Security Lab GRC Documentation

NIST SP 800-207 Zero Trust Architecture Alignment

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE



HOMELAB
DEVSECOPS PLATFORM

Created By: Paul Leone

April 7, 2026

Table of Contents

NIST SP 800-207 Zero Trust Architecture Alignment 2
Version 2.0: Change Log (from v1.0, January 2026) 2
Zero Trust Architecture Implementation Overview 4
Zero Trust Tenets Implementation 4
NIST SP 800-207 Logical Components 7
Data Sources for Policy Decisions 8
ZTA Deployment Model Assessment 11
ZTA Use Case Alignment 12
Threats and Mitigations 14
Deployment Maturity Assessment 16
Framework Alignment 17
Version History 17

NIST SP 800-207 Zero Trust Architecture Alignment

Document Control:

Version:	**2.0**
Last Updated:	April 2026
Owner:	Paul Leone
Prior Version:	1.0: January 2026

Version 2.0: Change Log (from v1.0, January 2026)

Cloud workload content integrated directly into each section. Cloud node inventory: AWS (2 nodes: Amazon Linux 2 EC2 t3.micro, Windows Server 2025 EC2 c7i-flex.large), Azure (2 nodes: Ubuntu 24.04 LTS Standard_B2ats_v2, Windows Server 2025 Standard_E2s_v3 Spot), GCP (2 nodes: Debian 13.4 e2.micro, Ubuntu e2.micro): 6 nodes total. All nodes connected via Tailscale WireGuard mesh VPN (tailf07c05.ts.net) with no public management ports exposed.

Section	Item	Change	Impact
Tenets	**Tenet 1**	Asset inventory expanded to include 6 cloud nodes across AWS, GCP, and Azure tracked via Checkmk, Wazuh, and PatchMon over Tailscale. Cloud VPC/VNet topology and Tailscale mesh routing tables added as resource documentation.	Implemented
Tenets	**Tenet 2**	Tailscale WireGuard (ChaCha20-Poly1305) added as mandatory encryption layer for all cloud-to-on-premises management traffic. AWS Security Groups, GCP VPC firewall policy (Google Threat Intelligence blocking), and Azure NSG enforce default-deny perimeter for cloud nodes. No public management ports on any cloud instance.	Implemented
Tenets	**Tenet 3**	Cloud node session controls added: SSH key-only access (passwords disabled globally via Ansible), 30-minute session timeout applied to cloud console sessions via provider MFA policy. Windows cloud nodes subject to same 30-minute Authentik timeout via domain join.	Implemented
Tenets	**Tenet 4**	Cloud-native dynamic policy sources added: AWS GuardDuty (ML-based behavioral detection), GCP Security Command Center (asset and threat findings), Azure Defender for Cloud and Sentinel (KQL detection rules). All	Implemented

		findings forwarded to on-premises SIEM via Wazuh agent telemetry.	
Tenets	**Tenet 5**	Wazuh CIS SCA extended to all 6 cloud nodes daily. PatchMon daily CVE correlation for 4 Linux cloud nodes. WSUS manages 2 Windows cloud nodes. AWS Inspector, GCP SCC vulnerability assessment, Azure Defender for Cloud provide supplemental cloud-native scanning.	Implemented
Tenets	**Tenet 6**	Cloud node authentication added: SSH Ed25519 key-only for Linux nodes; Kerberos via domain join for Windows nodes; Tailscale device-bound WireGuard for all management paths. Cloud console access enforces provider MFA independently.	Implemented
Tenets	**Tenet 7**	Cloud telemetry added: AWS CloudTrail, GCP Admin Activity/Data Access logs, Azure Activity Log and Monitor. Wazuh agents on all 6 cloud nodes forward endpoint events to on-premises Splunk. AWS VPC flow logs, GCP VPC flow logs, Azure NSG flow logs supplement on-premises pfSense flow data.	Implemented
Logical Components	**Policy Engine**	Cloud-native PE sources added: GuardDuty, SCC, and Sentinel findings feed policy decisions via Wazuh agent telemetry to on-premises SIEM. Cloud provider security scores (Security Hub, SCC, Defender for Cloud Secure Score) inform posture.	Implemented
Logical Components	**Policy Enforcement Point**	Cloud PEP added: AWS Security Groups + Tailscale ACL (agent/gateway model), GCP VPC firewall policy + Cloud Armor (enclave gateway), Azure NSG + DDoS Protection plan (enclave gateway). No public inbound ports on any cloud node.	Implemented
Use Cases	**Use Case 2**	Multi-cloud/cloud-to-cloud use case advanced from Medium to high applicability. Tailscale mesh connects AWS (172.31.0.0/16), GCP (10.128.0.0/16), and Azure (10.130.0.0/16) into unified overlay. Cloud nodes access on-premises Wazuh, DNS, PatchMon, Checkmk via Tailscale. Same Authentik OIDC policies enforced.	Implemented
Maturity	**Overall**	Overall ZTA maturity remains Advanced. Cloud integration strengthens evidence for Tenets 1, 2,	Implemented

	5, 7 and PEP deployment model. No new gaps introduced; existing gaps unchanged.

Zero Trust Architecture Implementation Overview

This cybersecurity lab demonstrates comprehensive Zero Trust Architecture (ZTA) principles aligned with NIST SP 800-207 and CISA Zero Trust Maturity Model v2.0. The implementation achieves Advanced maturity (Stage 3 of 4) across core Zero Trust pillars through explicit verification of every access request, least-privilege enforcement via RBAC, assume-breach mentality with continuous monitoring, and encrypt-everything policies using modern cryptographic standards. Version 2.0 extends the ZTA scope to a hybrid multi-cloud architecture spanning AWS (us-east-2), Azure (North Central US), and GCP (us-central1), with 6 cloud nodes integrated into the same device agent/gateway enforcement model applied to on-premises infrastructure.

Zero Trust Tenets Implementation

Tenet	Implementation	Status
Tenet 1: All Data Sources and Computing Services as Resources	Lab treats all assets as resources requiring explicit authentication/authorization. 25+ physical hosts, 50+ containers, 30+ VMs, network devices (pfSense, OPNsense, Traefik), storage systems, and cloud-hosted services all subject to access controls. BYOD consideration planned via Authentik device flow and Wazuh compliance validation. Small footprint devices (IoT sensors, network monitors) send data through authenticated channels to aggregators. Cloud extension: 6 cloud nodes across AWS (Amazon Linux 2 EC2 t3.micro, Windows Server 2025 EC2 c7i-flex.large), Azure (Ubuntu 24.04 LTS Standard_B2ats_v2, Windows Server 2025 Standard_E2s_v3), GCP (Debian 13.4 e2.micro, Ubuntu e2.micro) enrolled in Checkmk, Wazuh, and PatchMon as explicit managed resources. Cloud VPC/VNet topology and Tailscale mesh routing tables document all cloud resource relationships. Evidence: Proxmox inventory, Docker container registry, Wazuh agent deployment (31+ endpoints), NetAlertX network discovery, Checkmk infrastructure monitoring.	Advanced
Tenet 2: All Communication Secured Regardless of Network Location	Network location provides no implicit trust. TLS 1.3 mandatory for all web services (Traefik enforcement), SSH encrypted with Ed25519 certificates, VPN encryption via WireGuard/OpenVPN, syslog-ng TLS for log transmission. Internal traffic treated identically to external: Authentik ForwardAuth validates all requests regardless of source VLAN. Step-CA PKI provides certificate-based authentication for service-to-service communication. Cloud extension: Tailscale WireGuard (ChaCha20-Poly1305) is the mandatory encryption layer for all cloud-to-on-premises management traffic: no plaintext management paths on any cloud node. AWS Security Groups	Advanced

	enforce default-deny with explicit Tailnet-only inbound rules. GCP VPC firewall policy (17 rules) includes Google Threat Intelligence blocking for TOR exit nodes, known malicious IPs, and sanctioned countries. Azure NSG homelab-nsg2 enforces explicit allow-list with DenyAllInBound at priority 65500. Evidence: Traefik middleware configuration, syslog-ng TLS certificates, Step-CA issuance logs, VPN encryption audit logs, cloud provider firewall rule documentation.	
Tenet 3: Per-Session Resource Access with Least Privilege	Access granted per-session via Authentik OAuth2/OIDC with 30-minute session timeouts requiring re-authentication. OAuth2 scopes limit permissions to minimum operations. SSH sessions use temporary sudo elevation with explicit justification. No persistent elevated privileges: all access time-limited and activity-specific. Traefik ForwardAuth validates each request independently. Cloud extension: SSH key-only access for all 4 Linux cloud nodes (passwords disabled globally via Ansible); Windows cloud nodes (AWS, Azure) subject to 30-minute Authentik session timeout via domain join. No public management ports exist: all cloud access requires active Tailscale session with device-bound key. Cloud IAM instance profiles (AWS), service accounts (GCP), and Managed Identities (Azure) scoped to minimum required actions with no wildcard permissions. Evidence: Authentik session timeout logs, OAuth2 scope configurations, sudo elevation audit logs, Traefik access validation per-request.	Advanced
Tenet 4: Dynamic Policy Based on Observable State	Policy engine (Authentik) evaluates user identity, group membership, device compliance (Wazuh status), source IP reputation, time-of-day restrictions, MFA verification, and behavioral patterns. Policies adapt based on threat intelligence (MISP correlation), failed authentication patterns, geoIP anomalies. Environmental attributes include network location, reported active attacks, device patch level. Cloud extension: AWS GuardDuty provides ML-based behavioral detection (VPC flow logs, CloudTrail, DNS query logs) as an additional observable state source feeding policy decisions. GCP Security Command Center delivers asset and threat findings informing cloud node posture. Azure Defender for Cloud and Sentinel (KQL detection rules: NSG deny-inbound spikes, Entra ID sign-in from new geographic location, unexpected domain join events, AMA data gaps) provide cloud-layer dynamic intelligence. All cloud findings forwarded to on-premises Splunk via Wazuh agent telemetry for unified policy correlation. Evidence: Authentik policy configurations incorporating Wazuh compliance data, Splunk behavioral analytics, MISP threat correlation logs, cloud-native security service findings.	Advanced

Tenet 5: Monitor and Measure All Asset Integrity	Wazuh agents on 25+ on-premises endpoints provide real-time compliance validation against CIS Benchmarks (92-98% compliance). Nessus authenticated scans monthly, Ansible drift detection, container health checks, VM monitoring via Proxmox. Non-compliant devices quarantined to remediation VLAN. CDM-like capabilities via PatchMon (5,000+ packages tracked), vulnerability correlation to NVD, automated patch workflows. Cloud extension: Wazuh CIS SCA extended to all 6 cloud nodes daily: policies applied: CIS Amazon Linux (Amazon Linux 2), CIS Debian 12/13 (Debian 13.4), CIS Ubuntu 22.04/24.04 (Ubuntu nodes), CIS Windows Server 2025 (both Windows cloud nodes). PatchMon daily CVE correlation for 4 Linux cloud nodes. WSUS manages 2 Windows cloud nodes with automated approval workflows. AWS Inspector, GCP SCC vulnerability assessment, Azure Defender for Cloud recommendations provide supplemental cloud-native scanning. Critical less than 72h MTTR SLA maintained across all 31+ endpoints. Evidence: Wazuh SCA reports (on-premises + cloud), Nessus scan results, PatchMon vulnerability tracking, Ansible compliance playbooks, automated quarantine workflows.	Advanced
Tenet 6: Dynamic Authentication and Authorization	Authentik provides dynamic ICAM with MFA (TOTP, FIDO2/WebAuthn planning), OAuth2/OIDC integration, LDAP/SAML support. Continuous evaluation via session timeouts, behavioral monitoring (Splunk analytics), threat-triggered re-authentication. Asset management via Wazuh, NetAlertX, Checkmk. Policy-based re-authentication on resource changes, time-based intervals, anomalous activity detection. Cloud extension: all 4 Linux cloud nodes authenticate via SSH Ed25519 keys distributed by Ansible: passwords disabled globally, no shared credentials. Windows cloud nodes (AWS, Azure) authenticate via domain Kerberos over Tailscale, subject to same AD Group Policy and account lockout (5 failed attempts, 10-minute lockout). Cloud console access (AWS, GCP, Azure) independently enforces provider MFA. No cloud management path exists without active device-bound Tailscale session. Evidence: Authentik MFA enforcement logs, re-authentication triggers in SIEM, behavioral anomaly detection alerts, dynamic policy application.	Advanced
Tenet 7: Collect and Use Security Posture Data	Comprehensive telemetry: Wazuh endpoint data, Suricata/Snort network IDS, pfSense flow logs, Traefik access logs, DNS queries, Prometheus metrics, application logs. Data processed in dual SIEM (Splunk + Elastic) with correlation, behavioral analytics, threat hunting. Insights improve policy via monthly reviews, automated IOC blocking, vulnerability-driven patching. Cloud	Advanced

	extension: AWS CloudTrail captures all management events (IAM role assumptions, Security Group modifications, EC2 lifecycle events) delivered to S3 with SSE. GCP Admin Activity logs (always-on, cannot be disabled) and Data Access audit logs capture all resource changes. Azure Activity Log and Monitor record all ARM deployments. AWS VPC flow logs, GCP VPC flow logs, Azure NSG flow logs supplement on-premises pfSense flow data. Wazuh agents on all 6 cloud nodes forward endpoint security events to on-premises Splunk via Tailscale: unified telemetry pipeline regardless of infrastructure location. Evidence: SIEM ingestion rates (100% security events on-premises + cloud), cloud-native log retention (90 days matching on-premises), Wazuh cloud agent dashboard, cloud provider flow log configuration.	

NIST SP 800-207 Logical Components

Component	Implementation	Status
Policy Engine (PE)	Authentik serves as primary PE, evaluating access requests against enterprise policy, user attributes, device compliance (Wazuh integration), threat intelligence (MISP), behavioral baselines (Splunk), and environmental factors. Trust algorithm considers identity confidence, device posture, request context, historical behavior, current threat landscape. Trust algorithm type: Hybrid score-based and criteria-based, contextual evaluation considering subject history, access patterns, anomaly detection. Cloud extension: AWS GuardDuty ML-based behavioral detection, GCP Security Command Center findings, and Azure Sentinel KQL detection rules serve as additional PE data sources. Cloud provider security posture scores (AWS Security Hub score, GCP SCC security health, Azure Defender for Cloud Secure Score) inform cloud node trust level. All cloud-native findings forwarded to on-premises SIEM and surfaced in Authentik-adjacent policy decisions. Evidence: Authentik policy logs, access decision audit trails, Wazuh compliance integration, Splunk behavioral correlation, cloud security service dashboards.	Advanced
Policy Administrator (PA)	Authentik PA configures communication paths via Traefik middleware, generates OAuth2 tokens, manages session lifecycles, coordinates with Step-CA for certificate-based authentication. Controls session establishment/termination based on PE decisions and ongoing monitoring. Cloud extension: Tailscale admin console serves as cloud PA: managing ACL policy (default deny, explicit allow), node	Advanced

	enrollment/revocation, and subnet route advertisement for all cloud nodes. Changes to cloud ACL policy follow same Git version-control review process as on-premises IaC changes. Evidence: OAuth2 token generation logs, session establishment/teardown events, Traefik dynamic configuration updates, Step-CA certificate issuance coordination, Tailscale audit logs.	
Policy Enforcement Point (PEP)	Multi-component PEP architecture. Client-side: Authentik ForwardAuth integration in browsers, SSH certificate-based authentication, Wazuh agent compliance reporting, VPN device authentication. Resource-side: Traefik reverse proxy, pfSense/OPNsense firewalls, SafeLine WAF, service-specific gateways. Control plane: isolated management network for PE/PA/PEP communication. Data plane: application traffic on segregated VLANs. Deployment model: Hybrid agent/gateway (Authentik + Traefik), enclave gateway (DMZ services), resource portal (web applications). Cloud extension: cloud PEP deployed per provider: AWS: Tailscale ACL (agent/gateway) + Security Groups (enclave gateway); GCP: Tailscale ACL (agent/gateway) + VPC firewall policy with Google Threat Intelligence + Cloud Armor three-tier WAF/DDoS (enclave gateway); Azure: Tailscale ACL (agent/gateway) + NSG homelab-nsg2 + DDoS Protection plan homelab-ddos (enclave gateway). No public inbound management ports on any cloud node: PEP enforcement is the only access path. Evidence: Traefik ForwardAuth logs, firewall rule enforcement, WAF block rates, SSH certificate validation, VLAN isolation configs, cloud provider firewall rule documentation.	Advanced

Data Sources for Policy Decisions

Data Source	Implementation	Status
Continuous Diagnostics and Mitigation (CDM)	Wazuh provides CDM capabilities: vulnerability assessment, FIM, rootkit detection, CIS Benchmark compliance (SCA), patch management via PatchMon integration. Nessus authenticated scans complement. Ansible enforces configurations, detects drift. Container/VM monitoring via Proxmox and Docker health checks. Cloud extension: Wazuh CDM capabilities extended to all 6 cloud nodes: same FIM paths, rootkit detection, and SCA policies applied. PatchMon agents on 4 Linux cloud nodes provide daily package-level CDM data. WSUS provides Windows CDM for 2 Windows cloud nodes. AWS Inspector, GCP SCC, Azure Defender for Cloud provide cloud-native CDM data supplementing Wazuh.	Advanced

	Evidence: Wazuh vulnerability reports, compliance scan results (92-98%), PatchMon package tracking (5,000+ packages), Ansible drift detection alerts.	
Industry Compliance System	Policy framework aligned with CIS Benchmarks, NIST 800-53 controls, PCI-DSS requirements (where applicable), ISO 27001 standards. Wazuh SCA enforces CIS policies, vulnerability remediation follows NIST guidelines, encryption standards per NIST/PCI-DSS. Cloud extension: AWS Security Hub assesses CIS AWS Foundations Benchmark. Azure Defender for Cloud Secure Score tracks compliance against NIST SP 800-53 and CIS Azure Foundations. GCP SCC security health analytics validates GCP-specific CIS controls. Evidence: CIS Benchmark compliance reports, control mapping documentation, policy version control (Git), quarterly compliance reviews.	Advanced
Threat Intelligence Feeds	MISP threat intelligence platform correlates IOCs across network logs, endpoint telemetry, application data. Splunk integrates feeds for correlation. Suricata/Snort use threat signatures. GeoIP databases identify suspicious locations. Cortex analyzers (VirusTotal, Hybrid Analysis) provide malware analysis. Cloud extension: AWS GuardDuty integrates Amazon threat intelligence for ML-based detection of VPC flow, CloudTrail, and DNS anomalies. GCP VPC network firewall policy embeds Google Cloud Threat Intelligence as priority 100-130 rules (TOR exit nodes, malicious IPs, sanctioned countries). Azure Sentinel threat intelligence connectors feed KQL detection rules with real-time IOC correlation. Evidence: MISP IOC correlation logs, automated IOC blocking (Wazuh Active Response), threat intelligence-driven alerts, cloud-native threat intelligence integration.	Advanced
Network and System Activity Logs	Dual SIEM architecture (Splunk + Elastic) aggregates 100% security events: authentication logs, firewall traffic, DNS queries (Unbound/Technitium DNS), web access (Traefik), endpoint events (Wazuh), network IDS (Suricata), infrastructure metrics (Prometheus). Real-time correlation detects multi-stage attacks, lateral movement, data exfiltration patterns. Cloud extension: AWS CloudTrail (all management events, S3 with SSE), GCP Admin Activity logs (always-on), Azure Activity Log all forwarded to on-premises Splunk via Wazuh agents. AWS VPC flow logs (fl-03179f74e54bf1aa4 to CloudWatch Logs), GCP VPC flow logs (Flow Analyzer), Azure NSG flow logs (Network Watcher homelab-nsg2) supplement on-premises pfSense/Suricata data. Evidence: SIEM ingestion statistics,	Advanced

	correlation rule effectiveness, alert volumes, retention compliance (90-day hot, 1-year cold).	
Data Access Policies	RBAC via Authentik groups mapped to resource permissions. Filesystem ACLs, database role-based permissions, application-level authorization. Policies encoded in Authentik, enforced via Traefik middleware, validated quarterly. Sensitivity-based policies (Public, Internal, Confidential, Restricted) with handling requirements. Cloud extension: AWS IAM instance profiles enforce least-privilege data access (no wildcard actions, no long-lived access keys on EC2). GCP service accounts use minimal roles (no owner/editor on Compute instances). Azure RBAC scoped per resource group. Tailscale ACL policy governs all inter-node data access paths. Evidence: Authentik RBAC configurations, quarterly access reviews, policy documentation (version-controlled), filesystem/database ACL audits.	Advanced
Enterprise PKI	Step-CA provides automated certificate lifecycle: issuance, renewal, rotation (90-day lifetimes). SSH certificate-based authentication, TLS certificates for services, mutual TLS planning. Integration with Authentik for identity certificates. No reliance on external CA for internal services. Cloud extension: cloud nodes receive certificates via Step-CA over Tailscale: same ACME provisioner used for on-premises services. Ansible cert-manager playbooks distribute trust anchors to cloud Linux nodes. Windows cloud nodes receive certificates via Active Directory Certificate Services (dc02.home.com, Windows Server 2025 EnterpriseCA) through domain join over Tailscale. Evidence: Step-CA issuance logs, certificate rotation compliance, SSH cert validation logs, TLS certificate inventory.	Advanced
ID Management System	Authentik serves as authoritative identity source: user accounts, attributes, group memberships, device identities, service accounts. LDAP/OAuth2/OIDC/SAML support for federated identity. Integration with Step-CA for certificate binding. Account lifecycle management with automated provisioning/deprovisioning. Cloud extension: Linux cloud nodes managed via Ansible SSH key distribution (same centralized lifecycle as on-premises). Windows cloud nodes domain-joined to home.com via Tailscale: AD provides Kerberos, Group Policy, WSUS, and certificate auto-enrollment. AWS IAM roles, GCP service accounts, and Azure Entra ID accounts inventoried with 45-day dormancy review. Evidence: Authentik user database, group assignment logs, federated identity configurations, account lifecycle audit trails.	Advanced

SIEM System	Dual architecture: Splunk (primary analytics) and Elastic (secondary/redundancy) collect security-centric data for policy refinement, attack detection, forensics. 90-day hot retention, 1-year cold storage. Dashboards track vulnerabilities, patch compliance, authentication patterns, threat indicators. Alerts feed TheHive case management, Shuffle SOAR orchestration. Cloud extension: Wazuh Universal Forwarder from all 6 cloud nodes forwards to on-premises Splunk via Tailscale. AWS GuardDuty and Azure Sentinel incidents auto-create TheHive cases via Shuffle SOAR webhook. GCP SCC findings trigger alerting policy notifications routed to Discord/email. Cloud node telemetry visible in same Splunk dashboards as on-premises: unified single-pane-of-glass view. Evidence: SIEM correlation rules (100+ active), dashboard usage, alert-to-incident conversion rates, retention compliance, SOAR integration workflows.	Advanced

ZTA Deployment Model Assessment

Model	Implementation	Status
Primary Model: Device Agent/Gateway (Hybrid)	Authentik acts as central policy administrator. Client-side enforcement via browser-based ForwardAuth (no installed agent for web resources), SSH certificate agents for terminal access. Resource-side gateways include Traefik (web services), pfSense/OPNsense (network perimeter), SafeLine WAF (application layer). Strengths: no required client software for web access (BYOD-friendly), centralized policy management, defense-in-depth with multiple gateway layers. Weaknesses: limited endpoint visibility for non-enterprise devices, cannot enforce compliance before web access attempts, relies on network controls for non-web protocols. Cloud extension: Tailscale serves as the cloud agent/gateway: device-bound WireGuard keys enforce identity at the network layer before any cloud resource access. All 6 cloud nodes enforce this model with no exceptions. Evidence: Traefik ForwardAuth integration across 50+ services, SSH certificate distribution via Ansible, gateway configuration management, Tailscale node inventory.	Advanced
Secondary Model: Enclave-Based	DMZ services protected by enclave gateway (pfSense), application tier isolated behind Traefik, backend services (databases, SIEM, PKI) on dedicated VLANs with restricted access. Cloud extension: each cloud provider implements an independent enclave gateway: AWS Security Groups enforce default-deny per VPC; GCP VPC network firewall policy	Advanced

	(homelab, 17 rules) with Google Threat Intelligence blocking protects all Compute instances; Azure NSG homelab-nsg2 applied at subnet level with DenyAllInBound default; GCP Cloud Armor three-tier WAF/DDoS policies add edge, backend, and application-level enclave protection. Evidence: 3-tier architecture (DMZ, application, backend), VLAN isolation with firewall enforcement, gateway placement protecting service enclaves, cloud provider firewall documentation.	
Tertiary Model: Resource Portal	Web-based access to services via Traefik reverse proxy acting as portal. No client agents required. Authentication/authorization at portal before proxying to resources. Used for contractor access, cross-organization collaboration, public-facing authenticated services. Cloud extension: Traefik resource portal extended to cloud-hosted services where applicable. Cloudflare Tunnels provide zero-trust resource portal for external-facing cloud services: no inbound ports exposed, all access proxied through Cloudflare edge. Evidence: Traefik portal configurations, authentication workflows, contractor access logs, session management, Cloudflare Tunnel configuration.	Advanced

ZTA Use Case Alignment

Use Case	Implementation	Applicability
Use Case 1: Enterprise with Satellite Facilities (Remote Workers)	Tailscale mesh VPN provides secure remote access without traditional VPN concentrator. Authentik authenticates remote users, validates device compliance via Wazuh remote agent data. Cloud-ready architecture (Authentik cloud planning) enables direct cloud resource access without hairpinning through on-premises infrastructure. Cloud extension: cloud nodes (AWS EC2, Azure VM, GCP Compute) act as additional satellite facilities: same Tailscale mesh, same Wazuh compliance validation, same Authentik policy applies regardless of whether a node is on-premises or in a cloud provider. Evidence: Tailscale deployment, remote Wazuh agent reporting, Authentik MFA enforcement for remote sessions.	High
Use Case 2: Multi-Cloud/Cloud-to-Cloud	Applicability advanced from Medium to High. Tailscale mesh VPN connects all three cloud providers (AWS 172.31.0.0/16, GCP 10.128.0.0/16, Azure 10.130.0.0/16) and on-premises infrastructure in a unified overlay network. Cloud nodes can reach on-premises Wazuh Manager (192.168.1.219), DNS resolvers	High

	(192.168.1.153/154), PatchMon backend (192.168.200.0/24), and Checkmk server (192.168.1.126) via Tailscale without public internet exposure. Same Authentik OIDC policies, same CIS SCA baselines, same patch SLAs enforced across all providers. AWS GuardDuty, GCP SCC, and Azure Sentinel provide provider-native detection alongside on-premises SIEM. Evidence: Tailscale node inventory (9 enrolled nodes), subnet router advertisement table, cloud VPC/VNet topology documentation, unified PatchMon dashboard.	
Use Case 3: Contracted Services/Nonemployee Access	Open guest network with internet access but no enterprise resource visibility. Authentik provides time-limited contractor accounts with restricted resource access. Smart building systems isolated on dedicated VLAN, accessible only to vendor service accounts with MFA. Visitor devices cannot discover internal resources (SDP principles). Cloud extension: cloud contractor access scoped via Tailscale ACL tags: explicit per-node allow rules required; no implicit mesh access. Time-limited Tailscale pre-authorized keys for contractor cloud node access. Evidence: Guest VLAN isolation, contractor account lifecycle, vendor MFA enforcement, network segmentation.	High
Use Case 4: Cross-Enterprise Collaboration	Authentik supports OAuth2/OIDC/SAML federation, enabling cross-organization collaboration. Can establish federated trust with partner identity providers. Resource-specific policies grant external user access to designated collaboration resources while denying access to other systems. Cloud extension: cloud provider identity federation available: AWS IAM Identity Center, GCP Workload Identity Federation, Azure Entra ID B2B: provides cross-enterprise identity without credential sharing. Evidence: Authentik federation capabilities, external identity source configurations, resource-specific policy enforcement.	Medium
Use Case 5: Public/Customer-Facing Services	Public web services use Traefik with optional authentication. No enforcement of device posture for anonymous public access. Registered user portals (future) could enforce password policies, optional MFA, browser type validation. Metadata collection for attack detection (rate limiting, browser fingerprinting, bot detection). Cloud extension: GCP Cloud Armor provides public-facing WAF with Google Threat Intelligence and	Low

	DDoS protection for any cloud-hosted public services. Azure DDoS Protection plan homelab-ddos protects Azure VNet. Evidence: Traefik rate limiting, WAF rules blocking automated attacks, access pattern analysis.

Threats and Mitigations

Threat	Mitigations	Risk Level
Threat 1: Subversion of ZTA Decision Process	Authentik access restricted to dedicated administrator accounts with MFA. All configuration changes logged to SIEM with alerting. Git version control for policy configurations with approval workflow. Quarterly access reviews for administrative privileges. Authentik deployed on hardened, isolated systems with minimal attack surface. Cloud extension: cloud IAM policy changes (AWS CloudTrail, GCP Admin Activity, Azure Activity Log) alert on any PE/PA-equivalent modification. Tailscale admin console access enforces provider MFA. Evidence: Admin account audit logs, SIEM alerting on policy changes, Git commit history, privilege review documentation.	High
Threat 2: Denial-of-Service or Network Disruption	HA firewall cluster (pfSense CARP) with less than 5-second failover. Dual DNS (Unbound/Technitium DNS) with automatic failover. Dual SIEM architecture (Splunk + Elastic) for resilience. Redundant internet connections with automatic failover. Load balancing via Traefik across multiple backends. Cloud extension: GCP Cloud Armor three-tier DDoS protection (rate limiting at edge, backend, and application layers). Azure DDoS Protection plan (homelab-ddos) protects Azure VNet. AWS Security Group rate limiting. Cloud provider native DDoS mitigation operates independently of on-premises HA cluster. Evidence: Failover testing logs, uptime statistics, redundant service configurations, cloud DDoS protection configuration.	Medium
Threat 3: Stolen Credentials/Insider Threat	MFA enforcement (TOTP current, FIDO2/WebAuthn planned) reduces credential theft impact. Contextual trust algorithm detects anomalous behavior (unusual times, locations, access patterns). Session timeouts (30 minutes) limit exposure window. Behavioral analytics (Splunk) identify compromised account indicators. Least privilege limits blast radius. Lateral movement prevention via network segmentation, least privilege. Cloud extension: no passwords on cloud SSH nodes (key-only); Windows cloud nodes require domain Kerberos. Azure Sentinel KQL rule detects Entra ID sign-in from new geographic location. AWS GuardDuty CredentialAccess	Medium

	findings detect IAM credential misuse. Evidence: MFA enforcement logs, behavioral anomaly alerts, session timeout enforcement, privilege restriction audit logs.	
Threat 4: Visibility Limitations on Encrypted Traffic	Metadata collection from encrypted sessions (source, destination, timing, volume). Certificate inspection for TLS connections. DNS query logging identifies suspicious domains even with encrypted payloads. Endpoint visibility via Wazuh agents provides process-level context. Network behavior analysis detects anomalies without decryption. Cloud extension: AWS VPC flow logs, GCP VPC flow logs, Azure NSG flow logs capture encrypted traffic metadata (source/destination/port/action) for all cloud node communications. GuardDuty DNS query log analysis detects DGA domains and C2 callbacks within encrypted tunnels. Evidence: Flow log analysis, DNS-based threat detection, endpoint telemetry correlation, encrypted traffic metadata dashboards.	Low-Medium
Threat 5: Stored Data Compromise	SIEM data, network diagrams, configuration files stored with encryption at rest (AES-256). Access to security data repositories restricted to security team with MFA. Configuration management tools (Ansible, Terraform) protected with vault encryption. Most restrictive access policies on security infrastructure components. Regular access reviews for security data access. Cloud extension: AWS S3 CloudTrail logs with SSE (server-side encryption). GCP persistent disks and GCS buckets encrypted at rest (Google-managed keys). Azure Managed Disks and Log Analytics workspace homelab-log encrypted at rest by default. Evidence: Encryption-at-rest configurations, access restriction logs, security data access audit trails.	Medium
Threat 6: Vendor Lock-in/Proprietary Formats	Open-source focus (Authentik, Wazuh, Traefik, Suricata) reduces vendor lock-in. Standard protocols (OAuth2, OIDC, SAML, LDAP) enable interoperability. Infrastructure-as-code (Terraform, Ansible) allows migration to alternative platforms. Multi-vendor approach for critical functions (dual SIEM, multiple authentication methods). Regular evaluation of alternative solutions. Cloud extension: multi-cloud deployment across AWS, GCP, and Azure reduces single-provider dependency. Tailscale as transport layer is provider-agnostic: cloud nodes can be migrated between providers without changing the ZTA enforcement model. Evidence: Open-source tool selection, standard protocol usage, IaC repositories, vendor diversity in architecture.	Medium

Threat 7: Automated Agent/NPE Compromise	Service account credentials stored in Vaultwarden with automated retrieval. API keys rotated quarterly with automated expiration. Service account activity logged and monitored for anomalies. Principle of least privilege for automation accounts (read-only where possible). Automated agent authentication via certificate-based methods (Step-CA). Cloud extension: AWS EC2 instance profiles replace service account passwords (no long-lived access keys on any cloud node). GCP uses Workload Identity-compatible service accounts with minimal roles. Azure Managed Identity for service-to-service authentication without credentials. Ansible automation uses SSH key authentication for all cloud node access. Evidence: Service account activity logs, API key rotation schedules, certificate-based automation authentication, anomaly detection for NPE accounts.	Medium

Deployment Maturity Assessment

Overall NIST ZTA Maturity: Advanced

Strengths

- Comprehensive implementation of ZT tenets 1-7 with cloud scope extending all tenets to hybrid infrastructure.
- Mature logical component deployment (PE, PA, PEP) extended to cloud via Tailscale ACL, provider-native firewall policies, and Wazuh compliance validation.
- Rich data sources for policy decisions (CDM, threat intel, SIEM, PKI, IAM) now include cloud-native sources (GuardDuty, SCC, Defender for Cloud).
- Hybrid deployment model supporting diverse use cases: Use Case 2 (Multi-Cloud) advanced from Medium to High applicability.
- Strong threat mitigation posture with cloud-specific mitigations for all 7 identified threats.
- Open standards and interoperability focus: Tailscale, Wazuh, and Ansible are provider-agnostic across all three cloud platforms.

Gaps to Optimal

- Device agents for comprehensive endpoint coverage on all cloud node types.
- Full passwordless authentication (FIDO2/WebAuthn) across on-premises and cloud.
- Continuous authentication beyond session-based model.
- Machine learning/UEBA for predictive analytics: cloud-native ML (GuardDuty, Sentinel) partially fills this for cloud nodes.
- Mutual TLS (mTLS) for all service-to-service communication including cloud workloads.
- Just-in-time access provisioning enterprise-wide.
- Hardware security modules for critical key material.
- Azure Spot instance eviction automation (manual restart documented, automated restart workflow pending).

Recommended Priorities Q2-Q3 2026

- FIDO2/WebAuthn deployment for passwordless MFA (on-premises and cloud console).
- Trivy/Grype for comprehensive SBOM tracking across on-premises and cloud node packages.
- UEBA capabilities in SIEM platforms: supplement GuardDuty/Sentinel ML for on-premises behavioral analytics.
- Mutual TLS for all service-to-service communication.
- Azure Spot instance restart automation via Azure Automation or ARM template trigger.
- Formal federated identity program for cross-enterprise collaboration (Use Case 4).

Framework Alignment

Framework	Alignment
NIST SP 800-207	Advanced maturity: all 7 ZT tenets implemented across on-premises and hybrid cloud scope.
NIST RMF	Access policies risk-based, continuous monitoring aligned, cloud node risk assessment integrated.
FICAM	Strong identity governance, MFA enforcement, lifecycle management extended to cloud IAM.
TIC 3.0	Network security capabilities aligned, PEP-based enforcement: cloud nodes use provider-native PEP equivalents.
CDM	Mature diagnostics and mitigation via Wazuh/PatchMon, extended to all cloud nodes.
Cloud Smart	Full hybrid deployment demonstrated: AWS, Azure, GCP nodes with consistent ZTA enforcement.

Version History

Version	Date	Changes
1.0	January 2026	Initial release.
2.0	April 2026	Cloud IaaS integration (AWS, Azure, GCP: 6 nodes). Cloud content integrated into Notes column of all relevant controls. Change log added.