MYTHOS SYSTEMS

PERMANENT LIBRARY PUBLICATION

ENGINEERING STANDARDS LIBRARY / NETWORK ENGINEERING

Access, NAC, Wireless, and RF Engineering Standard

Defines access switching, 802.1X, profiling, wireless design, RF, roaming, and validation.

PERMANENT DOCUMENT ID
MYTHOS-NET-0011

PUBLICATION
Candidate Standard

ASSURANCE SURFACE
6 Atomic Criteria / 6 Families

PERMANENT PUBLICATION IDENTITY

Access, NAC, Wireless, and RF Engineering Standard

Defines access switching, 802.1X, profiling, wireless design, RF, roaming, and validation.

DOCUMENT ID
MYTHOS-NET-0011

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-23

SCHEDULED REVIEW
2027-01-23

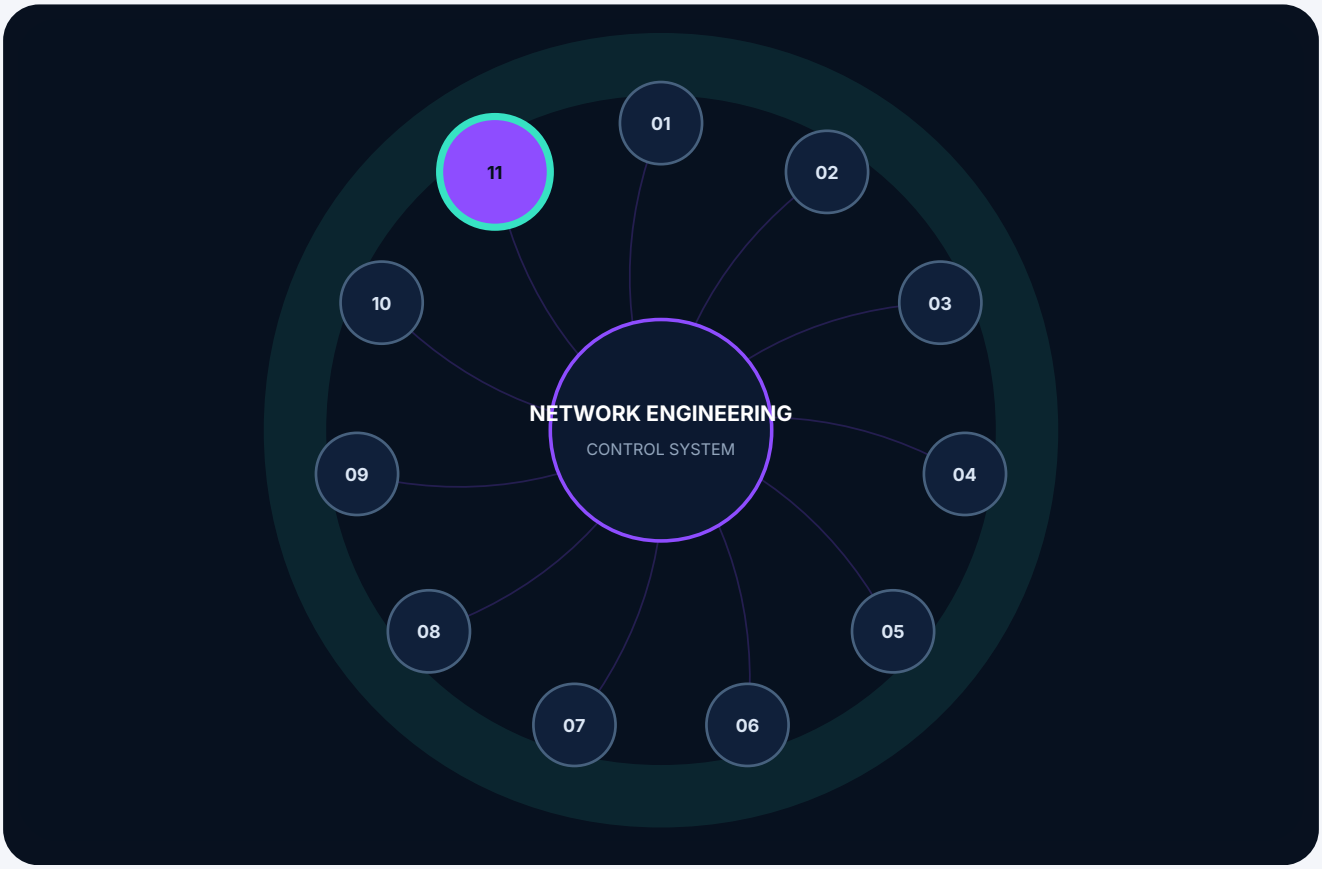
CLASSIFICATION
Public

6	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-0011 inside the network engineering standard constellation



Connected assurance

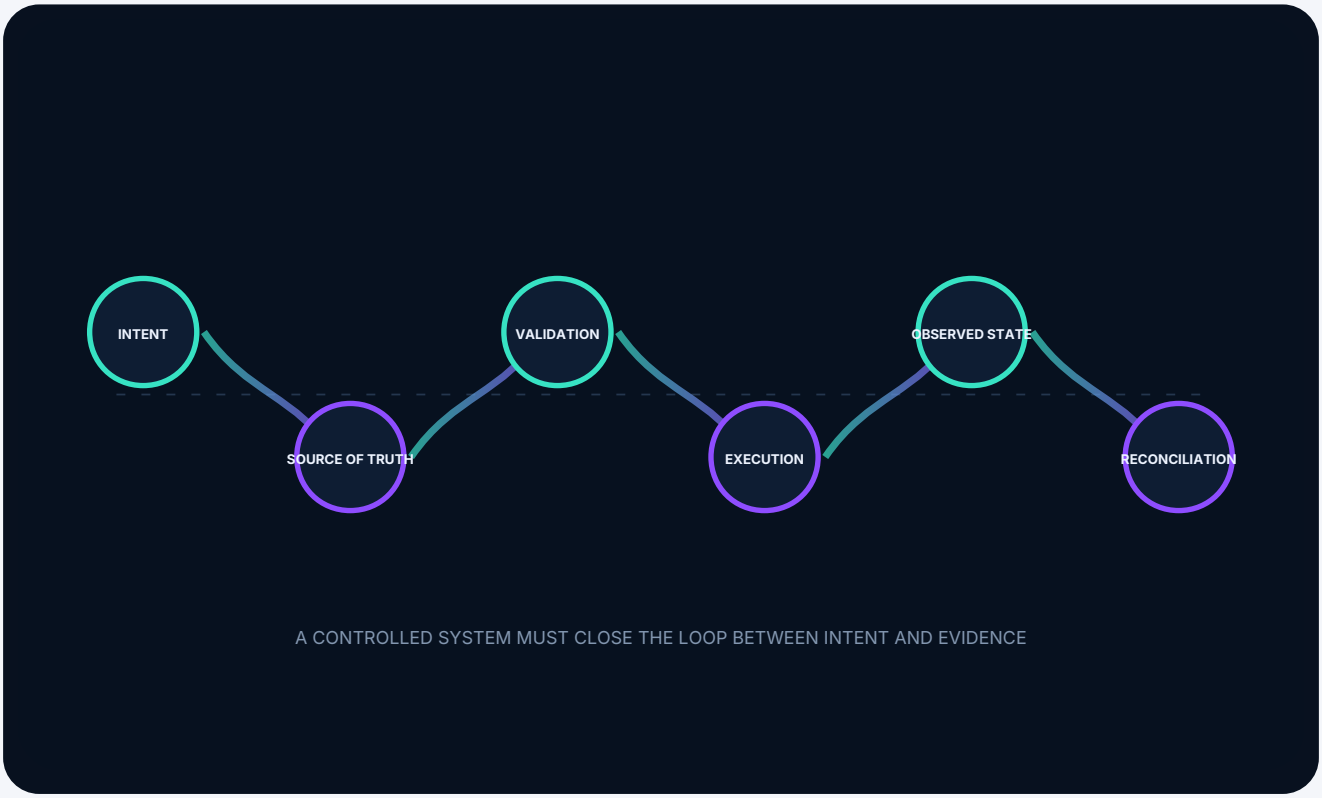
Architecture, policy, implementation, operations, and evidence are evaluated as one controlled system.

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-0011

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 architecture of network access has failed.

Organizations continue to secure their internal networks using flat Layer 2 VLANs and Pre-Shared Keys (PSKs) for Wi-Fi. They grant remote access via legacy VPNs that put unmanaged, potentially compromised devices directly onto the corporate LAN. When a single device is compromised, the attacker instantly gains lateral movement access to the entire flat network, bypassing all perimeter firewalls.

This standard exists because:

1. **PSKs and MAC Auth are Security Theater:** A Wi-Fi PSK is shared, leaks to departing employees, and is easily cracked. MAC authentication is trivially spoofed. Network access MUST be predicated on cryptographic identity (802.1X / EAP-TLS), not shared strings or burned-in hardware addresses.
2. **VPNs are Perimeter Anachronisms:** A VPN grants Layer 3 network access based on a single cryptographic check. Once connected, the user has the keys to the kingdom. Systems MUST replace VPNs with Zero Trust Network Access (ZTNA), which grants Layer 7 application access based on continuous identity and device posture verification.
3. **Flat Networks Breed Ransomware:** A network where an authenticated device can reach any other device is a ransomware acceleration vector. NAC MUST be used to dynamically assign devices to microsegmented VLANs or Software-Defined Perimeters based on their identity, role, and real-time security posture.
4. **Wi-Fi is a Physical Attack Surface:** RF signals do not respect physical walls. An attacker in the parking lot can launch deauthentication attacks, spin up Evil Twins, or exploit WPA3 downgrade vulnerabilities. Wireless engineering MUST include Wireless Intrusion Prevention (WIPS), spectrum analysis, and strict certificate pinning.

This document establishes the **Mythos Access & NAC Standard (MANS)**, a comprehensive, evidence-based methodology for evaluating network access architectures against identity-based isolation, continuous posture validation, and RF resilience.

ENGINEERING DOCTRINE

Part I. Scope and Applicability

1.1 In Scope

This standard covers the evaluation of:

- Network Access Control (NAC) platforms (Cisco ISE, Aruba ClearPass, Forescout)
- 802.1X authentication (EAP-TLS, EAP-PEAP) and RADIUS/TACACS+
- Wireless engineering (Wi-Fi 6E/7, WPA3-Enterprise, OWE, 6GHz spectrum)
- Zero Trust Network Access (ZTNA) and SASE/SSE architectures
- Device posture attestation (TPM, Secure Boot, EDR status)
- Wireless Intrusion Prevention Systems (WIPS) and RF spectrum analysis

1.2 Out of Scope

- General network routing and IPAM (covered in MYTHOS-NET-0010)
- General zero-trust policy architecture (covered in MYTHOS-SEC-0003)
- Endpoint OS hardening (covered in MYTHOS-END-0001)

1.3 Audience

- Network access engineers and WLAN architects
- Security engineers designing NAC and ZTNA pipelines
- Platform engineers managing device fleet onboarding
- Standards bodies seeking a reference access control methodology

---

ENGINEERING DOCTRINE

Part II. Definitions and Taxonomy

2.1 Access Dimensions

Dimension	Definition
802.1X	The IEEE standard for port-based Network Access Control, requiring authentication before a switch port or WLAN allows traffic.
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security. The most secure 802.1X protocol, requiring mutual cryptographic certificate validation by both the client and the authentication server.
ZTNA (Zero Trust Network Access)	A security paradigm replacing VPNs, granting contextual, application-level access based on user identity and device posture, without exposing the corporate L3 network.
Device Posture Attestation	The process of cryptographically verifying the security state (e.g., TPM measurements, EDR running, OS patched) of a device before granting it network access.
Evil Twin	A fraudulent wireless access point that imitates a legitimate one, often using the same SSID, to capture credentials or execute Man-in-the-Middle (MITM) attacks.

2.2 The Access Control Doctrine

> A PSK is a shared liability. A VPN is a wide-open door. A flat VLAN is a ransomware superhighway. If the device is not attested, the network is compromised.

ENGINEERING DOCTRINE

Part III. Evaluation Methodology

3.1 Scoring Model

Each capability is scored from 0 to 5.

Score	Meaning
0	Fails basic task; PSKs, flat networks, traditional VPNs, no NAC
1	Basic 802.1X exists, but allows MAC auth fallback and flat VLANs
2	Functional NAC, but lacks continuous posture checks or ZTNA
3	Solid production performance; EAP-TLS enforced, dynamic VLANs, ZTNA, WPA3-Enterprise
4	Strong performance; TPM attestation, WIPS, automated quarantine, 6GHz Wi-Fi 7
5	Best-in-class; sets the standard for mathematically verified, zero-trust network access

Weighting

Category	Weight	Rationale
Identity-Based Access (802.1X/NAC)	20%	PSKs and MAC auth cannot guarantee identity
ZTNA & VPN Replacement	20%	Legacy VPNs grant excessive lateral movement access
Dynamic Microsegmentation	15%	Flat networks allow unchecked ransomware spread
Device Posture & Attestation	15%	A compromised device with valid credentials is a threat
Wireless Security (WPA3/RF)	15%	Wi-Fi is a physical boundary; downgrades and Evil Twins are constant threats
Device Admin (RADIUS/TACACS+)	15%	Local device accounts prevent centralized auditing

Total: 100%

A system MUST score at least 3.0 in Identity-Based Access and ZTNA to be considered for production use.

EVALUATION AND ASSURANCE SYSTEM

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

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

4.1 / CAPABILITY FAMILY

Identity-Based Access (802.1X / NAC)

SOURCE WEIGHT 20%

4.1.1
Authentication Rigor

MYTHOS-NET-0011-EVAL-4.1.1

Authentication Rigor

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Identity-Based Access (802.1X / NAC)	4.1.1	20%	Evidence-led

Is network access predicated on cryptographic identity rather than shared secrets?

0
Open Wi-Fi or WPA2-PSK; switches use MAC authentication bypass (MAB)

1
802.1X using PEAP-MSCHAPv2 (vulnerable to rogue RADIUS/AP attacks)

2
EAP-TLS enforced for corporate devices, but IoT devices use PSK

3
EAP-TLS enforced for all entities (humans, devices, IoT); zero MAC auth fallback

4
Continuous authentication: session keys rotated and validated periodically; not just at join time

5
Leading identity: formally verified cryptographic bounds, zero ability to spoof identity, hardware-bound client certificates

ENGINEERING INTERPRETATION

This criterion evaluates whether authentication rigor 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.

4.2 / CAPABILITY FAMILY

ZTNA and VPN Replacement

SOURCE WEIGHT 20%

MYTHOS-NET-0011-EVAL-4.2.1

Remote Access Architecture

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
ZTNA and VPN Replacement	**4.2.1**	**20%**	**Evidence-led**

Are remote users granted network access or application access?

0
Traditional IPsec/SSL VPN placing clients on the flat L3 corporate LAN

1
VPN with split-tunneling, but lateral movement is still possible

2
Basic ZTNA deployed, but coexists with VPN (legacy crutch)

3
100% ZTNA: VPNs removed from the controlled workflow; users connect via identity-aware proxy to specific L7 applications

4
Continuous ZTNA: access is re-evaluated on every request; idle sessions are terminated

5
Leading isolation: formally verified L7 boundaries, zero L3 network exposure, cryptographic proof of application isolation

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.

4.3 / CAPABILITY FAMILY

Dynamic Microsegmentation

SOURCE WEIGHT 15%

4.3.1
Lateral Movement Prevention

MYTHOS-NET-0011-EVAL-4.3.1

Lateral Movement Prevention

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Dynamic Microsegmentation	4.3.1	15%	Evidence-led

Can a compromised device communicate with unrelated devices on the same network?

0
Single flat corporate VLAN; any device can ping any other device

1
Basic VLAN segmentation by department (e.g., HR, IT), but broad internal access

2
NAC assigns VLANs dynamically based on identity

3
Software-Defined Perimeter (SDP) or dynamic microsegmentation (Cisco TrustSec/Cilium); devices can only reach explicitly allowed resources

4
Real-time policy updates: if device posture changes, NAC instantly moves it to a quarantine VLAN

5
Leading segmentation: formally verified zero-trust east-west traffic, zero lateral movement possible, mathematical proof of isolation

ENGINEERING INTERPRETATION

This criterion evaluates whether lateral movement prevention 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

- zone and identity model, policy graph, enforcement exports, and east-west telemetry
- approved architecture or policy record
- current configuration or platform export

ASSESSMENT PROCEDURE

1. test intended and prohibited flows across normal and degraded conditions
2. Examine authoritative design, policy, configuration, and lifecycle records.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- VLAN-only assumptions, transitive access, broad service accounts, and undocumented bypass
- The control exists only in diagrams or policy text.

OPERATIONAL MEASURES

- policy coverage
- prohibited-flow success rate
- exception age
- 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.

4.4 / CAPABILITY FAMILY

Device Posture and Attestation

SOURCE WEIGHT 15%

4.4.1
Health Verification

MYTHOS-NET-0011-EVAL-4.4.1

Health Verification

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Device Posture and Attestation	**4.4.1**	**15%**	**Evidence-led**

Is the security state of the device verified before and during network access?

0
No posture checks; any device with a valid cert is admitted

1
Basic agent checks if antivirus is running

2
OS patch level and EDR status verified at connection time

3
Hardware-backed attestation (TPM 2.0) verifying Secure Boot and OS integrity via RADIUS extensions

4
Continuous posture monitoring; degraded posture instantly triggers NAC quarantine

5
Leading attestation: formally verified hardware roots of trust, zero ability to bypass posture agents, cryptographic proof of system integrity

ENGINEERING INTERPRETATION

This criterion evaluates whether health verification 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

- attestation evidence, endorsement chain, measurement policy, key-release logs, and verifier records
- approved architecture or policy record
- current configuration or platform export

ASSESSMENT PROCEDURE

1. test valid, stale, revoked, mismatched, and unavailable attestation paths
2. Examine authoritative design, policy, configuration, and lifecycle records.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- trusting self-asserted state, stale measurements, and fail-open key release
- The control exists only in diagrams or policy text.

OPERATIONAL MEASURES

- attestation coverage
- verification failure rate
- revocation propagation
- 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.

4.5 / CAPABILITY FAMILY

Wireless Security and RF

SOURCE WEIGHT 15%

4.5.1
Airwave Integrity

MYTHOS-NET-0011-EVAL-4.5.1

Airwave Integrity

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Wireless Security and RF	4.5.1	15%	Evidence-led

Is the wireless infrastructure resilient to RF attacks and downgrades?

0
WPA2-PSK; no RF monitoring

1
WPA3 supported, but allows WPA2 transition mode (vulnerable to Dragonblood downgrade)

2
WPA3-Enterprise strictly enforced; 802.11w (PMF) mandatory

3
Wi-Fi 6E/7 (6GHz) utilized for spectrum relief; WIPS detecting and containing Evil Twins

4
Client certificate pinning preventing rogue RADIUS MITM; spectrum AI auto-optimizing channels/power

5
Leading integrity: formally verified cryptographic handshakes, zero downgrade capability, real-time geofencing of RF boundaries

ENGINEERING INTERPRETATION

This criterion evaluates whether airwave integrity 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

- RF survey, channel and power plan, authentication logs, and client telemetry
- approved architecture or policy record
- current configuration or platform export

ASSESSMENT PROCEDURE

1. test roaming, capacity, interference, authentication, and degraded-band behavior
2. Examine authoritative design, policy, configuration, and lifecycle records.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- coverage holes, sticky clients, co-channel interference, and insecure fallback
- The control exists only in diagrams or policy text.

OPERATIONAL MEASURES

- coverage compliance
- authentication success
- roaming interruption
- airtime utilization
- 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.

4.6 / CAPABILITY FAMILY

Device Admin (RADIUS/ TACACS+)

SOURCE WEIGHT 15%

4.6.1
Infrastructure Access Control

MYTHOS-NET-0011-EVAL-4.6.1

Infrastructure Access Control

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Device Admin (RADIUS/ TACACS+)	4.6.1	15%	Evidence-led

How are engineers authenticated to network devices (switches, routers)?

0
Local accounts on every switch/router; shared passwords

1
Centralized TACACS+/RADIUS, but uses shared passwords

2
Centralized auth with individual named accounts (RADIUS/TACACS+)

3
Just-in-Time (JIT) access: engineers check out a time-boxed session via PAM; commands logged via TACACS+

4
Command-level authorization (TACACS+); dangerous commands (e.g., `reload`, `write erase`) require dual-control

5
Leading governance: formally verified zero local accounts, cryptographic attestation of admin sessions, zero unlogged CLI actions

ENGINEERING INTERPRETATION

This criterion evaluates whether infrastructure 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.

LIFECYCLE AND ASSURANCE

Part V. The Mythos Access & NAC Suite (MANS)

Traditional network benchmarks measure authentication latency. The MANS evaluates posture enforcement, lateral movement resistance, and RF attack resilience.

5.1 Suite Composition

5.1.1 MANS-Access

- **Rogue Device Test:** 100+ tests attempting to connect a device without a valid client certificate, verifying NAC blocks it at the port level.
- **Posture Degradation Test:** 50+ tests disabling EDR or altering firewall rules on an active device, verifying NAC instantly quarantines it.

5.1.2 MANS-Wireless

- **Evil Twin Simulation:** 100+ tests spinning up a high-power Rogue AP with the same SSID, verifying WIPS detects and contains it, and clients refuse to connect.
- **Downgrade Attempt:** 50+ tests forcing a WPA2 fallback, verifying the client strictly requires WPA3 and drops the connection.

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.