MYTHOS SYSTEMS

PERMANENT LIBRARY PUBLICATION

ENGINEERING STANDARDS LIBRARY / NETWORK ENGINEERING

Network Security Architecture and Zero-Trust Networking Standard

Defines identity-aware networking, segmentation, enforcement, telemetry, and continuous validation.

PERMANENT DOCUMENT ID
MYTHOS-NET-0004

PUBLICATION
Candidate Standard

ASSURANCE SURFACE
10 Atomic Criteria / 6 Families

PERMANENT PUBLICATION IDENTITY

Network Security Architecture and Zero-Trust Networking Standard

Defines identity-aware networking, segmentation, enforcement, telemetry, and continuous validation.

DOCUMENT ID
MYTHOS-NET-0004

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-23

SCHEDULED REVIEW
2027-01-23

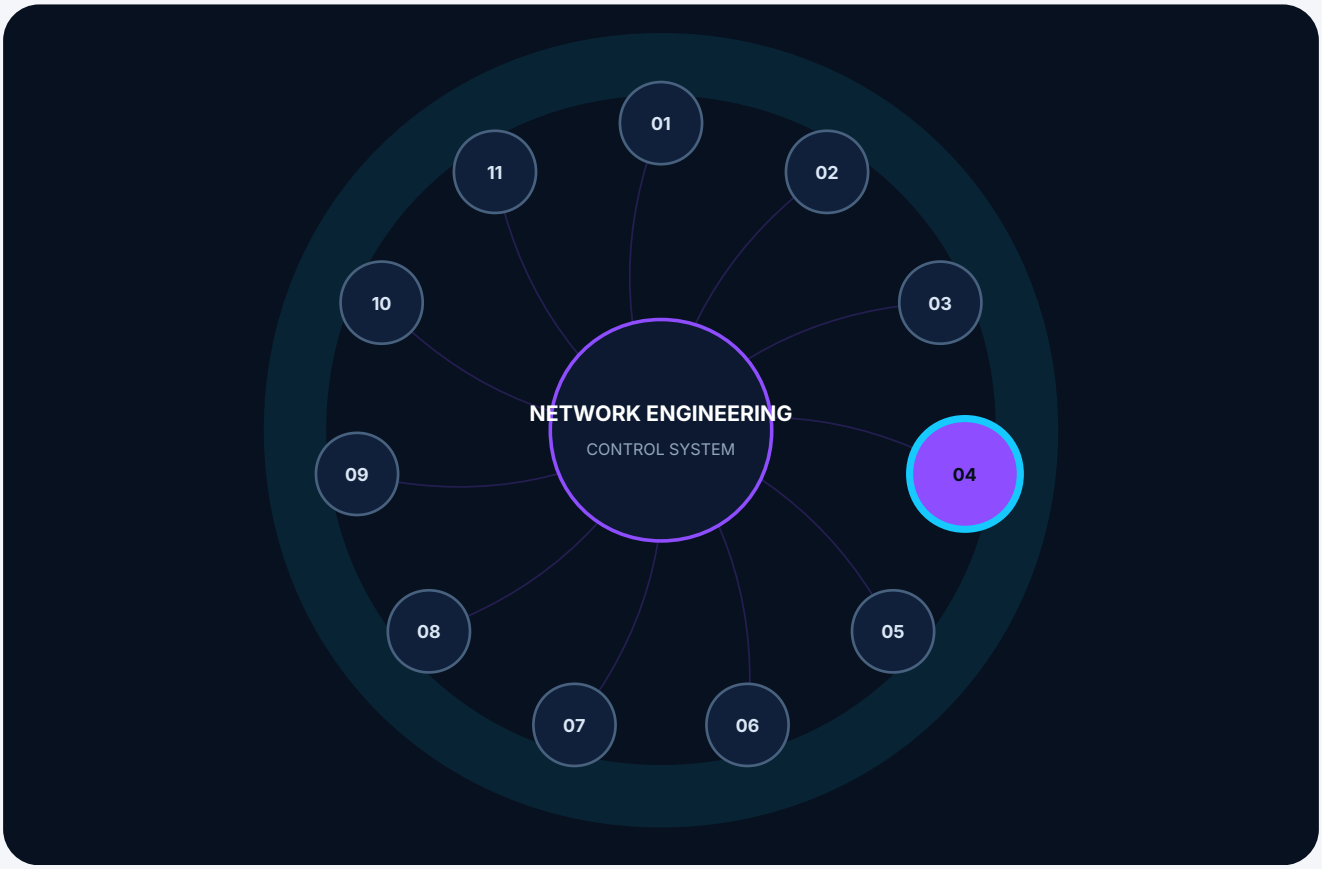
CLASSIFICATION
Public

10	6	4	1
ATOMIC CRITERIA	CAPABILITY FAMILIES	ASSESSMENT PROFILES	PERMANENT IDENTITY

Publication doctrine. This standard establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, recorded evidence, and formal revision history.

DOMAIN CONTROL SYSTEM

MYTHOS-NET-0004 inside the network engineering standard constellation



Connected assurance

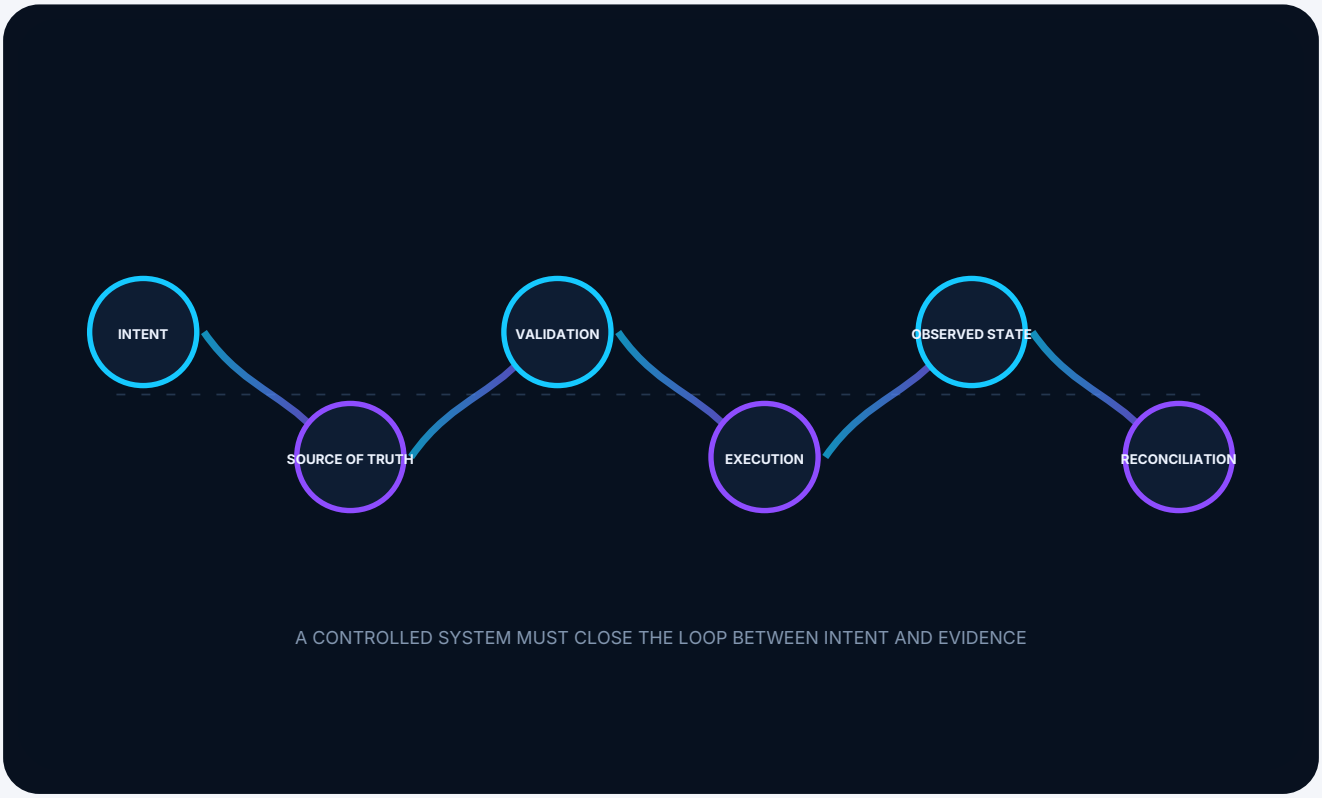
Architecture, policy, implementation, operations, and evidence are evaluated as one controlled system.

Specialization rule

Companion standards may add precision, but they cannot silently weaken this publication's requirements.

CLOSED-LOOP ARCHITECTURE

Intent becomes trustworthy only when observed state returns as evidence



State separation

Desired, approved, deployed, observed, historical, and simulated states must remain distinguishable.

Recoverable change

Material change requires validation, authorization, monitoring, containment, and a credible recovery path.

EVALUATION TOPOLOGY

The capability families and atomic criteria of MYTHOS-NET-0004

Capability families

Families expose the major engineering surfaces and preserve the source weighting model.

Atomic criteria

Each criterion carries a question, maturity spectrum, evidence expectations, assessment method, and operational signals.

NAVIGATION

Contents

ENGINEERING DOCTRINE

0. Executive Mandate

The internal network is hostile. The perimeter has dissolved.

Organizations continue to architect their networks assuming a trusted interior, relying on North-South firewalls while ignoring the free-flowing East-West traffic of their data centers and clouds. This architecture is a relic. Once an attacker - or a compromised AI agent - breaches the perimeter, the flat internal network provides zero resistance to lateral movement.

This standard exists because:

1. **IP Addresses are Not Identity:** Firewalls and ACLs that filter on IP addresses are easily spoofed and fundamentally incapable of enforcing zero-trust principles. Network policy MUST be bound to cryptographic workload identity (SPIFFE/SPIRE) and user identity, not static IPs.
2. **The Network Must Encrypt Everything:** Unencrypted internal traffic (East-West) is an open book to anyone with a packet sniffer. MACsec for physical layers, IPSec/WireGuard for overlays, and PQC-TLS for API planes are mandatory, not optional.
3. **Network Access Control Must be Dynamic:** 802.1X and RADIUS must move from simple port-authentication to dynamic, posture-aware identity assignment. Devices and AI agents that fail posture checks must be quarantined automatically.
4. **AI Agents are Untrusted Workloads:** An AI agent processing untrusted data (e.g., RAG from the internet) must be treated as a potentially compromised entity. The network fabric MUST isolate agent execution planes from production data planes.

This document establishes the **Mythos Zero-Trust Networking Standard (MZTNS)**, a comprehensive, evidence-based methodology for evaluating the network fabric, identity integration, and encryption posture required for true zero-trust architecture.

ENGINEERING DOCTRINE

Part I. Scope and Applicability

1.1 In Scope

This standard covers the evaluation of:

- Zero-Trust Network Access (ZTNA) and Software-Defined Perimeters (SDP)
- Network Access Control (NAC), 802.1X, RADIUS, and dynamic VLAN assignment
- Identity-aware network fabrics (SPIFFE/SPIRE integration)
- Encryption in transit (MACsec, IPSec, WireGuard, PQC-TLS)
- Network-level isolation and quarantine for AI agents
- DNS security (DoH, DoT, DNSSEC)

1.2 Out of Scope

- Microsegmentation policy and blast radius (covered in MYTHOS-SEC-0007)
- Zero-Trust policy engine authority and RBAC (covered in MYTHOS-SEC-0003)
- Post-Quantum Cryptography algorithm standardization (covered in MYTHOS-SEC-0001)

1.3 Audience

- Network security architects designing zero-trust fabrics
- Identity and Access Management (IAM) engineers
- Platform engineers managing SPIFFE/SPIRE or ZTNA overlays
- AI infrastructure teams securing agent network paths
- Standards bodies seeking a reference zero-trust networking methodology

---

ENGINEERING DOCTRINE

Part II. Definitions and Taxonomy

2.1 Zero-Trust Networking Dimensions

Dimension	Definition
ZTNA	Zero-Trust Network Access. Replaces VPNs with identity-aware, per-application access, hiding the network from unauthorized users.
MACsec	Media Access Control Security. IEEE 802.1AE standard for encrypting data on Ethernet links, providing hop-by-hop confidentiality and integrity.
SPIFFE	Secure Production Identity Framework for Everyone. A set of open-source standards for securely identifying software systems in dynamic and heterogeneous environments.
802.1X	IEEE standard for port-based Network Access Control, authenticating devices before allowing network access.
Posture Assessment	The evaluation of a device's security state (OS patches, antivirus, configuration) before granting network access.

2.2 The Zero-Trust Networking Doctrine

> The internal network is hostile. IPs are not identity. Unencrypted traffic is a breach. A device without posture is a threat. An AI agent without network isolation is a loaded weapon.

ENGINEERING DOCTRINE

Part III. Evaluation Methodology

3.1 Scoring Model

Each capability is scored from 0 to 5.

Score	Meaning
0	Fails basic task; flat network, no encryption, IP-based ACLs
1	Basic ZTNA for remote users, but internal network is flat
2	Functional but lacks identity integration or hardware encryption
3	Solid production performance; identity-aware, encrypted, NAC-enforced
4	Strong performance; SPIFFE-integrated, PQC-ready, agent-isolated
5	Best-in-class; sets the standard for autonomous, cryptographically-verified zero-trust networking

Weighting

Category	Weight	Rationale
Identity-Aware Networking (SPIFFE)	25%	IP-based trust is the root cause of lateral movement
Encryption in Transit & PQC Readiness	20%	Unencrypted East-West traffic is an open book
NAC & Dynamic Posture Enforcement	15%	Unassessed devices are attack vectors
AI Agent Network Isolation	15%	Agents are high-risk workloads
ZTNA & Application Access	15%	VPNs provide excessive network access
Operational Lifecycle & DNS Security	10%	DNS is the most abused protocol

Total: 100%

A system MUST score at least 3.0 in Identity-Aware Networking and Encryption in Transit to be considered for production use.

EVALUATION AND ASSURANCE SYSTEM

Capability claims are bounded by evidence, context, and reproducible assessment.

10 atomic criteria across 6 capability families define the evaluation surface of this standard.

4.1 / CAPABILITY FAMILY

Identity-Aware Networking

SOURCE WEIGHT 25%

4.1.1
Cryptographic Workload Identity

4.1.2
User-to-Workload Binding

MYTHOS-NET-0004-EVAL-4.1.1

Cryptographic Workload Identity

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Identity-Aware Networking	**4.1.1**	**25%**	**Evidence-led**

Does the network fabric bind policy to cryptographic identity (SPIFFE/SPIRE) rather than IP addresses?

0
All policies based on static IP addresses

1
Service accounts exist but network policy still uses IPs

2
mTLS used for application layer; network layer still IP-dependent

3
Network fabric ingests SPIFFE IDs for policy enforcement (e.g., Cilium)

4
Network policy is 100% identity-aware; IPs are dynamic and irrelevant

5
Leading identity: formally verified mapping of cryptographic identity to network flows, zero IP-based rules, and automatic policy rotation with SVIDs

ENGINEERING INTERPRETATION

This criterion evaluates whether cryptographic workload identity is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- cryptographic inventory, algorithm registry, key records, certificate data, and compatibility tests
- approved architecture or policy record
- current configuration or platform export

ASSESSMENT PROCEDURE

1. test rotation, hybrid negotiation, rollback, revocation, and algorithm-policy enforcement
2. Examine authoritative design, policy, configuration, and lifecycle records.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- hardcoded algorithms, unknown dependencies, missing rollback, and unverifiable keys
- The control exists only in diagrams or policy text.

OPERATIONAL MEASURES

- inventory coverage
- deprecated algorithm count
- rotation success rate
- coverage of in-scope assets or flows

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

MYTHOS-NET-0004-EVAL-4.1.2

User-to-Workload Binding

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Identity-Aware Networking	4.1.2	25%	Evidence-led

Can the network trace a flow from a human user identity through to a specific workload?

0
No user-to-workload mapping

1
Logs correlate via IP addresses

2
Identity-aware proxies (Envoy) provide L7 user context

3
Network fabric tags packets with user identity context

4
Full chain: User OIDC token → Service SVID → Network Flow logged in Clio

5
Leading binding: cryptographic attestation of the entire user-to-workload path, zero unattributable network flows

ENGINEERING INTERPRETATION

This criterion evaluates whether user-to-workload binding is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.2 / CAPABILITY FAMILY

Encryption in Transit and PQC Readiness

SOURCE WEIGHT 20%

4.2.1
East-West Encryption

4.2.2
PQC Network Readiness

MYTHOS-NET-0004-EVAL-4.2.1

East-West Encryption

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Encryption in Transit and PQC Readiness	**4.2.1**	**20%**	**Evidence-led**

Is internal network traffic (East-West) encrypted at the link or network layer?

0
Unencrypted internal traffic

1
Application-layer encryption (TLS) only where enforced by app

2
Overlay encryption (IPSec/WireGuard) for cross-zone traffic

3
Hop-by-hop MACsec on all physical links within data centers

4
Combined MACsec (L2) + mTLS (L7) for defense in depth

5
Leading encryption: MACsec + mTLS + PQC hybrid key exchange, formally verified cryptographic boundaries, zero unencrypted internal traffic

ENGINEERING INTERPRETATION

This criterion evaluates whether east-west encryption is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

MYTHOS-NET-0004-EVAL-4.2.2

PQC Network Readiness

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Encryption in Transit and PQC Readiness	4.2.2	20%	Evidence-led

Are network control planes and data planes ready for Post-Quantum Cryptography?

0
Classical crypto only (RSA, ECC)

1
PQC evaluated but not implemented

2
PQC-enabled TLS terminations at edge

3
Hybrid classical+PQC key exchange (e.g., X25519+ML-KEM) for control plane (BGP, gNMI)

4
Hybrid PQC for data plane overlays (IPSec/WireGuard)

5
Leading PQC readiness: full hybrid PQC for L2/L3/L7, crypto-agile algorithm registries, and PQC-attested MACsec

ENGINEERING INTERPRETATION

This criterion evaluates whether pqc network readiness is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- cryptographic inventory, algorithm registry, key records, certificate data, and compatibility tests
- approved architecture or policy record
- current configuration or platform export

ASSESSMENT PROCEDURE

1. test rotation, hybrid negotiation, rollback, revocation, and algorithm-policy enforcement
2. Examine authoritative design, policy, configuration, and lifecycle records.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- hardcoded algorithms, unknown dependencies, missing rollback, and unverifiable keys
- The control exists only in diagrams or policy text.

OPERATIONAL MEASURES

- inventory coverage
- deprecated algorithm count
- rotation success rate
- coverage of in-scope assets or flows

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.3 / CAPABILITY FAMILY

NAC and Dynamic Posture Enforcement

SOURCE WEIGHT 15%

4.3.1
Dynamic Access Control

4.3.2
Quarantine Enforcement

MYTHOS-NET-0004-EVAL-4.3.1

Dynamic Access Control

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
NAC and Dynamic Posture Enforcement	**4.3.1**	**15%**	**Evidence-led**

Does the network dynamically assign access based on device posture and identity?

0
No NAC; any device can connect

1
Basic 802.1X but static VLAN assignment

2
Dynamic VLAN assignment based on RADIUS attributes

3
Dynamic VLAN + posture assessment (OS patch level, EDR status)

4
Continuous posture reassessment; dynamic quarantine on degradation

5
Leading NAC: continuous posture, cryptographic device identity (TPM/EK), automatic quarantine, and zero static network assignments

ENGINEERING INTERPRETATION

This criterion evaluates whether dynamic access control is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

MYTHOS-NET-0004-EVAL-4.3.2

Quarantine Enforcement

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
NAC and Dynamic Posture Enforcement	4.3.2	15%	Evidence-led

Can the network instantly isolate a compromised device without manual intervention?

0
Manual cable pull or switch port shutdown

1
Manual reassignment to quarantine VLAN

2
Automated quarantine triggered by SIEM alert

3
Automated quarantine triggered by EDR/XDR in real-time

4
Micro-quarantine: isolating only the compromised process/port, not the whole device

5
Leading quarantine: formally verified isolation, automatic forensic capture, and zero lateral movement capability

ENGINEERING INTERPRETATION

This criterion evaluates whether quarantine enforcement is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.4 / CAPABILITY FAMILY

AI Agent Network Isolation

SOURCE WEIGHT 15%

4.4.1
Agent Egress Control

4.4.2
Agent Data Path Isolation

MYTHOS-NET-0004-EVAL-4.4.1

Agent Egress Control

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
AI Agent Network Isolation	4.4.1	15%	Evidence-led

Are AI agents restricted to minimum necessary network access?

0
Agents have broad, unmonitored network access

1
Agents are in a separate VLAN but with broad egress

2
Agents have explicit allow-list egress rules

3
Egress is identity-scoped per task (capability-based networking)

4
Agents are routed through ZTNA proxies; no direct network access

5
Leading isolation: ephemeral network identities, per-task egress scopes, cryptographic attestation of network flows, and automatic quarantine on anomaly

ENGINEERING INTERPRETATION

This criterion evaluates whether agent egress control is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

MYTHOS-NET-0004-EVAL-4.4.2

Agent Data Path Isolation

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
AI Agent Network Isolation	4.4.2	15%	Evidence-led

Are the network paths used by AI agents to access sensitive data isolated from production traffic?

0
Agents share production data paths

1
Agents use separate VLANs

2
Agents use VRF-lite or separate VRFs

3
Agents use encrypted overlays (VXLAN/IPSec) with separate routing tables

4
Agents use dedicated compute + network fabrics (SR-IOV with isolated VFs)

5
Leading isolation: hardware-enforced paths (DPU offload), zero shared state, and formally verified path separation

ENGINEERING INTERPRETATION

This criterion evaluates whether agent data path isolation is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.5 / CAPABILITY FAMILY

ZTNA and Application Access

SOURCE WEIGHT 15%

MYTHOS-NET-0004-EVAL-4.5.1

Remote Access Architecture

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
ZTNA and Application Access	4.5.1	15%	Evidence-led

Has the organization replaced VPNs with Zero-Trust Network Access (ZTNA)?

0
Full-tunnel VPN providing excessive network access

1
Split-tunnel VPN but broad internal access

2
ZTNA for third-party/contractor access; VPN for employees

3
ZTNA for all human access; VPN deprecated

4
ZTNA with continuous posture checking and micro-segmented application access

5
Leading ZTNA: per-resource cryptographic identity, continuous behavioral analysis, and zero implicit network trust

ENGINEERING INTERPRETATION

This criterion evaluates whether remote access architecture is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.6 / CAPABILITY FAMILY

Operational Lifecycle and DNS Security

SOURCE WEIGHT 10%

4.6.1
DNS Security

MYTHOS-NET-0004-EVAL-4.6.1

DNS Security

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Operational Lifecycle and DNS Security	4.6.1	10%	Evidence-led

Is DNS traffic encrypted and validated?

0
Unencrypted DNS (Port 53) with no validation

1
DNSSEC validation for external zones

2
DoH (DNS over HTTPS) or DoT (DNS over TLS) for clients

3
DoH/DoT + DNSSEC for all internal and external resolution

4
Encrypted DNS + zero-trust DNS policy (filtering, RPZ)

5
Leading DNS: PQC-encrypted DNS, cryptographic DNS identity, zero plaintext DNS queries, and formally validated DNS paths

ENGINEERING INTERPRETATION

This criterion evaluates whether dns security is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

LIFECYCLE AND ASSURANCE

Part V. The Mythos Zero-Trust Networking Suite (MZTNS)

Traditional network benchmarks measure throughput and latency. The MZTNS evaluates identity binding, encryption coverage, and quarantine efficacy.

5.1 Suite Composition

5.1.1 MZTNS-Identity

- **IP Spoofing:** 100+ tests attempting to bypass network policy by spoofing IP addresses (must fail if identity-aware).
- **SVID Rotation:** 50+ tests verifying network policy dynamically updates when SPIFFE SVIDs rotate.

5.1.2 MZTNS-Encryption

- **Unencrypted Flow Detection:** 100+ tests verifying no internal traffic passes without MACsec or mTLS.
- **PQC Downgrade:** 50+ tests attempting to force classical crypto negotiation (must fail).

5.1.3 MZTNS-Quarantine

- **Rogue Device:** 50+ tests connecting unauthorized devices to verify NAC quarantine.
- **Agent Anomaly:** 50+ tests simulating agent network scanning to verify automatic egress quarantine.

5.2 Execution Protocol

PUBLICATION BOUNDARY

Candidate standard. Permanent identity. Evidence before authority.

Approval requires designated technical, security, legal, accessibility, and governance review with recorded findings and dispositions.