Threat Surface Analysis  
ACDA

**Application: ACDA**Security Zone: DATA\_TIER  
Generated: October 17, 2025  
Classification: Confidential

Prepared by: Network Security Team  
Auto-generated by Network Segmentation Analyzer v3.0

# Executive Summary

This document analyzes the security posture of ACDA and provides actionable recommendations specific to your application. Focus on the issues and action items highlighted in this document - they are tailored to your application's actual network traffic and configuration.

## Your Application at a Glance

|  |  |
| --- | --- |
| **Security Zone** | DATA\_TIER |
| **Total Dependencies** | 14 |
| **External Services** | 0 |
| **Internal Services** | 3 |
| **DNS Issues Found** | 0 |

## Key Findings for Your Application

* ✓ Data tier - requires strict access controls and monitoring
* ✓ 14 dependencies - manageable complexity
* ✓ No DNS configuration issues detected

## Top 3 Priority Actions for Your Team

* **1.** Enable database activity monitoring and audit logging

# Your Application Architecture

ACDA operates in the DATA\_TIER security zone and communicates with the following services based on observed network traffic:

## Service Dependencies

### Cache (1)

* • cache\_service

### Database (2)

* • database\_service
* • 2001:db8:2bda:f8d3:8d72:48e2:951f:58d0

### Message Queue (1)

* • message\_queue\_service

### Other Apis (1)

* • other\_apis\_service

### Unknown (9)

* • 10.164.116.238
* • 10.164.116.109
* • 10.100.160.174
* • 10.100.160.82
* • 10.165.116.139
* • 10.164.145.191
* • 10.164.116.216
* • 10.164.105.128
* • 10.164.145.111

## Communication Patterns

Based on network flow analysis, ACDA exhibits the following communication patterns:

* Connects to 2 database(s)
* Uses 1 cache service(s) for performance

# Security Findings for Your Application

This section highlights specific security issues identified for your application based on network traffic analysis and DNS validation.

## DNS Configuration Issues

**✓ Good news!** No DNS configuration issues detected for your application.

## Network Exposure

**✓ Your application is in the Data Tier (not internet-facing).**

* Ensure the following controls are in place:
* • Only accessible from application tier
* • Database activity monitoring enabled
* • Encrypted connections (TLS)
* • Regular backup and recovery testing

## Dependency Security Review

# Action Plan for Your Team

This action plan is specific to ACDA. Work with your network and security teams to implement these recommendations.

## Immediate Actions (This Week)

* ⚠ Enable database activity monitoring and audit logging

## Short-Term Actions (Next 30 Days)

* ◆ Document all application dependencies and communication patterns
* ◆ Implement service-to-service authentication (mTLS or API keys)
* ◆ Configure network monitoring and alerting for your application
* ◆ Review and update firewall rules based on actual traffic patterns
* ◆ Implement rate limiting and throttling for API endpoints

## Long-Term Improvements (Next 90 Days)

* ○ Implement automated security scanning in CI/CD pipeline
* ○ Deploy runtime application self-protection (RASP)
* ○ Establish disaster recovery and business continuity plans
* ○ Conduct regular penetration testing and security assessments
* ○ Implement security metrics and KPI tracking

# Required Firewall Rules

The following firewall rules are required for ACDA based on observed network traffic. Work with your network team to implement these rules.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Direction** | **Source** | **Destination** | **Port/Protocol** | **Purpose** |
| OUTBOUND | ACDA | database\_service | TCP/5432 | Communication with database |
| OUTBOUND | ACDA | cache\_service | TCP/6379 | Communication with cache |
| OUTBOUND | ACDA | message\_queue\_service | TCP/443 | Communication with message\_queue |
| OUTBOUND | ACDA | other\_apis\_service | TCP/443 | Communication with other\_apis |
| OUTBOUND | ACDA | 10.164.116.238 | TCP/443 | Communication with unknown |
| OUTBOUND | ACDA | 10.164.116.109 | TCP/443 | Communication with unknown |
| OUTBOUND | ACDA | 10.100.160.174 | TCP/443 | Communication with unknown |
| OUTBOUND | ACDA | 10.100.160.82 | TCP/443 | Communication with unknown |
| OUTBOUND | ACDA | 10.165.116.139 | TCP/443 | Communication with unknown |
| OUTBOUND | ACDA | 10.164.145.191 | TCP/443 | Communication with unknown |
| OUTBOUND | ACDA | 10.164.116.216 | TCP/443 | Communication with unknown |
| OUTBOUND | ACDA | 10.164.105.128 | TCP/443 | Communication with unknown |
| OUTBOUND | ACDA | 10.164.145.111 | TCP/443 | Communication with unknown |
| OUTBOUND | ACDA | 2001:db8:2bda:f8d3:8d72:48e2:951f:58d0 | TCP/5432 | Communication with database |

**Important:** These rules should be implemented with a default-deny policy. All traffic not explicitly allowed should be blocked and logged.