ISAUnited
INSTITUTE OF SECURITY ARCHITECTURE UNITED

Defensible 10

Annex A (Normative): D01-Network Security Architecture & Engineering

Technical Standard

Standards Committee
10-29-2025

About ISAUnited

The Institute of Security Architecture United is the first dedicated Standards Development Organization (SDO) focused exclusively on cybersecurity architecture and engineering through security-by-design. As an international support institute, ISAUnited helps individuals and enterprises unlock the full potential of technology by promoting best practices and fostering innovation in security.

Technology drives progress; security enables it. ISAUnited equips practitioners and organizations across cybersecurity, IT operations, cloud/platform engineering, software development, data/AI, and product/operations with vendor-agnostic standards, education, credentials, and a peer community—turning good practice into engineered, testable outcomes in real environments.

Headquartered in the United States, ISAUnited is committed to promoting a global presence and delivering programs that emphasize collaboration, clarity, and actionable solutions to today's and tomorrow's security challenges. With a focus on security by design, the institute champions integrating security into every stage of architectural and engineering practices, ensuring robust, resilient, and defensible systems for organizations worldwide.

Disclaimer

ISAUnited publishes the ISAUnited Defensible 10 Standards Technical Guide to provide informational and educational content regarding security architecture and engineering practices. While efforts have been made to ensure accuracy and reliability, the content is provided “as is,” without any express or implied warranties. This guide is for informational purposes only and does not constitute legal, regulatory, compliance, or professional advice. Consult qualified professionals before making decisions.

Limitation of Liability

ISAUnited - and its authors, contributors, and affiliates - shall not be liable for any direct, indirect, incidental, consequential, special, exemplary, or punitive damages arising from the use of, inability to use, or reliance on this guide, including any errors or omissions.

Operational Safety Notice

Implementing security controls can affect system behavior and availability. First, validate changes in non-production, use change control, and ensure rollback plans are in place.

Third-Party References

This guide may reference third-party frameworks, websites, or resources. ISAUnited does not endorse and is not responsible for the content, products, or services of third parties. Access is at the reader’s own risk.

Use of Normative Terms (“Shall,” “Should,” “Must”)

- Must / Shall: A mandatory requirement for conformance to the standard.
- Must Not / Shall Not: A prohibition; implementations claiming conformance shall not perform the stated action.
- Should: A strong recommendation; valid reasons may exist to deviate in particular circumstances, but the full implications must be understood and documented.

Acceptance of Terms

By using this guide, readers acknowledge and agree to the terms in this disclaimer. If you disagree, refrain from using the information provided.

For more information, please visit our Terms and Conditions page.

License & Use Permissions

The Defensible 10 Standards (D10S) are owned, governed, and maintained by the Institute of Security Architecture United (ISAUnited.org).

Practitioner & Internal Use (Allowed):

- You are free to download, share, and apply this standard for non-commercial use within your organization, departments, or for individual professional, academic, or research purposes.
- Attribution to ISAUnited.org must be maintained.
- You may not modify the document outside of Sub-Standard authorship workflows governed by ISAUnited, excluding the provided Defensible 10 Standards templates and matrices.

Commercial Use (Prohibited Without Permission):

- Commercial entities seeking to embed, integrate, redistribute, automate, or incorporate this standard in software, tooling, managed services, audit products, or commercial training must obtain a Commercial Integration License from ISAUnited.

To request permissions or licensing:
info@isaunited.org

Standards Development & Governance Notice

This standard is one of the ten Parent Standards in the Defensible 10 Standards (D10S) series. Each Parent Standard is governed by ISAUnited's Standards Committee, peer-reviewed by the ISAUnited Technical Fellow Society, and maintained in the Defensible 10 Standards GitHub repository for transparency and version control.

Contributions & Collaboration

ISAUnited maintains a public GitHub repository for standards development. Practitioners may view and clone materials, but contributions require:

- ISAUnited registration and vetting
- Approved Contributor ID
- Valid GitHub username

All Sub-Standard contributions must follow the Defensible Standards Submission Schema (D-SSF) and are peer-reviewed by the Technical Fellow Society during the annual Open Season.

Abstract

The ISAUnited Defensible 10 Standards provide a structured, engineering-grade framework for implementing robust and measurable cybersecurity architecture and engineering practices. The guide outlines the frameworks, principles, methods, and technical specifications necessary for designing, building, verifying, and operating reliable systems.

Developed under the ISAUnited methodology, the standards align with modern enterprise realities, integrating Security by Design, continuous technical validation, and resilience-based engineering to address emerging threats. The guide is written for security architects and engineers, IT and platform practitioners, software and product teams, governance and risk professionals, and technical decision-makers seeking a defensible approach that is testable, auditable, and scalable.

This document includes a series of Practitioner Guidance, Cybersecurity Students & Early-Career Guidance, and Quick Win Playbook callouts.

Practitioner Guidance- Actionable steps and patterns to apply the technical standards in real environments.

Cybersecurity Student & Early-Career Guidance- Compact, hands-on activities that turn each section's ideas into a small, verifiable artifact.

Quick Win Playbook- Immediate, evidence-driven actions that improve posture now while reinforcing good engineering discipline.

Together, these elements help organizations translate intent into engineered outcomes and sustain long-term protection and operational integrity.

Foreword

Message from ISAUnited Leadership

Cybersecurity is at a turning point. As digital systems scale, reactive and checklist-driven practices do not keep pace with adversaries. The ISAUnited position is clear: security must be practiced as engineered design, grounded in scientific principles, structured methods, and defensible evidence. Our mission is to professionalize cybersecurity architecture and engineering with standards that are actionable, testable, and auditable.

ISAUnited Defensible 10 Standards: First Edition is a practical framework for that shift. The standards in this book are not theoretical. They translate intent into measurable specifications, controls, and verification, and enable teams to design and operate resilient systems at enterprise scale.

About This First Edition

This edition publishes ten Parent Standards, one for each of the core domains of security architecture and engineering. Sub-standards will follow in subsequent editions, contributed by ISAUnited members and reviewed by our Technical Fellow Society, to add focused and technology-aligned detail. Adopting the Parent Standards now positions organizations for seamless integration of Sub Standards as they are released on the ISAUnited annual update cycle.

Why “Defensible Standards”

Defensible means the work can withstand technical, operational, and adversarial scrutiny. These standards are designed to be demonstrated with evidence, featuring clear architecture, measurable specifications, and verification, so that practitioners can confidently stand behind their designs.

Contents

Annex A (Normative): D01-Network Security Architecture & Engineering

ISAUnited's Defensible 10 Standards
Parent Standard: D01-Network Security Architecture & Engineering
Document: ISAU-DS-NS-1000
Last Revision Date: October 2025
Peer-Reviewed By: ISAUnited Technical Fellow Society
Approved By: ISAUnited Standards Committee

Section 1. Standard Introduction

The Network Security Architecture & Engineering Parent Standard (ISAU-DS-NS-1000) establishes the engineering baseline for securing enterprise connectivity across campuses, data centers, cloud interconnects, WAN/SD-WAN, and remote access. It defines common terminology, scope, requirements (inputs), technical specifications (outputs), and verification/validation expectations that subordinate sub-standards inherit through flow-downs. The standard is vendor-neutral and implementation-agnostic, aligning with recognized foundational frameworks while extending them with normative, testable guidance. It aims to make network security a built-in property of the architecture—encompassing zoning, boundary controls, secure transport, identity-aware access, and verifiable telemetry—rather than a bolt-on. Applied consistently, it enables defensible, measurable, and auditable network security across on-premises, cloud, and hybrid environments.

Objective

This standard establishes foundational principles for Network Security Architecture & Engineering, ensuring that enterprise network infrastructures are designed and maintained with security resilience, segmentation, and secure interconnectivity in mind. This standard provides a structured and defensible approach to designing, implementing, and governing network architectures that align with modern security engineering principles.

Justification

Network Security Architecture & Engineering is foundational to a defensible cybersecurity posture because the network remains the primary conduit for both legitimate business operations and adversarial activity. In modern enterprise environments—spanning on-premises, cloud, and hybrid architectures—the network serves as the connective tissue, linking users, workloads, and data. As such, it is both a critical asset and a frequent target for attackers seeking to exploit flat topologies, misconfigured segmentation, or insufficient access controls.

Despite advances in endpoint, application, and cloud security, most significant breaches exploit weaknesses in network design, including unsegmented environments, permissive firewall policies, and a lack of continuous identity verification. Traditional perimeter-based models are no longer sufficient, as adversaries routinely bypass or

circumvent legacy controls through lateral movement, credential compromise, or supply chain attacks.

This standard addresses those persistent gaps by mandating a shift from compliance-driven perimeter defenses to engineering-grade, adaptive network architectures. It codifies principles such as business-driven segmentation, zero-trust networking, least-privilege access, and encrypted communications, ensuring that security is not an afterthought but an intrinsic property of network design.

By establishing a defensible, measurable, and resilient network security architecture, this standard enables organizations to reduce risk proactively, contain breaches, and validate their security posture against regulatory requirements and real-world adversarial tactics. It provides the architectural foundation for all subsequent network security standards and controls, supporting the ISAUnited mission to advance cybersecurity as a structured, engineering-driven discipline.

Section 2. Definitions

802.1X — Port-based network access control used by NAC to authenticate devices before link-layer access.

ACL (Access Control List) — Rule set applied to interfaces or objects to permit or deny specific flows by source, destination, protocol, and port.

ADR (Architecture Decision Record) — Short, versioned record of a design decision: problem, options, constraints, trade-offs, decision, invariants, and test/evidence plan.

ATT&CK (MITRE ATT&CK) — Knowledge base of adversary tactics and techniques used to inform testing and validation.

BAS (Breach-and-Attack Simulation) — Automated execution of adversary techniques to validate control effectiveness and detection.

Bastion — Hardened access broker for the management plane, enforcing MFA, JIT, and full session recording.

Blast Radius — Maximum scope of impact if a component or zone is compromised; reduced by effective segmentation and least-privilege paths.

CaC (Configuration-as-Code) — Expression of device and platform configuration as version-controlled code with automated checks and approvals.

Canary/Staged Rollout — Progressive, reversible deployment pattern that limits change impact while collecting health and security signals.
Change Management — Documented, auditable process governing modifications to network and security configurations.

CI/CD (Continuous Integration/Continuous Delivery) — Automated pipelines that build, test, and deploy configurations and policies with peer review and rollback.

CIS Controls v8 — Prescriptive cybersecurity safeguards referenced for control alignment in §9.

Configuration Drift — Deviation between intended (version-controlled) and running configurations; must be detected and remediated.

CSA CCM (Cloud Controls Matrix) — Cloud control framework referenced for control alignment in §9.

Default-Deny / Allow-by-Exception — Policy stance in which all traffic is denied unless an explicit, reviewed rule or contract allows it.

DevSecOps — Integration of security controls and checks into development and operations pipelines.

DDoS (Distributed Denial of Service) — Multi-source flooding or resource-exhaustion attacks impacting availability.

DHCP (Dynamic Host Configuration Protocol) — Core service assigning IP parameters; must be secured and monitored.

DPI (Deep Packet Inspection) — Layer-7 inspection to identify applications, threats, and policy violations.

DNS (Domain Name System) — Core name-resolution service; harden and monitor to prevent abuse and exfiltration.

East-West / North-South Traffic — East-West: internal inter-zone flows. North-South: flows crossing external boundaries.

Evidence Pack (EP-01.x) — Single, hierarchical evidence repository for this annex (parent EP-01, child artifacts EP-01.1, EP-01.2, …) containing plans, proofs, logs, and results referenced in §12.

HA (High Availability) — Redundant patterns (active/active or active/standby) to preserve service continuity.

IaC (Infrastructure-as-Code) — Declarative, version-controlled definitions for infrastructure and network/security policy.

ICD (Interface Control Document) — Record defining an interface's contract: authentication/authorization model, data classification, allowed flows, limits, error handling, telemetry, and invariants.

IdP (Identity Provider) — Authoritative service that authenticates subjects and issues identity claims used in policy evaluation.

Immutable Logging — Write-once or tamper-evident storage of logs and artifacts with authenticated time synchronization and enforced retention.

IPsec — Authenticated and encrypted IP communications (for example, IKEv2/IPsec) for site-to-site, overlay, or management traffic.

IPS (Intrusion Prevention System) — Inline detection and prevention capability often integrated with NGFWs.

ISO/IEC 27001/27002/27033 — Foundational ISO/IEC standards referenced for alignment in §8.

JIT (Just-in-Time) Access — Time-bounded elevation for administrative actions, typically requiring approval and MFA.

KMS (Key Management Service) — Centralized key lifecycle operations used by TLS/mTLS/IPsec and device credentials.

Lateral Movement — Adversary traversal across systems and zones after initial access.
Management Plane Isolation — Dedicated, restricted management networks and interfaces, brokered through a bastion and encrypted channels.

MFA (Multi-Factor Authentication) — Authentication using two or more independent factors.

mTLS (Mutual TLS) — TLS in which both client and server present and validate certificates (service identity).

MTTD / MTTR / MTTC — Mean Time to Detect / Respond (or Recover) / Contain; operational performance metrics.

NAC (Network Access Control) — Identity- and posture-aware admission control (for example, 802.1X, agent checks) granting, restricting, or quarantining access.

NDR (Network Detection and Response) — Detection and investigation based on network telemetry (flows and packets) with response workflows.

NetFlow / IPFIX / PCAP — Flow records (NetFlow/IPFIX) and packet captures (PCAP) for visibility, detection, and forensics.

NGFW (Next-Generation Firewall) — Firewall with application awareness, identity integration, IPS, and advanced inspection.

NIST SP 800-41 / 800-53 / 800-207; NIST CSF 2.0 — Foundational NIST guidance and framework referenced for alignment in §8.

NTP (Network Time Protocol) — Time synchronization for devices and logs; authentication required for evidentiary integrity.

OPA (Open Policy Agent) — Policy-as-code engine used to evaluate and enforce policies in pipelines and at runtime.

OWASP API Security Top 10 — API-focused risk list referenced for control alignment (for example, API2 Broken Authentication).

PaC (Policy-as-Code) — Expression of network and security policy in version-controlled code with automated checks and approvals.

PKI (Public Key Infrastructure) — Certificates, CAs, and policies enabling trust for TLS/mTLS, IPsec, and device identities.

Posture (Device Posture) — Measured security state of a device (for example, OS version, patches, EDR status, disk encryption) used by NAC/ZTNA policy.

RBAC (Role-Based Access Control) — Authorization model granting permissions based on roles; used for device/admin access and flow mediation.

Remote Access (VPN/ZTNA) — Encrypted access patterns for users and partners; ZTNA brokers access by identity and posture.

Red Team / Blue Team — Adversary emulation (red) and defense/response (blue) exercises for validation and improvement.

SD-WAN — Centrally orchestrated WAN overlays using multiple underlays with security and traffic-steering policies.

Secure Network Design — Architecture emphasizing redundancy, segmentation, encrypted communications, governed egress, and automated enforcement.

Segmentation Contract (Inter-Zone Contract) — Explicitly documented, approved communication allowed between zones, including direction, protocol, ports, and identities.

Service Identity — Cryptographic identity for services/workloads (certificates/keys issued by PKI/KMS) used to authenticate peers (for example, mTLS) and authorize flows.

SIEM (Security Information and Event Management) — Central aggregation, normalization, and correlation of logs and telemetry for alerting and investigations.

SSH (Secure Shell) — Encrypted remote administration; strong algorithms and keys required; legacy ciphers disabled.

TLS 1.3 — Recommended transport encryption for external edges and internal services where feasible.

Trust Boundary / Trust Zone — The boundary where differing trust assumptions meet; crossing it requires mediation, authorization, and logging.

VLAN (Virtual LAN) — Logical L2 segmentation domain used to separate broadcast domains and implement zone boundaries.

VPC / VNet — Cloud virtual networks enabling tenant-isolated routing, security controls, and peering.

VPN (Virtual Private Network) — Encrypted overlay (TLS/IPsec) for user or site-to-site connectivity.

WAN — Wide-Area Network interconnecting sites, data centers, and clouds.

ZTNA (Zero Trust Network Access) — Access pattern that grants application or network access based on identity and posture, typically replacing or augmenting VPN.

ZTN (Zero Trust Networking) — Network-centric enforcement of Zero Trust principles (no implicit trust, continuous verification).

Section 3. Scope

Modern enterprise networking spans campus, data center, cloud interconnects, WAN/SD-WAN, and remote access—creating complex, distributed connectivity that demands clear boundaries and defensible engineering practices. The scope of this standard covers enterprise network architectures across on-premises, cloud, and hybrid environments, including remote and third-party access.

This standard defines the architectural expectations and technical guardrails necessary to achieve measurable network resilience. It is designed to help practitioners enforce

access boundaries, contain lateral movement, secure transport, and maintain verifiable observability while supporting business operations at scale.

Applicability

- **Enterprise, Government, and Academic Environments:** Intended for teams designing and operating production networks in regulated and unregulated sectors.
- **Hybrid & Multi-Environment Networks:** Campus, data center, inter-DC, cloud VPC/VNet, WAN/SD-WAN, and remote access (VPN/ZTNA).
- **Brownfield and Greenfield Deployments:** Applies to new builds and incremental modernization programs.
- **Converged IT/OT/IoT Segments:** Guidance for isolating and brokering connectivity to operational technology and IoT where present.

Key Focus Areas

- **Trust Zoning & Segmentation:** Definition and enforcement of L3–L7 segmentation (including micro segmentation) to restrict lateral movement and scope blast radius.
- **Boundary & Egress Controls:** Next-generation firewalling/IPS/DPI at trust boundaries; management-plane isolation; controlled egress with allowlists.
- **Identity-Aware Access:** Network Access Control (e.g., 802.1X/posture), device trust, and Zero Trust enforcement; Just-in-Time/MFA for administrative access.
- **Secure Transport & Cryptography:** TLS 1.3 at edges, mTLS for service-to-service where required, IPsec/SSH for administrative and interconnect channels, with managed PKI/KMS.
- **Telemetry & Observability:** NetFlow/IPFIX/PCAP at boundaries; normalized logs to centralized SIEM with immutable retention and time synchronization.
- **Resilience & Change Control:** Policy-as-code, staged rollouts, rollback, drift detection, and tested failover paths for critical services and routes.
- **Core Network Services Hygiene:** Hardened DNS/DHCP/NTP and routing/security controls appropriate to enterprise contexts.

Outcomes

By defining this scope, the standard ensures that network security architecture is:

- **Defensible:** Built on clear, enforceable boundaries and identity-aware controls.
- **Measurable:** Validated through configuration assessment, traffic testing, and adversary-informed exercises.

- **Adaptive:** Automated and capable of adjusting to topology changes, workload mobility, and evolving threats.
- **Aligned:** Consistent with organizational policy and applicable frameworks and regulations, and designed to integrate with adjacent security domains.

This comprehensive scope provides the foundation for resilient, secure enterprise networking that supports organizational objectives while protecting critical assets and data.

Section 4. Use Case

The following use case illustrates how the Network Security Architecture & Engineering standard can be applied to secure a complex, global enterprise network against lateral movement attacks. It highlights the challenges, technical solutions, and measurable outcomes achieved through the implementation of segmentation, Zero Trust, and advanced threat detection.

Table A-1:

Use Case Name	**Securing a Global Enterprise Network Against Lateral Movement Attacks**
Objective	Mitigate lateral movement risks and improve network security posture through segmentation, Zero Trust, governed egress, and enhanced threat detection.
Scenario	A multinational financial services company faced risk due to a flat network that exposed critical financial systems to lateral movement. Threat actors attempted to pivot internally after compromising endpoints.
Actors	Security Architect, Network Engineer, SOC Analyst, Firewall Administrator, IT Operations Specialist.
Challenges Identified	• Lack of network segmentation (broad internal reachability). • Overly permissive and inconsistent firewall rules. • No Zero Trust enforcement (implicit trust for internal devices). • Limited visibility of east-west traffic. • Uncontrolled egress from sensitive zones. • Management plane reachable from production networks.
Technical Solution	Network Segmentation & Micro-Segmentation: Categorize systems into trust zones (e.g., Finance, HR, DevOps, End-User, Management). Deploy VLAN/software-defined segmentation and enforce default-deny inter-zone policies.

	Zero Trust Networking (ZTN) Principles: Enforce identity-based access with device posture checks (NAC/802.1X). Require JIT and MFA for administrative access; broker application access via ZTNA where applicable. Firewall Rule Optimization & Policy Automation: Audit and remove redundant rules; standardize deny-by-default at ingress, egress, and inter-zone boundaries; express rules as policy-as-code with peer review and drift detection. Egress Governance: Implement zone-specific allowlists; validate egress policies via CI/CD checks and runtime monitoring. Management Plane Isolation: Move device management to dedicated networks reachable only via bastion; require encrypted channels, JIT, MFA, and session recording. Network Visibility & Threat Detection: Deploy NDR for east-west and north-south traffic; centralize firewall and network telemetry in SIEM with immutable retention and authenticated time synchronization. Validation Activities: Use BAS and ATT&CK-informed emulation to test lateral movement controls and detection coverage.
Expected Outcome	Lateral Movement Prevention: Zero successful unauthorized lateral movements in production; ≥ 95% block rate in BAS lateral scenarios. Reduced Attack Surface: ~80% reduction in exposed inter-zone services following segmentation and rule cleanup. Firewall Rule Optimization: ~35% reduction in redundant/obsolete rules; no critical shadowed rules. Detection and Response: MTTD ≤ 10 minutes for boundary/east-west anomalies; MTTC ≤ 30 minutes in tier-1 zones. Management Plane: 100% of device management reachable only through isolated management networks/bastion; direct production access disabled.

Section 5. Requirements (Inputs)

To successfully implement a Defensible Network Security Architecture, organizations must ensure that the following foundational requirements are in place before proceeding with the technical implementation. These inputs represent the critical conditions, resources, and organizational readiness needed to support defensible, measurable, and resilient network security engineering:

5.1 Asset Inventory and Network Mapping

All network-connected assets (devices, systems, endpoints, applications) must be identified, inventoried, and mapped. Maintain up-to-date diagrams showing

logical and physical segmentation, trust boundaries, data flows (north-south and east-west), and declared inter-zone “contracts.” Management networks must be identified distinctly from production networks.

5.2 Business-Driven Network Segmentation
Networks must be logically or physically segmented based on business-critical functions, risk profiles, regulatory requirements, and operational dependencies. Business processes and threat modeling inform segmentation strategies. Define default-deny policies between trust zones and state intended blast-radius limits.

5.3 Firewall and Perimeter Security Strategy
Firewalls and filtering controls must be strategically deployed at ingress, egress, and inter-segment boundaries. Policies default to deny-all, with allow-by-exception, stateful inspection, and routine rule validation. Include egress governance (zone-specific allowlists) and explicitly block management-plane reachability from production networks.

5.4 Zero Trust Implementation Readiness
The organization must be prepared to apply Zero Trust principles across all access requests, including identity verification, risk-based and adaptive authentication, device posture checks, continuous authorization, and session evaluation—regardless of source or location.

5.5 Network Access Control (NAC) Capability
NAC must be available and configured to evaluate identity and device posture (e.g., 802.1X/agent checks) and to grant, restrict, or quarantine access dynamically. Guest/unmanaged device handling is defined and enforced.

5.6 Secure Protocol Usage
Only encrypted and authenticated protocols (e.g., TLS 1.3, IPsec, SSH) are permitted for administrative and data paths. Legacy/insecure protocols are identified for removal or mitigation. PKI/KMS readiness is established (certificate issuance/rotation/revocation), and service identity requirements (e.g., mTLS) are documented where applicable.

5.7 Network Logging and Anomaly Detection Enablement
Comprehensive logging for network devices, boundary controls, and access events is enabled and centralized. Telemetry (e.g., NetFlow/IPFIX/PCAP) is collected at boundaries. Logs are forwarded to a SIEM and/or NDR with anomaly/behavioral analytics. Time synchronization is authenticated (NTP), and retention is immutable/tamper-evident.

5.8 Change Management and Configuration Control
All network and security control changes follow documented, auditable change management processes with peer review, staged rollout, rollback, and configuration drift detection.

5.9 Baseline Documentation and Policy Alignment
Network security policies, segmentation standards, device baselines, and operational runbooks are current, approved, and aligned with organizational risk and compliance objectives. Management-plane isolation, egress policy, and access broker patterns are explicitly captured.

Practitioner Guidance:

Use these requirements as readiness gates before implementing §6 and scheduling tests in §12.

- Map each §5 item to exactly one evidence artifact and one verification/validation test in §12.
- Maintain single sources of truth (one diagram set, one policy set, one repo) to minimize drift.
- Assign clear ownership per item (who approves, who maintains, who audits).

Section 6. Technical Specifications (Outputs)

The following technical specifications outline the measurable, enforceable, and auditable controls necessary to establish a Defensible Network Security Architecture. Each output represents an implementation area that requires validation through an engineering review and operational testing.

Outputs must be:

- **Measurable:** validated by scans, logs, audits, or tests
- **Actionable:** implementation-ready, not policy slogans
- **Aligned:** traceable to §5 Requirements and sub-standards

6.1. Network Segmentation & Isolation
• Implement VLAN-based segmentation, micro-segmentation, and application-aware isolation to restrict lateral movement and contain threats.
• Define and enforce segmentation policies that limit traffic between network zones according to business function, sensitivity, and risk, with zone-specific egress allowlists (default-deny).
• Ensure segmentation is documented, regularly reviewed, and validated through penetration testing and network mapping.

6.2. Firewall Engineering & Network Filtering
• Enforce least-privilege network access using default-deny firewall policies at all

ingress, egress, and inter-segment boundaries.
• Deploy next-generation firewalls (NGFWs) with intrusion prevention systems (IPS) and deep packet inspection (DPI) for real-time threat identification.
• Automate firewall rule management and use policy-as-code with automated analysis to optimize enforcement and reduce redundant or obsolete rules.
• All network device management interfaces (e.g., routers, switches, firewalls, wireless controllers) must be isolated on dedicated management networks and accessed only over secure, encrypted channels (e.g., SSH, TLS VPN, or IPsec).

6.3. Zero Trust Network Design

• Require identity-based authentication for all network connections, with mandatory multi-factor authentication (MFA) and adaptive access policies.
• Deploy Network Access Control (NAC) solutions that dynamically assess device posture, user identity, and risk to grant or restrict network access.
• Continuously re-evaluate and re-authorize devices and users—by identity, posture, and context—regardless of location or network segment.

6.4. Secure Network Protocols & Encryption

• Use only encrypted and authenticated protocols (e.g., TLS 1.3, IPsec, SSH) for both internal and external network communications, including administrative access and inter-service connections.
• All sensitive data in transit, whether internal (east-west) or external (north-south), must be protected using strong encryption. Legacy or insecure protocols (e.g., Telnet, FTP, SNMPv1/v2) must be disabled or replaced.
• Enforce end-to-end encryption for critical business communications and sensitive data flows across all network paths.

6.5. Network Monitoring & Threat Detection

• Deploy NDR systems to monitor east-west and north-south traffic using behavioral/anomaly analytics to detect lateral movement and advanced threats.
• Integrate network security telemetry, firewall logs, and access events into a centralized SIEM for real-time alerting, incident response, and forensic analysis, with authenticated time synchronization and immutable retention.
• Establish automated incident response workflows to contain and remediate detected threats rapidly.

Practitioner Guidance:

Treat §6 items as enforceable build targets; verify in §12 with one primary test per item.

- Keep policies/configs in version control; changes flow through peer-reviewed pipelines.
- Prove segmentation and egress controls with traffic tests and BAS scenarios.

	• Validate monitoring by detecting known lateral techniques and timing to targets defined in §12.

	**Quick Win Playbook:** **Title:** Egress Default-Deny (Staged) **Objective:** Rapidly implement and validate zone-level egress control in a safe, reversible way that produces audit-ready evidence and aligns to §6.1/§6.2. **Target:** Enforce staged default-deny egress with zone-specific allowlists (§6.1, §6.2). **Component/System**: Boundary firewall/NGFW policy + egress policy-as-code repo + CI/CD pipeline + SIEM/NDR. **Protects:** Sensitive zones from unintended outbound communication, command-and-control, and data exfiltration. **Stops/Detects**: Unapproved destinations/ports, shadow rules, policy drift; logs missed contracts before enforcement. **Action**: Enable default-deny egress in staged/log-only mode for one sensitive zone; define minimal allowlist (FQDN/CIDR/proto/port) as policy-as-code; run CI checks; simulate both allowed and unallowed egress from that zone; review hits; promote to enforce after sign-off. **Proof**: Policy diff/commit, pipeline run result, staged hit logs, final enforce change record, and zone rule export; attach to Evidence Pack ID <EP-01.1> and reference Table A-6 rows for §5.2/§5.3. **Metric:** 100% of non-allowlisted egress attempts are blocked/logged; no business-critical false positives during promote; rule base shows no shadowed rules for that zone. **Rollback**: Revert to previous policy commit in the repo and redeploy; restore prior rule export; record exception owner and expiry under Evidence Pack <EP-01.1>.

Section 7. Cybersecurity Core Principles

The following ISAUnited Cybersecurity Core Principles are foundational to the design, implementation, and ongoing management of a secure network security architecture. Each principle guides architectural decisions, technical controls, and operational practices to ensure networks are resilient, measurable, and engineered to withstand real-world threats.

Table A-2:

Principle Name	Code	Applicability to Network Security Architecture & Engineering
Least Privilege	ISAU-RP-01	Segmentation, ACLs, and firewall policies grant only necessary inter-zone flows and admin rights.
Zero Trust	ISAU-RP-02	No implicit trust; every connection is authenticated/authorized by identity, posture, and context.
Complete Mediation	ISAU-RP-03	All flows crossing trust boundaries are explicitly checked and logged; no backdoor paths.
Defense in Depth	ISAU-RP-04	Layered controls (segmentation, NGFW/IPS, NAC/ZTNA, NDR/SIEM) prevent single-point failures.
Secure by Design	ISAU-RP-05	Controls are embedded in topology and runbooks from initial design through operations.
Minimize Attack Surface	ISAU-RP-06	Reduce exposed services via zoning, private/isolated paths, strict egress, and protocol hardening.
Fail-Safe Defaults	ISAU-RP-09	Default-deny at ingress/egress/inter-zone; exceptions are explicit, reviewed, and time-bound.
Secure Defaults	ISAU-RP-10	Devices and policies start in secure configuration; deviations require approved change.
Separation of Duties	ISAU-RP-11	Distinct roles for network admin, monitoring, and change control to reduce insider/error risk.
Security as Code	ISAU-RP-12	Policies/segmentation/egress expressed as version-controlled code with CI/CD validation.
Resilience & Recovery	ISAU-RP-14	Redundant paths, tested failover/DR, and bounded blast radius maintain service under fault.
Evidence Production	ISAU-RP-15	Time-synced, immutable logs/flows and artifacts enable defensibility and forensics.

Principle Name	Code	Applicability to Network Security Architecture & Engineering
Make Compromise Detection Easier	ISAU-RP-16	NDR/SIEM coverage and tuned analytics surface lateral movement quickly.
Protect Confidentiality	ISAU-RP-18	TLS 1.3/mTLS, IPsec, and access controls protect data in transit across all paths.
Protect Integrity	ISAU-RP-19	Controls and monitoring prevent/detect unauthorized traffic or config changes.
Protect Availability	ISAU-RP-20	DDoS protection, capacity planning, and resilient routing sustain operations.

Practitioner Guidance:

Embed these principles as design defaults and tie each to concrete controls and tests.

- Map each selected principle to at least one §6 output and one §12 test.
- Prefer RP-10 (Secure Defaults), RP-12 (Security as Code), and RP-15 (Evidence Production) to strengthen enforceability and auditability.
- Record principle-to-control traceability in the Evidence Pack for V&V.

Section 8. Foundational Standards Alignment

Network Security Architecture & Engineering must be grounded in globally recognized foundational standards to ensure interoperability, regulatory compliance, and a consistent risk management baseline. While ISAUnited Defensible Standards provide the technical depth and engineering rigor necessary for defensible security, alignment with foundational frameworks remains essential for auditability, industry acceptance, and integration into existing security programs.

Table A-3. The following foundational standards are most relevant to this parent standard:

Framework	Standard ID	Reference Focus
NIST	CSF 2.0	Cybersecurity Framework (Core, Profiles, Tiers) used to organize outcomes and governance across Identify–Protect–Detect–Respond–Recover.

Framework	Standard ID	Reference Focus
NIST	SP 800-53 Rev. 5	Security and Privacy Controls for Information Systems and Organizations (foundational control catalog for alignment).
NIST	SP 800-41 Rev. 1	Guidelines on Firewalls and Firewall Policy (network boundary guidance).
NIST	SP 800-207	Zero Trust Architecture (model and components for continuous verification).
ISO/IEC	27001:2022	Information Security Management System (ISMS) requirements.
ISO/IEC	27002:2022	Code of practice for information security controls.
ISO/IEC	27033 (family)	Network security framework (architecture, design, and management across parts 1–6).

As sub-standards are developed and published under this parent standard, more specific references to NIST and ISO foundational standards will be included to provide detailed, control-level alignment and facilitate practical implementation.

Practitioner Guidance:

Use this parent standard to drive design; cite NIST/ISO here for audit traceability.

- Map each §6 output to at least one NIST or ISO/IEC reference.
- Keep a single crosswalk per sub-standard (NIST ↔ ISO/IEC) to prevent drift.
- When in doubt, prefer the most specific NIST/ISO clause that matches the control intent.

Section 9. Security Controls

This section identifies the technical control families and control references that are directly supported or enforced by the Network Security Architecture & Engineering

Parent Standard. These controls explicitly link the architectural and engineering guidance to ISAUnited's adopted control frameworks, CIS Controls v8, the CSA Cloud Controls Matrix (CCM), and OWASP, ensuring traceability, auditability, and consistent implementation across diverse environments.

Purpose and Function:

Security controls translate the architectural intent defined in this standard into actionable, measurable safeguards. These controls provide tactical grounding for enforcing confidentiality, integrity, availability, authentication, authorization, and auditability in network environments.

By explicitly mapping to CSA CCM, CIS Controls v8, and OWASP standards, ISAUnited ensures:

- Clear alignment with recognized industry control practices and regulatory expectations.
- Interoperability across diverse organizational contexts and environments.
- Consistency and reusability of controls in sub-standards aligned to this Parent Standard, facilitating structured implementation and validation.

Implementation Guidance:

Sub-Standard Authors must adhere to the following guidelines:

- Explicitly reference at least three technical controls from CIS Controls v8, CSA CCM, and/or OWASP.
- Provide the framework name, specific control identifiers, and concise, implementation-level descriptions.
- Align chosen controls with the Technical Specifications (§6) and Core Principles (§7) in this Parent Standard.
- Select concrete, implementation-level controls rather than high-level policy statements.

Table A-4. Control Mappings for Network Security Architecture & Engineering:

Framework	Control ID	Control Name / Description
CSA CCM	IVS-09	Network Security – Implement network segmentation to isolate critical information systems, thereby reducing opportunities for lateral movement.
CSA CCM	IAM-09	Identity & Access – Implement strong authentication mechanisms (e.g., MFA) for network access to reduce unauthorized access risks.

Framework	Control ID	Control Name / Description
CIS v8	12.2	Network Infrastructure Management – Establish and maintain secure network architecture, including segmentation, traffic filtering, and secure configurations of network devices.
CIS v8	13.5	Network Traffic Filtering – Implement filtering and inspection (e.g., NGFW/IPS/DPI) at network boundaries and critical segments to protect against unauthorized access and malicious activity.
OWASP API Security Top 10	API2	Broken Authentication – Implement strong, consistent authentication mechanisms (OAuth 2.0, OpenID Connect, mTLS) to protect APIs from authentication vulnerabilities.

Additional References:

- As the network security domain matures, sub-standard Authors may incorporate supplementary controls from CIS v8, CSA CCM, or OWASP to maintain robustness and relevance.

Sub-Standard Expectations:

Sub-standards developed under the Network Security Architecture & Engineering Parent Standard are required to:

- Select and enforce explicit technical controls relevant to their targeted network security focus (e.g., firewall rule management, micro-segmentation, Zero Trust enforcement).
- Provide detailed mappings of these controls to defined validation, implementation, and operational criteria.
- Justify and document any deviation from control families referenced at this Parent Standard level, ensuring transparency and defensibility of any modifications or exceptions.

This structured approach to defining and mapping security controls ensures that network security architectures derived from ISAUnited's Defensible Standards are consistently defensible, auditable, and measurable against recognized cybersecurity best practices.

Section 10. Engineering Discipline

This section defines the architectural thinking, rigorous engineering processes, and disciplined operational behaviors required to implement the Network Security Architecture & Engineering Parent Standard. ISAUnited's Defensible Standards are not compliance checklists; they are engineered systems, grounded in systems thinking, critical reasoning, and Verification & Validation (V&V), that produce measurable, auditable, defensible outcomes in network security.

10.1 Purpose & Function

Purpose. Establish a repeatable, auditable way of working that integrates systems thinking, lifecycle controls, adversary-aware design, and measurable outcomes.

Function in D10S. Parent Standards set expectations and invariants. Sub-Standards convert them into controls-as-code, test specifications, and evidence artifacts embedded in delivery and operations.

10.2 Systems Thinking

Goal: Make the system legible end-to-end—components, interfaces, dependencies, and failure modes—so controls sit where risk manifests.

10.2.1 System Definition & Boundaries

- Declare system purpose, scope, stakeholders, and in-/out-of-scope assets.
- Model trust zones, segmentation, and interconnects (campus/DC, WAN/SD-WAN, VPC/VNet, peering, VPN/ZTNA, service endpoints, and other private/isolated endpoints).

10.2.2 Interfaces & Contracts

- Maintain Interface Control Documents (ICDs) for every interconnection (links/peers, APIs to network services, identity providers, telemetry exports).
- For each interface, specify: authentication/authorization model, data/classification, allowed flows (ports/protos), rate/flow limits, error handling, telemetry, and **security invariants**.

10.2.3 Dependencies & Emergent Behavior

- Map shared services (PKI/KMS, DNS/DHCP/NTP, NAC/IdP, logging/SIEM, NDR) and blast radius per dependency.
- Identify emergent risks from composition (for example, benign route at A + permissive ACL at B → unintended east-west path).

10.2.4 Failure Modes & Safeguards

- For critical paths, document failure modes (misconfig, drift, overload, credential abuse) and safeguards (default-deny, least privilege, rate caps, circuit breakers, staged/canary policy rollout, immutable configs).
- Treat security invariants as non-negotiable requirements (for example, “no public ingress to management plane,” “egress default-deny per zone,” “service-to-service uses mTLS where required”).

Required Artifacts (min): Context diagram with trust boundaries; interface map with ICDs; dependency & blast-radius matrix; invariants register.

10.3 Critical Thinking

Goal: Replace assumptions with explicit reasoning that survives review, attack, and audit.

10.3.1 Decision Discipline

- Use Architecture Decision Records (ADRs): problem → options → constraints/assumptions → trade-offs → decision → invariants → test/evidence plan.

10.3.2 Engineering Prompts

- **Boundaries:** What is the system? Where are the trust boundaries and why?
- **Interfaces:** What must always be true at each interface (invariants)? How do we test it?
- **Adversary:** Which attack techniques are credible here? What is the shortest attack path?
- **Evidence:** What objective signals prove this control works today and after change?
- **Failure:** When this fails, does it fail safe? What is the operator’s next action?

Required Artifacts (min): ADRs; assumptions & constraints log; evidence plan per decision.

10.4 Domain-Wide Engineering Expectations

Secure System Design

- Define network security boundaries (zones/segments, VLANs/subnets, routing/ACLs, boundary devices). Validate boundaries and trust relationships via structured reviews using §10.2 artifacts.

Implementation Philosophy — “Built-in, not bolted-on”

- Integrate controls at design-time and pipeline-time; avoid post-hoc patching.
- Express controls as policies/configurations-as-code bound to the invariants in §10.2.4.

Lifecycle Integration

- Embed controls into DevSecOps (IaC/PaC), change management, and immutable deployments.

- Enforce version-controlled reviews with required ADRs and evidence updates.

Verification Rigor (V&V)

- Combine automated checks (policy validation, IaC scanning, runtime guardrails) with manual tests (penetration testing, BAS/ATT&CK-informed emulation).
- Require continuous validation in pipelines and runtime monitoring tied to invariants.

Operational Discipline

- Monitor for drift and unauthorized change (including management-plane paths and egress policies); auto-remediate where safe.
- Maintain pre-approved playbooks for misconfiguration, key/cert rotation, incident containment, and rollback.

10.5 Engineering Implementation Expectations

- **Policy/Config as Code.** Manage policies and configurations as code under version control with peer review and provenance.
- **Structured Enforcement Pipelines.** CI/CD gates for unit/policy tests → security integration tests → staged/canary rollout → rollback.
- **Explicit Security Boundaries.** Maintain diagrams and ICDs; perform continuous validation with posture checks and targeted audits.
- **Automated Security Testing.** Integrate IaC scanning, configuration validation, secrets detection, dependency checks, and BAS/ATT&CK-informed emulation before production.
- **Traceable Architecture Decisions.** Link ADRs to controls, tests, and evidence; update ADRs and evidence on every change request.

Required Artifacts (min): Controls-as-code repository; pipeline policy gates; boundary/ICD set; automated test results; evidence ledger (see §10.7 and §12).

10.6 Sub-Standard Alignment (inheritance rules)

Sub-Standards must operationalize this discipline with domain-specific detail:

- **Network Segmentation (e.g., ISAU-DS-NS-1010).** Segmentation intents as code; default-deny inter-zone; micro-segmentation for critical apps; automated validation of declared contracts; staged/canary promotion with rollback.
- **Firewall Engineering & Rule Management (e.g., ISAU-DS-NS-1020).** Versioned rule definitions; policy-as-code validation (deny-by-default at ingress/egress/inter-zone); drift detection; peer review; negative tests for shadow/over-permissive rules before deploy.
- **Zero Trust Network Access (e.g., ISAU-DS-NS-1030).** Continuous authentication/authorization and device posture checks; per-request policy evaluation; telemetry-verified decisions; attack-path tests for lateral movement and credential abuse.
- **Monitoring & Response (e.g., ISAU-DS-NS-1040).** NDR/SIEM integration; behavioral/anomaly analytics; authenticated time; immutable retention; V&V tied to MTTD/MTTC targets.

10.7 Evidence & V&V (what proves it works)

Use the annex's single Evidence Pack **EP-01** with child IDs (**EP-01.x**) containing:

- **Design Evidence:** diagrams with trust boundaries, ICDs, invariants register, ADRs.
- **Build Evidence:** IaC/PaC repositories, signed artifacts, pipeline logs, automated test results.
- **Operate Evidence:** runtime policy decisions, drift reports, control telemetry, incident and rollback records.
- **Challenge Evidence:** red-team/penetration reports, BAS/ATT&CK outcomes, remediation closure with re-test.

Each control requires objective pass/fail criteria, a test frequency, a responsible owner, and a retention policy. Map Evidence Pack IDs into §12 traceability.

10.8 Example: Sub-Standard Discipline Alignment (Firewall Engineering & Rule Management)

Scope: ISAU-DS-NS-1020 Firewall Engineering & Rule Management
Design: Define boundary points and inter-zone contracts; record invariants (for example, "egress default-deny per zone," "management plane reachable only via bastion").
Implement: Manage rules as code; enforce deny-by-default at ingress/egress/inter-zone; validate with policy checks for shadow/over-permissive rules; require peer review and staged/canary rollout with rollback.
V&V: Automated negative tests for unauthorized flows; live traffic tests confirm only registered contracts pass; BAS/ATT&CK-informed scenarios validate lateral-movement resistance; monitor targets for MTTD and MTTC per §12.
Operate: Evidence Pack includes rule repo history, policy-gate results, runtime deny/allow logs, drift alerts, incident records, and closed-loop remediation.

Section 11. Associate Sub-Standards Mapping

Purpose of Sub-Standards

ISAUnited Defensible Sub-Standards serve as detailed, domain-specific extensions to this Parent Standard. Each Sub-Standard provides granular technical guidance, actionable implementation strategies, and precise validation methodologies that are explicitly aligned with the foundational architectural principles and technical specifications outlined in the Parent Standard.

Sub-Standards bridge the gap between broad architectural direction (provided by Parent Standards) and the detailed technical requirements necessary for practical engineering implementation, validation, and auditing.

Scope and Focus of Sub-Standards

Sub-Standards developed under this Parent Standard will address specialized network security topics, including but not limited to:

- Detailed technical configurations and architectures for network segmentation and isolation.
- Firewall and boundary security engineering, including configuration management, rule lifecycle management, and automated enforcement.
- Explicit methodologies for implementing Zero Trust network principles and identity-based access control systems.
- Advanced network monitoring, detection, and response techniques, incorporating modern technologies and emerging practices.

Each Sub-Standard will define explicit inputs (requirements), measurable outputs (technical specifications), structured validation methodologies, and implementation guidelines to ensure consistent, actionable cybersecurity practices, including a crosswalk to §5 Requirements, §6 Technical Specifications, §12 Verification & Validation tests (with Evidence Pack IDs), and §9 control mappings (CIS v8 / CSA CCM / OWASP).

Table A-5. Example Future Sub-Standards under ISAU-DS-NS-1000

Sub-Standard ID	Sub-Standard Name	Focus Area
ISAU-DS-NS-1010	Network Segmentation Architecture & Policy	Engineering, implementing, and validating VLAN, micro-segmentation, and trust zone policies.
ISAU-DS-NS-1020	Firewall Engineering & Rule Management	Secure firewall design, rule lifecycle management, automated policy validation, and enforcement pipelines.
ISAU-DS-NS-1030	Zero Trust Network Access (ZTNA) Design & Implementation	Identity-based access control, continuous verification/re-authorization, device posture validation (NAC/802.1X), and policy enforcement.
ISAU-DS-NS-1040	Network Monitoring & Response (NDR) Design & Operations	NDR integration, behavioral/anomaly analytics tuning, ATT&CK/BAS-informed validation, automated response workflows, **authenticated time synchronization, and immutable retention of telemetry.

Sub-Standard ID	Sub-Standard Name	Focus Area
ISAU-DS-NS-1050	Secure Network Protocol & Encryption Enforcement	Mandatory encrypted protocol enforcement, legacy protocol mitigation, and **conformance validation with runtime enforcement.
ISAU-DS-NS-1060	Network Access Control (NAC) Implementation Standards	NAC policy design, device onboarding workflows, and posture-based access enforcement.

Development and Approval Process

ISAUnited employs a structured, annual Open Season Process for developing, reviewing, and publishing Sub-Standards:

- **Open Season Submission:** Members and registered contributors submit proposed Sub-Standards that are aligned with the Parent Standard's objectives and technical scope.
- **Technical Peer Review:** Technical Peer Review: Submissions undergo rigorous evaluation by ISAUnited's Technical Fellow Society, ensuring engineering validity, technical accuracy, alignment with core principles, and practical applicability, including measurable targets (e.g., where applicable, MTTD/MTTC) and defined Evidence Pack IDs (EP-01.x) for all tests.
- **Approval and Publication:** Upon successful review and validation, approved Sub-Standards receive a formal version stamp and are officially published, becoming authoritative, actionable extensions of the Parent Standard.

Future Development (Q3 2025)

ISAUnited will begin publishing approved Sub-Standards for Network Security Architecture & Engineering starting Q3 2025. At that time, contributors and practitioners can expect detailed technical guidance for implementing and validating specific network security practices and technologies aligned with the Parent Standard.

Practitioners interested in contributing Sub-Standards should monitor official ISAUnited communications for detailed submission guidelines, timelines, and instructions on participating in the Open Season.

Section 12. Verification and Validation

The effectiveness and defensibility of a network security architecture must be continuously verified and validated through structured, engineering-grade assessment methods. While detailed testing requirements for specific technologies and controls will be defined in sub-standards, the following parent-level expectations establish a gold standard for all organizations:

> **Verification** confirms that the system has been implemented in accordance with the defined Requirements (Inputs) and Technical Specifications (Outputs) of this standard.
>
> **Validation** ensures that the system performs effectively in real-world operational conditions and withstands adversarial testing.

Core Verification Activities

- Confirm that all network security controls defined in the Technical Specifications have been implemented in the production or target environment (e.g., segmentation, zone-level egress default-deny, firewall policies, management-plane isolation with bastion access, encryption enforcement, and authenticated time synchronization).
- Review and validate network device configuration baselines against recognized engineering and security benchmarks (e.g., CIS Benchmarks; NIST SP 800-41 for firewall policy).
- Verify network interoperability and integration points to ensure that segmentation, NAC, and Zero Trust enforcement do not introduce new vulnerabilities or disrupt business-critical services.
- Conduct peer review of network architecture diagrams, segmentation maps, firewall rule sets, and security control mappings to ensure completeness and accuracy.

Core Validation Activities

- Perform adversarial testing—such as penetration testing, red teaming, and BAS/ATT&CK-informed emulation—focusing on lateral movement resistance, boundary control effectiveness, Zero Trust enforcement, and egress governance.
- Validate network security posture using automated and manual methods to ensure resilience against relevant threat models (e.g., MITRE ATT&CK techniques targeting network infrastructure).

- Test operational resilience, including failover of critical network paths, disaster recovery routing, and incident response capabilities tied to network-based events.
- Measure control performance against defined metrics such as Mean Time to Detect (MTTD), Mean Time to Contain (MTTC), Mean Time to Respond/Recover (MTTR), and network control coverage rate.

Required Deliverables

All Verification & Validation efforts must produce documented outputs that include:

1. Test Plans & Procedures – Detailed scope, tools, and testing methodologies for both verification and validation phases.
2. Validation Reports – Results with pass/fail status, residual risk ranking, and remediation priorities.
3. Evidence Artifacts – Logs, packet captures, screenshots, and configuration exports proving test execution and results, each labeled with an Evidence Pack ID referenced in Table A-6.
4. Corrective Action Plans – Documented remediation steps for any findings requiring resolution before system acceptance.

Common Pitfalls to Avoid:

- Treating penetration testing as a check-the-box exercise rather than a rigorous, adversary-informed assessment.
- Failing to document validation activities, leading to gaps in audit trails and lessons learned.
- Neglecting continuous validation in dynamic or high-risk network segments.

Table A-6. Traceability Matrix: Requirements (§5) to Verification/Validation (§12) and Technical Specifications (§6):

Requirement ID	Requirement (summary)	Verification (build-correct)	Validation (works-right)	Related Technical Specs
5.1	Asset inventory and network mapping	• Current inventory of devices, paths, and inter-zone flows exists	• Sample path tests match declared contracts; synthetic traffic proves	§6.1 Segmentation & Isolation; §6.5

Requirement ID	Requirement (summary)	Verification (build-correct)	Validation (works-right)	Related Technical Specs
		• Architecture and segmentation diagrams are versioned and approved	documented routes; unauthorized paths are not routable	Monitoring & Detection
5.2	Business-driven network segmentation	• Trust zones and policies are defined and deployed; default-deny between zones	• Breach-and-attack simulation across zones shows east–west block rate meets target; blast radius testing contained to intended zone	§6.1 Segmentation & Isolation
5.3	Firewall and perimeter security strategy	• Boundary controls with default-deny are enforced at ingress, egress, and inter-zone • Management plane is unreachable from production; access is via bastion with MFA/JIT • Rule bases are change-controlled and documented	Live traffic tests confirm only registered contracts pass; IPS/DPI triggers expected signatures without excess false positives; egress attempts outside allowlists are blocked and logged	§6.2 Firewall Engineering & Filtering
5.4	Zero Trust implementation readiness	• Identity-aware policies are present; MFA and JIT for admin paths are enforced	• Phishing or credential replay simulations require step-up; lateral movement attempts that rely on implicit trust are blocked	§6.3 Zero Trust Network Design
5.5	Network Access Control (NAC) capability	• NAC posture checks and identity-based admission controls are configured	• Onboard and non-compliant device drills show quarantine/deny works; guest and unmanaged devices cannot access protected zones	§6.3 Zero Trust Network Design
5.6	Secure protocol usage	• TLS 1.3 at edges; mTLS where required; legacy management protocols disabled	• External and internal transport scans achieve required grades; service-to-service calls without mTLS are blocked	§6.4 Secure Protocols & Encryption

Requirement ID	Requirement (summary)	Verification (build-correct)	Validation (works-right)	Related Technical Specs
5.7	Network logging and anomaly detection enablement	• NetFlow/IPFIX/PCAP at boundaries; normalized logs to immutable store; SIEM integrations active	• Anomaly and threat simulations are detected within target MTTD (e.g., ≤ 10 min); incident triage playbooks execute with target MTTC (e.g., ≤ 30 min for tier-1 zones)	§6.5 Monitoring & Detection
5.8	Change management and configuration control	• Policy-as-code pipelines enforce peer review and staged rollout; device config drift alerts are active	• Introduce safe policy change in staging; pipeline blocks until checks pass; drift is detected and remediated within the target window	§6.2 Firewall Engineering & Filtering; §6.1 Segmentation & Isolation
5.9	Baseline documentation and policy alignment	• Security policies, segmentation standards, and device baselines are published and current	• Random configuration samples match baselines; audit spot checks pass with no high-severity deviations	§6.1–§6.5 (all apply)

Evidence guidance

• Attach plans and procedures, approved diagrams, policy-as-code repositories, rule exports, scan results, SIEM detections, BAS reports, NAC posture logs, certificate inventories, config drift reports, and dated sign-offs. Include authenticated NTP configuration evidence and proof of immutable log retention settings.
• Store artifacts in a secure repository and reference each row with an Evidence Pack ID in this matrix.

How to use the matrix

• During planning: confirm each §5 requirement has at least one verification and one validation activity scheduled.
• During execution: record the Evidence Pack ID for each row when completed.
• During review: when a requirement or control changes, update its linked activities and §6 references to keep the chain intact.

Practitioner Guidance:

Treat §12 as a continuous engineering function, not a one-time event.

- Map every §5 requirement to one verification and one validation in Table A-6, each with a unique Evidence Pack ID.
- Exercise BAS/ATT&CK techniques that match your architecture; track MTTD/MTTC against targets and adjust controls.
- Validate management-plane isolation and egress default-deny during every major change window.

Quick Win Playbook:

Title: Segmentation and Egress Proof (MTTD/MTTC)

Objective: Demonstrate, in 10–30 minutes, that inter-zone segmentation and zone egress default-deny are both effective and observable, producing audit-ready evidence mapped to §5.1/§5.2/§5.7 and §6.1/§6.5.

Target: Prove segmentation and egress enforcement for one sensitive zone within MTTD/MTTC targets (§6.1, §6.5, §12).

Component/System: Test host in sensitive zone + synthetic path tester + firewall/egress policy + NDR/SIEM.

Protects: Inter-zone boundaries and outbound controls against bypass and lateral movement paths.

Stops/Detects: Unauthorized east-west pathing and unallowlisted egress; confirms telemetry timeliness.

Action: Execute two synthetic tests: 1) attempt an unauthorized inter-zone connection (expect deny); 2) attempt an unallowlisted egress (expect deny); then run one allowed contract (expect pass). Confirm alerts in SIEM/NDR and ticket creation per playbook.

Proof: Test script output, firewall/NDR event IDs with timestamps, SIEM alert and ticket links, and current zone contract list; attach to Evidence Pack ID <EP-01.2> and cite Table A-6 rows for §5.1/§5.2/§5.7.

Metric: Block events detected within target MTTD (≤ 10 min) and containment actions executed within target MTTC (≤ 30 min for tier-1); allowed contract passes without alert.

Rollback: Remove temporary test routes/entries; restore pre-test state; tag all artifacts in <EP-01.2> as “completed.”

By embedding structured, continuous, and evidence-based testing and validation into network security engineering, organizations move beyond compliance and achieve true defensibility, ensuring that controls are not only present but also practical and resilient against real-world threats.

Section 13. Implementation Guidelines

This section does not prescribe vendor-specific tactics. Parent Standards are stable, long-lived architectural foundations. Here, we define how sub-standards and delivery teams must translate the Parent's intent into operational behaviors that are testable, automatable, and auditable.

Purpose of This Section in Sub-Standards

Sub-standards must use Implementation Guidelines to:

- Translate architectural expectations from the Parent Standard into enforceable run-time and pipeline behaviors.
- Provide platform-agnostic practices that improve adoption, avoid failure, and align with ISAUnited's defensible design philosophy.
- Highlight common failure modes and how to prevent them with measurable gates and checks.
- Offer repeatable patterns (as code) that enforce controls, trust models, and engineering discipline.

Open Season Guidance for Contributors

Contributors developing sub-standards Must:

- Align all guidance with the strategic posture in this Parent Standard.
- Avoid vendor/product terms; express controls as requirements, tests, and evidence.
- Include lessons learned (what fails, why, and how the test proves it).
- Focus on repeatable engineering patterns, not one-offs.
- Provide a minimal Standards Mapping (Spec/Control → NIST/ISO clause from §8 → Evidence Pack ID).

Technical Guidance

A. Organizing Principles (normative)

1. **Everything as code** – Policies, configs, network intents, pipelines, runbooks, and tests Must be version-controlled, peer-reviewed, and promoted through environments on protected branches.
2. **Gated change** – Every merge and deployment Must pass non-bypassable security gates tied to quantitative acceptance criteria (see §6 and §12).
3. **Immutable, reproducible releases** – No manual device or policy changes post-build; releases Must be reproducible from source and verified at deploy.
4. **Least privilege & JIT** – Pipeline identities, automation runners, and administrators Must use scoped permissions with time-bound elevation; break-glass Must be exceptional and fully audited.
5. **Environment parity** – Staging Must mirror production controls (authentication/authorization, egress, TLS/mTLS, logging schema) so test results are predictive; drift Must be monitored and reconciled.

B. Guardrails by Pipeline Stage (normative)

1. **Pre-commit / local**
   - Secrets scanning and commit signing required.
   - Pre-commit hooks Should run linters and policy checks for network/IaC definitions.
2. **Pull request (PR) / code review**
   - CODEOWNERS approval required; Threat-Model Delta recorded in PR template for significant change.
   - IaC policy-as-code gate (OPA or equivalent) for segmentation, identity, cryptography, logging, and egress rules; Critical = 0.
   - Require evidence pointers in PR (planned tests and Evidence Pack ID stubs).
3. **Build & package**
   - Deterministic artifacts (pinned versions; no ad-hoc fetch at deploy).
   - Artifacts signed; integrity verified prior to promotion.
   - Transitive dependency review for automation/pipeline components.
4. **Pre-deploy / release**
   - Config drift detection against approved baselines; change approval as code.
   - Progressive rollout (staged/canary) for network policies; define health thresholds and automatic rollback.
   - Negative/positive traffic contract tests for inter-zone flows; egress allowlist tests.
5. **Deploy & runtime**
   - TLS 1.3 at edges; mTLS for service-to-service/admin paths where required; certificates managed via PKI/KMS with rotation.
   - Egress allowlists per zone/workload; runners/automation isolated with restricted outbound.
   - Unified logging schema (timestamp, actor, action, resource, result, trace_id, control_id, env); logs to immutable store with authenticated NTP.

- Management-plane isolation with bastion, MFA/JIT, and full session recording.

6. **Post-deploy validation & operations**
   - Continuous validation (BAS/ATT&CK scenarios) scheduled; failover and disaster recovery routing drills.
   - Security objectives tracked: target MTTD/MTTC per §12; segmentation block-rate goals; egress violations = 0 in sensitive zones.
   - Append artifacts to the single Evidence Pack **EP-01.x** per release (configs, policy diffs, validation results, logs, drift reports, ADR links).

C. Identity, Secrets, and Keys (normative alignment to §6)

- Use KMS for key storage; define certificate issuance/rotation/revocation; maintain service identity inventories.
- Use short-lived credentials for pipelines and bastions; scope secrets to job/environment; redact in logs.
- No secrets in repos or device images; inject at runtime; full auditability of access.

D. Supply-Chain Integrity (normative)

- Only deploy signed, verified configurations and images from trusted sources; restrict registries/repositories.
- Quarantine and verify third-party artifacts (scripts, modules); enforce license and integrity checks.
- Separate build and deploy identities; forbid production write from build jobs.

E. Measurement & Acceptance (aligned to §6 and §12)

- mTLS coverage for designated paths meets target; certificate inventory current with no expirations inside policy window.
- Zone egress: default-deny enforced; allowlisted destinations only; exceptions time-bounded with approvals.
- Logging: authenticated time sync; required fields present; evidence retention immutable.
- Detection: MTTD/MTTC targets met for boundary/east-west anomalies; monthly review and tuning.
- Each change linked to an Evidence Pack ID tying artifacts to §5 → §6 → §12.

Common Pitfalls (and the engineered countermeasure)

1. Pipelines as suggestions → Enforce non-bypassable gates; block merges/releases on fails; store failing artifacts as proof.
2. One-time scanning → Treat checks as gates with thresholds; require coverage for changed items.
3. Manual hot-fixes/drift → Detect and reconcile drift; forbid out-of-band edits; require Architecture Decision Records.
4. Open egress / shared runners → Isolate runners; restrict outbound; allowlist per zone/workload.

5. Management plane exposure → Bastion-only with MFA/JIT; block direct access from production subnets.
6. Weak crypto / stale certs → Enforce TLS 1.3/mTLS where required; rotate and monitor via PKI/KMS.
7. Incomplete logging/time → Enforce unified schema, authenticated NTP, and immutable retention.
8. No evidence → Every release Must have an Evidence Pack ID with linked tests and results.

Practitioner Guidance:

Keep §13 small, routine, and evidence-first.

- Update baselines (diagrams, policies, runbooks) with every approved change and attach to an Evidence Pack ID.
- Validate management-plane isolation and zone egress during each change window.
- Review detection performance monthly; tune to meet §12 MTTD/MTTC targets.

Quick Win Playbook:

Title: Bastion-Only Management Access

Objective: Enforce, in 10–30 minutes, bastion-only access to the management plane and produce audit-ready evidence mapped to §5.3 and §6.2.

Target: Enforce bastion-only access to the network management plane (§6.2)

Component/System: Management network + bastion host + MFA/JIT service + device ACLs + SIEM/NDR

Protects: Routers, switches, firewalls, and controllers from direct access via production subnets or user VLANs

Stops/Detects: Direct management logins from non-bastion sources; stale admin sessions; unauthorized lateral movement into the management plane

Action: Update device ACLs to allow management protocols only from the bastion; require MFA + JIT on the bastion; disable legacy direct-access paths; attempt 1) direct login from a production subnet (deny) and 2) bastion-mediated login (allow); verify session recording enabled

Proof: ACL/policy diff, bastion MFA/JIT setting screenshot, device login attempt logs (deny/allow), and session record pointer; attach to Evidence Pack ID <EP-

	01.4> and reference Table A-6 row for §5.3 **Metric:** 100 % of direct management attempts from non-bastion sources are denied and logged; 100 % of successful management sessions originate from the bastion with MFA/JIT and session recording **Rollback:** Revert ACL/policy to the previous commit; temporarily issue a time-bounded exception if required; archive artifacts under <EP-01.4>.

Appendices

Appendix A: Engineering Traceability Matrix (ETM)

Req ID	Requirement (Inputs) (§5)	Technical Specification (Outputs) (§6)	Core Principles (§7)	Control Mappings (§9)	Verification (Build-Correct) (§12)	Validation (Works-Right) (§12)	Evidence Pack ID
R5.1	Asset Inventory & Network Mapping	TS6.1 Segmentation & Isolation TS6.5 Monitoring	RP-01 Least Privilege RP-15 Evidence Production	CIS 1.1, CIS 12.2, CCM IVS-09	Inventory + diagram review Segmentation map approval	Path testing & synthetic traffic proving zone boundaries.	EP-01.01
R5.2	Business-Driven Segmentation	TS6.1 Segmentation Policies	RP-01 Least Privilege RP-06 Minimize Attack Surface	CIS 12.5, CCM IVS-09	Trust zone definition review	BAS cross-zone block rate ≥ target Blast-radius testing	EP-01.01
R5.3	Firewall & Boundary Security Strategy	TS6.2 Firewall Engineering	RP-04 Defense in Depth RP-09 Fail-Safe Defaults	CIS 13.5, CCM IAM-09	Firewall rule audit Management-plane isolation check	Live traffic tests; IPS/DPI validation Egress deny validation	EP-01.02
R5.4	Zero Trust Readiness	TS6.3 Zero Trust Network Design	RP-02 Zero Trust RP-03 Complete Mediation	OWASP API2, CIS 6.2	Identity/MFA/JIT rule enforcement checks	Credential replay tests ZTNA lateral movement validation	EP-01.03
R5.5	Network Access Control (NAC)	TS6.3 NAC Enforcement	RP-02 Zero Trust RP-11 Separation of Duties	CIS 6.6	NAC posture check verification Guest access policy review	Device posture drills (quarantine/deny) Unmanaged device validation	EP-01.03
R5.6		TS6.4 Secure	RP-18 Confidentia		TLS/mTLS configuration	TLS/mTLS scan results	EP-01.05

	Secure Protocol Usage	Protocols & Encryption	lity RP-19 Integrity	CIS 3.4, CCM KMS-01	review Legacy protocol disablement	IPsec/SSH/PKI enforcement tests	
R5.7	Logging & Anomaly Detection	TS6.5 Monitoring & NDR	RP-15 Evidence Production RP-16 Detection Easier	CIS 8.2, CCM LOG-01	SIEM/NDR pipeline validation NTP/authenticated time checks	Detection of simulated threats within MTTD Incident triage MTTC ≤ target	EP-01.04
R5.8	Change & Configuration Control	TS6.1 Segmentation & Isolation TS6.2 Firewall Engineering	RP-12 Security as Code RP-10 Secure Defaults	CIS 4.1, CIS 4.2	I aC/PaC pipeline checks Drift detection verification	Fail-closed negative testing Drift remediation validation	EP-01.02
R5.9	Baseline Alignment	TS6.1–TS6.5 (All Outputs)	RP-05 Secure by Design RP-15 Evidence Production	CIS 4.3	Baseline documentation review	Random config sampling Architecture compliance audit	EP-01

Appendix B: EP-01 Summary Matrix – Evidence Pack Overview

Layer	EP Identifier	Purpose	Evidence Categories Included
Parent EP	EP-01	Serves as the master Evidence Pack for the D01 Parent Standard. Stores all architecture-level evidence, global V&V artifacts, and major design documentation supporting §5, §6, §10, and §12.	• Network architecture diagrams • Trust zone & segmentation maps • Management-plane isolation diagrams • Invariants register • Interface Control Documents (ICDs) • Architecture Decision Records (ADRs) • Parent-level V&V evidence • Cross-domain logs, scans, and configuration exports
Sub-EP	EP-01.01	Supports Sub-Standard ISAU-DS-NS-1010 (Segmentation Architecture & Policy). Focuses on segmentation definitions, boundaries, and enforcement.	• Segmentation contracts • VLAN/VNet/subnet maps • Micro-segmentation evidence • East-west block test results • BAS/ATT&CK segmentation tests • Egress allowlist definitions • Boundary device configuration exports
Sub-EP	EP-01.02	Supports Sub-Standard ISAU-DS-NS-1020 (Firewall Engineering & Rule Management). Provides evidence of boundary control correctness.	• Firewall rulebase exports • Rule lifecycle history • Policy-as-Code validation results • Shadow/over-permissive rule analysis • Deny-by-default enforcement proof • Drift detection reports • IPS/DPI alert validation
Sub-EP	EP-01.03	Supports Sub-Standard ISAU-DS-NS-1030 (Zero Trust Network Access). Captures identity, posture, and policy enforcement validation.	• NAC posture logs • ZTNA decision logs • MFA/JIT administrative access evidence • Device trust validations • Credential replay/phishing test results • Lateral movement prevention evidence • Bastion session recordings
Sub-EP	EP-01.04	Supports Sub-Standard ISAU-DS-NS-1040 (Network Monitoring & Response). Contains detection quality, telemetry assurance, and incident response validation.	• NDR detection logs • SIEM alert data • Analytics tuning outputs • Packet captures (PCAPs) • Authenticated time sync proof • Immutable log configuration evidence • MTTD/MTTC performance data
Sub-EP	EP-01.05	Supports Sub-Standard ISAU-DS-NS-1050 (Secure Network Protocol & Encryption	• TLS 1.3/mTLS scan results • Certificate inventory & rotation logs • SSH configuration evidence

Layer	EP Identifier	Purpose	Evidence Categories Included
		Enforcement). Documents protocol hardening and cryptographic validation.	• IPsec tunnel validations • Legacy protocol disablement proof • Service identity enforcement evidence
Sub-EP (Future)	EP-01.06	Reserved for future network security sub-standards published through ISAUnited's Open Season.	• Will follow the same EP structure as above • Will inherit domain-specific evidence requirements

Change Log and Revision History

Review Date	Changes	Committee	Action	Status
December 2025	Standards Revision	Standards Committee	Publication	Pending
November 2025	Standards Submitted	Technical Fellow Society	Peer review	Pending
October 2025	Standards Revision	Task Group ISAU-TG39-2024	Draft submitted	Complete
December 2024	Standards Development (Parent D01)	Task Group ISAU-TG39-2024	Draft complete	Complete