. Implement jump servers for administrative access
5. Deploy security groups for cloud-based applications
6. Begin Zero Trust Network Architecture (ZTNA) pilot program

## 6.3 Long-Term Roadmap (90+ days)

1. Complete enterprise-wide Zero Trust Network Architecture deployment
2. Implement Software-Defined Perimeter (SDP) for all applications
3. Deploy Identity-Aware Proxy (IAP) for application access
4. Implement continuous network behavior analytics
5. Deploy automated micro-segmentation based on application behavior
6. Achieve full network visibility with NDR (Network Detection & Response)

# 7. Implementation Roadmap

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Phase | Timeline | Milestone | Effort | Priority |
| Phase 1 | Week 1-2 | Network discovery & flow analysis | Low | P0 |
| Phase 1 | Week 2-3 | Deploy basic ACLs | Medium | P0 |
| Phase 1 | Week 3-4 | Enable logging & monitoring | Low | P0 |
| Phase 2 | Month 2 | VLAN segmentation - Web tier | High | P1 |
| Phase 2 | Month 2 | VLAN segmentation - App tier | High | P1 |
| Phase 2 | Month 2-3 | VLAN segmentation - DB tier | High | P0 |
| Phase 2 | Month 3 | Deploy tier-boundary firewalls | Medium | P1 |
| Phase 3 | Month 4 | Micro-segmentation pilot | High | P1 |
| Phase 3 | Month 4-5 | ZTNA pilot program | High | P2 |
| Phase 3 | Month 5-6 | SDP deployment | Very High | P2 |
| Phase 4 | Month 6+ | Enterprise-wide ZTNA rollout | Very High | P2 |
| Phase 4 | Ongoing | Continuous optimization | Medium | P3 |

# 8. Success Metrics & KPIs

Track the following metrics to measure segmentation effectiveness:

|  |  |  |
| --- | --- | --- |
| KPI | Current Baseline | Target (6 months) |
| Unauthorized tier-to-tier flows | 59 | < 100 |
| External exposure points | 59 | < 29 |
| Mean time to detect (MTTD) breaches | Unknown | < 5 minutes |
| Segmentation coverage | 0% | > 95% |
| Micro-segmented applications | 0 | 72 |
| Zero Trust adoption | 0% | > 50% |
| Attack surface reduction | 0% | > 70% |
| Lateral movement prevention | 0% | > 90% |
| Firewall rule optimization | 0% | > 80% |
| Compliance score | TBD | > 90% |