**White Paper: Zero Trust Architecture (ZTA)**

Principles, Design, and Implementation for the Modern Enterprise (VA Context)

White Paper: Zero Trust Architecture (ZTA) – Principles, Design, and Implementation for the Modern Enterprise (VA Context)

## Executive Summary

The traditional network perimeter model is inadequate in today’s VA environment, where users, data, and workloads span on-premises and multi-cloud systems. Zero Trust Architecture (ZTA) mandates a model of continuous verification and context-aware access, eliminating implicit trust regardless of network location. This paper expands on key principles, VA-relevant designs, implementation strategies, and tools aligning ZTA to NIST SP 800-207 and the CISA ZTA Maturity Model.

1. Core Principles of Zero Trust Architecture

## 1.1 'Never Trust, Always Verify'

- This principle eliminates the assumption that users or systems within the VA's internal network are inherently trustworthy.

- Every access request must be authenticated, authorized, and encrypted, regardless of origin.

- Context-awareness includes evaluating device health (via EDR), user behavior (via SIEM), and risk level at each request.

- VA staff, contractors, and services (e.g., Lambda functions or Kubernetes pods) are all subject to verification.

- References: NIST SP 800-207, CISA Zero Trust Maturity Model.

## 1.2 Least Privilege Access

- Restricts user and system access to only what is necessary for the job function or application requirement.

- Example: Read-only scoped tokens to access MPI records, ensuring no write/delete unless explicitly granted.

- IAM role assumption with time-limited access is enforced via IAM Identity Center (AWS) or Conditional Access (Azure).

- Enhances mitigation against lateral movement and privilege escalation attacks.

- Additional Info: Principle of Least Privilege in NIST 800-53 AC family controls.

## 1.3 Micro-Segmentation

- Splits network resources into logical zones or segments to prevent lateral threat movement.

- Used to isolate BGS from VA Profile or EHR subsystems unless policy permits communication.

- Enforced through AWS Security Groups, CrowdStrike firewall rules, or Kubernetes service mesh (Istio).

- Enables fine-grained inspection and policy enforcement per communication path.

2. ZTA Design Considerations

## 2.1 Identity as the New Perimeter

- Identity becomes the primary control surface replacing traditional firewall boundaries.

- Identity Providers (IdPs): Azure AD, Okta, or PingFederate integrate with SAML, OIDC, or SCIM.

- Multi-factor authentication (MFA) is mandatory across VA OIT assets.

- Access decisions are dynamically evaluated through RBAC (role-based) or ABAC (attribute-based).

- For example, an identity token may be evaluated for user role, location, and device compliance status.

- Reference: VA Handbook 6500 IAM requirements.

## 2.2 Policy Enforcement Points (PEPs)

- PEPs are systems or software components that enforce access control decisions at runtime.

- Deployed across:

- API gateways (e.g., Kong, AWS API Gateway with Lambda authorizers)

- Network layer (AWS Network Firewall, Azure Firewall)

- Application runtime (sidecars in Kubernetes using Istio + Envoy)

- PEPs ingest contextual trust signals (risk score, IP reputation) and apply policies via OPA or IAM constructs.

## 2.3 Telemetry and Continuous Monitoring

- Telemetry ensures visibility into actions, anomalies, and threats.

- Logs from endpoints, API calls, firewall activity, and user behavior feed into SIEM platforms:

- Splunk and Azure Sentinel aggregate and correlate security events.

- AWS CloudTrail and GuardDuty detect behavioral anomalies.

- EDR tools (e.g., CrowdStrike Falcon, Microsoft Intune) validate device posture and enforce quarantine if out-of-policy.

- Monitoring is central to both detection and continuous evaluation under Zero Trust.

3. Implementation Strategy

## 3.1 ZTA Pilots and Phased Adoption

- ZTA rollouts should begin with low-risk, high-value use cases:

- Example: Limiting third-party contractor access to Salesforce using conditional access and device health checks.

- Key controls:

- Identity federation using VA IdPs

- Conditional Access policies for risk-adaptive responses

- Device posture checks integrated with endpoint compliance tools

- Red/Blue teams simulate attacks and detection as part of the CRISP (Continuous Readiness Information Security Program) evaluation.

## 3.2 Mapping ZTA to Cloud Environments

- In AWS:

- IAM Identity Center for SSO and scoped role delegation

- Cognito for user pools and federated identities

- API Gateway enforces token verification and policy-based routing

- KMS encrypts data and enforces key usage policies

- In Azure:

- Conditional Access and Defender for Cloud Apps monitor and block anomalous sessions

- Intune enforces MDM/MAM on endpoint devices

- In Hybrid:

- Okta or PingFederate brokers authentication between on-prem (e.g., BGS) and cloud services

- ZTNA proxies or VPN replacements enforce encrypted tunnels and access control

4. ZTA Maturity and Assessment

## 4.1 CISA ZTA Maturity Model

- Maturity stages:

- Traditional: Flat network, broad access, perimeter firewall

- Advanced: Segmented access, basic continuous auth

- Optimal: Adaptive access decisions, automation, telemetry feedback loops

- VA CRISP reviews map current controls across five pillars:

- Identity, Device, Network, Application, and Data

- Progression measured through ZTA capability benchmarking and control scoring.

## 4.2 NIST SP 800-207 Reference Architecture

- Key components:

- Policy Decision Point (PDP): Makes access decisions based on policies and signals

- Policy Enforcement Point (PEP): Enforces PDP outcomes (e.g., block, allow, elevate challenge)

- Data Plane & Telemetry Layer: Captures logs, risk signals, user activity

- VA examples:

- PDP implemented via OPA (Open Policy Agent) in container platforms

- PEP integrated with API Gateway + Lambda Authorizer

- CRISP dashboard surfaces telemetry from SIEMs, CloudTrail, and Intune for audit and policy refinement

5. Tools and Technologies

## | Function | Tools / Services |

|---------------------|-------------------------------------------------------------|

| Identity | Azure AD, Okta, AWS IAM, PingFederate |

| Segmentation | AWS Security Groups, Azure NSG, Istio |

| Enforcement | Cloudflare, Zscaler, AWS API Gateway + OPA |

| Monitoring | Splunk, Azure Sentinel, CrowdStrike Falcon, AWS GuardDuty |

| Endpoint Compliance | Microsoft Intune, Jamf, CrowdStrike Falcon |

## Conclusion

ZTA is more than a cybersecurity posture – it's a security transformation. For the VA, implementing Zero Trust safeguards sensitive Veteran data while enabling scalable and secure modernization of services like VA.gov, Salesforce, and internal claims platforms. Anchoring access in verifiable identity, segmenting by design, and enforcing continuous risk evaluation ensures a breach-aware and resilient infrastructure.

## Next Steps:

- Define critical assets and access boundaries for phased ZTA rollout.

- Map all cloud and on-prem apps to identity-based controls.

- Configure IAM federation across cloud providers and VA data centers.

- Instrument telemetry feeds into Splunk/Sentinel and CRISP for observability.

- Conduct periodic ZTA maturity assessments using the CISA model and adjust roadmaps accordingly.