MYTHOS SYSTEMS

PERMANENT LIBRARY PUBLICATION

ENGINEERING STANDARDS LIBRARY / CYBERSECURITY AND NETWORK SECURITY

DMZ, Perimeter, Remote Access, and Isolation Standard

Defines exposed services, segmentation, access, inspection, monitoring, resilience, and validation.

PERMANENT DOCUMENT ID
MYTHOS-SEC-0017

PUBLICATION
Candidate Standard

ASSURANCE SURFACE
6 Atomic Criteria / 6 Families

PERMANENT PUBLICATION IDENTITY

DMZ, Perimeter, Remote Access, and Isolation Standard

Defines exposed services, segmentation, access, inspection, monitoring, resilience, and validation.

DOCUMENT ID
MYTHOS-SEC-0017

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-23

SCHEDULED REVIEW
2027-01-23

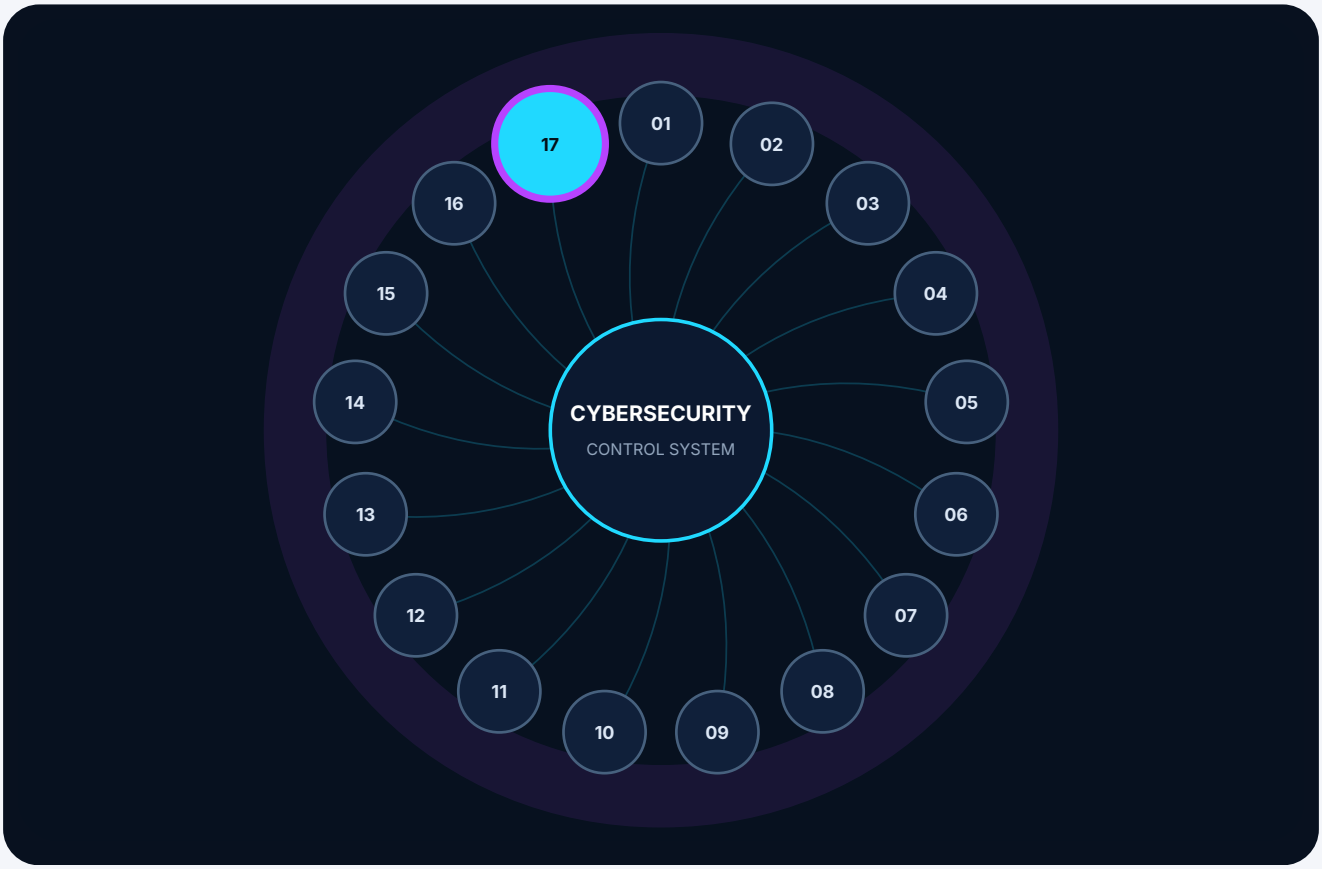
CLASSIFICATION
Public

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-SEC-0017 inside the cybersecurity and network security standard constellation



Connected assurance

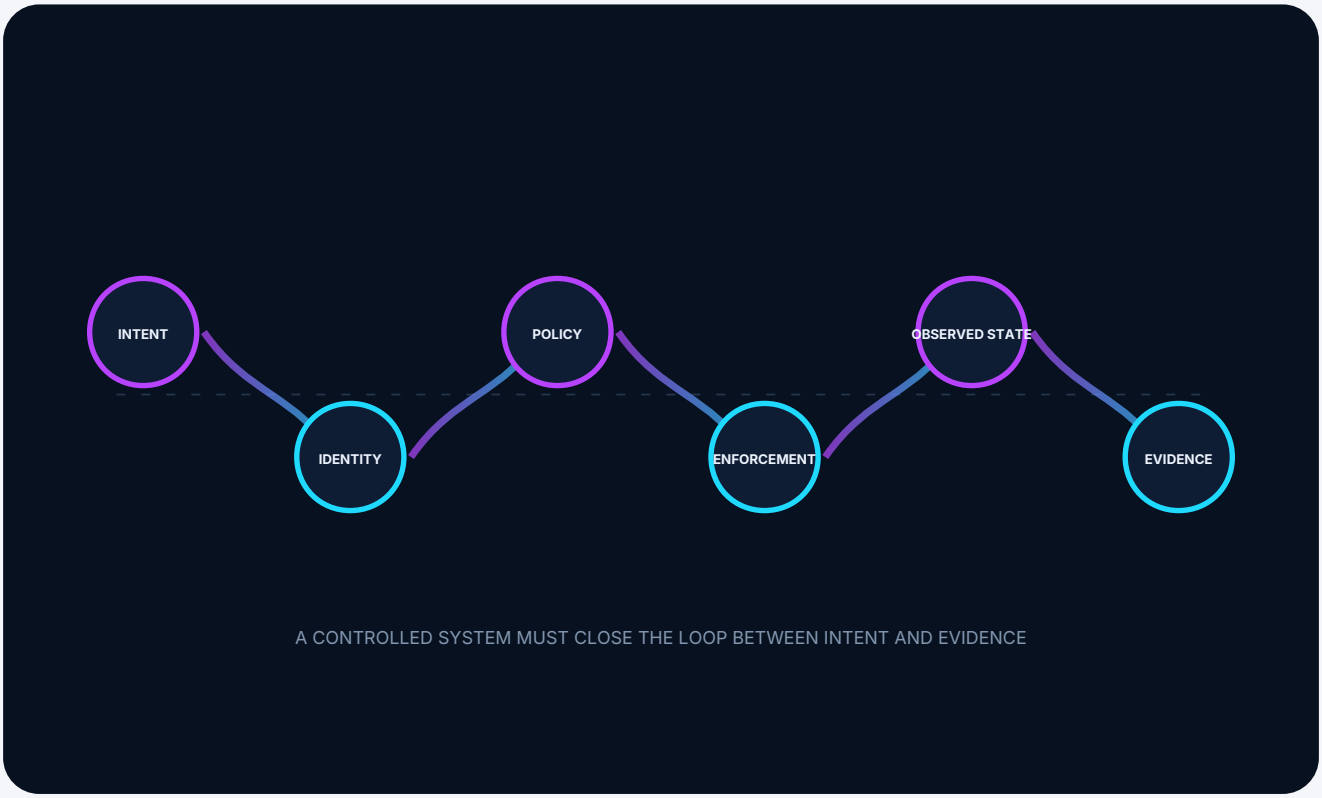
Architecture, policy, implementation, operations, and evidence are evaluated as one controlled system.

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-SEC-0017

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 perimeter isolation has failed.

Organizations attempt to secure external-facing services by connecting them to the internet via a single firewall device utilizing a "triple-homed" design (Internet, DMZ, Internal). When a vulnerability in the DMZ web server is inevitably exploited, the attacker instantly has a direct network path to the corporate internal network, bypassing the perimeter entirely. Furthermore, to ease application connectivity, developers place databases directly in the DMZ alongside the web servers. When the web server is breached, the database is immediately exfiltrated.

This standard exists because:

1. **Single-Firewall DMZs are a Single Point of Failure:** A triple-homed firewall relies on the OS of a single device to separate untrusted attackers from the corporate crown jewels. If the firewall OS is compromised, or a routing rule is misconfigured, the internal network is instantly exposed. Systems MUST implement dual-firewall back-to-back architectures or abolish the physical DMZ entirely in favor of Zero-Trust Network Access (ZTNA).
2. **The "Zero Database Rule" is Absolute:** Databases contain the data; web servers render it. Placing a database in a DMZ is an unconditional security failure. Databases MUST reside in the highly restricted internal zone, and DMZ application servers MUST only communicate with them over strictly bounded, unidirectional firewall ports.
3. **Security Appliances Break High-Performance Computing (HPC):** Standard DMZs force all traffic through stateful inspection firewalls and IPS appliances. For massive scientific data transfers (e.g., genome sequencing, particle physics), this stateful tracking causes catastrophic packet loss and latency. HPC fabrics MUST utilize a Science DMZ that physically bypasses stateful security appliances.
4. **IT/OT Convergence is a Physical Threat:** Connecting corporate IT networks to Operational Technology (OT) networks via a standard DMZ allows ransomware to pivot into physical infrastructure (power grids, manufacturing). OT boundaries MUST utilize an Industrial DMZ (iDMZ) enforcing the Purdue Model, with absolutely no direct routing between IT and OT.

This document establishes the **Mythos Perimeter Standard (MPS)**, a comprehensive, evidence-based methodology for evaluating DMZ architectures against defense-in-depth, data sovereignty, and physics-aware isolation.

ENGINEERING DOCTRINE

Part I. Scope and Applicability

1.1 In Scope

This standard covers the evaluation of:

- Standard Enterprise DMZs (Dual-firewall, Back-to-back)
- The "Zero Database Rule" and application tiering
- Science DMZs for High-Performance Computing (HPC) and research data transfers
- Industrial DMZs (iDMZ) for IT/OT separation under the Purdue Model (ISA-99/IEC 62443)
- Zero-Trust Network Access (ZTNA) as a DMZ alternative/overlay

1.2 Out of Scope

- General firewall rule management (covered in MYTHOS-SEC-0006)
- General microsegmentation of internal east-west traffic (covered in MYTHOS-SEC-0007)
- Internal SCADA/PLC security hardening (covered in MYTHOS-OT-0001)

1.3 Audience

- Network architects and security engineers designing perimeter defenses
- HPC and research compute engineers managing massive data transfers
- OT/ICS engineers managing industrial boundaries
- Cloud architects replacing physical DMZs with ZTNA overlays
- Standards bodies seeking a reference DMZ methodology

ENGINEERING DOCTRINE

Part II. Definitions and Taxonomy

2.1 Perimeter Dimensions

Dimension	Definition
Dual-Firewall DMZ	An architecture where the DMZ is "sandwiched" between an external firewall (facing the internet) and an internal firewall (facing the corporate network), providing defense-in-depth.
Zero Database Rule	The architectural absolute that persistent data stores (databases) must never reside in the DMZ. Only stateless application servers are permitted in the DMZ.
Science DMZ	A specialized network perimeter designed for high-performance computing, bypassing stateful security appliances in favor of dedicated Data Transfer Nodes (DTNs) and precise Access Control Lists (ACLs) to achieve maximum throughput.
Industrial DMZ (iDMZ)	A buffer zone (Purdue Level 3.5) separating enterprise IT networks from Industrial Control Systems (ICS) networks. No direct routing is permitted; all traffic must terminate and be proxied.
Data Transfer Node (DTN)	A specialized, high-performance server in a Science DMZ equipped with high-speed network interfaces and tuned TCP buffers, designed to maximize data transfer throughput over long distances.

2.2 The Perimeter Doctrine

> A triple-homed firewall is a single point of compromise. A database in the DMZ is a breach waiting to happen. A stateful firewall in front of an HPC cluster is a bottleneck. If IT can route to OT, the plant is a bomb.

ENGINEERING DOCTRINE

Part III. Evaluation Methodology

3.1 Scoring Model

Each capability is scored from 0 to 5.

Score	Meaning
0	Fails basic task; triple-homed firewall, databases in DMZ, IT/OT direct routing
1	Basic dual-firewall, but lacks Zero Database Rule or HPC/OT specializations
2	Functional DMZ, but relies on legacy proxies or lacks Science/iDMZ segmentation
3	Solid production performance; Dual-firewall (or ZTNA), Zero DB Rule, Science DMZ, iDMZ Purdue enforcement
4	Strong performance; Multi-vendor dual-firewalls, unidirectional gateways for OT, formally verified ACLs
5	Best-in-class; sets the standard for mathematically verified, physics-aware perimeter isolation

Weighting

Category	Weight	Rationale
Perimeter Defense-in-Depth	20%	Single-firewall designs guarantee internal exposure upon compromise
The Zero Database Rule	20%	Databases in the DMZ guarantee massive data exfiltration
Science DMZ (HPC) Architecture	15%	Standard firewalls physically cannot handle 100Gbps+ research data
Industrial DMZ (iDMZ) & Purdue Model	15%	IT/OT convergence without an iDMZ allows physical destruction
Traffic Flow & Unidirectional Enforcement	15%	Bidirectional rules allow reverse shells and lateral movement
Zero-Trust Overlay Integration	15%	Physical DMZs are being replaced by identity-bound ZTNA overlays

Total: 100%

A system MUST score at least 3.0 in Perimeter Defense and the Zero Database Rule to be considered for production.

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

Perimeter Defense-in-Depth

SOURCE WEIGHT 20%

4.1.1
Firewall Topology

MYTHOS-SEC-0017-EVAL-4.1.1

Firewall Topology

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Perimeter Defense-in-Depth	4.1.1	20%	Evidence-led

How is the DMZ isolated from the external internet and the internal network?

0
Single triple-homed firewall device separates Internet, DMZ, and Internal

1
Single firewall, but highly hardened with strict ACLs

2
Dual-firewall back-to-back, but both from the same vendor (shared exploit risk)

3
Dual-firewall back-to-back utilizing different vendors (e.g., Palo Alto external, Fortinet internal)

4
Internal firewall enforces strict mTLS/ identity-aware proxies between DMZ and internal apps

5
Leading isolation: formally verified firewall rules, zero shared routing planes, mathematical proof of boundary integrity

ENGINEERING INTERPRETATION

This criterion evaluates whether firewall topology 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

- rulebase export, ownership matrix, hit counts, recertification records, and flow logs
- approved architecture or policy record
- current configuration or platform export

ASSESSMENT PROCEDURE

1. test allow, deny, shadowing, expiration, asymmetric flow, and failover scenarios
2. Examine authoritative design, policy, configuration, and lifecycle records.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- orphan rules, broad services, hidden shadowing, stale objects, and weak ownership
- The control exists only in diagrams or policy text.

OPERATIONAL MEASURES

- owned-rule coverage
- stale-rule count
- policy verification pass 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

The Zero Database Rule

SOURCE WEIGHT 20%

4.2.1
Data Sovereignty

MYTHOS-SEC-0017-EVAL-4.2.1

Data Sovereignty

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
The Zero Database Rule	4.2.1	20%	Evidence-led

Are persistent data stores and high-value assets isolated from the internet-facing tier?

0
Databases hosted in the DMZ alongside web servers (critical failure)

1
Databases in internal zone, but DMZ servers have broad SQL access (e.g., root DB user)

2
Databases in internal zone; DMZ servers restricted to specific tables/stored procedures

3
Absolute Zero Database Rule: DMZ contains only stateless API/web servers; DBs are deep internal

4
Internal DBs communicate with DMZ via message queues (e.g., Kafka) rather than direct SQL links

5
Leading sovereignty: Cryptographic data isolation, zero direct DMZ-to-DB protocols, mathematical proof of statelessness in the DMZ

ENGINEERING INTERPRETATION

This criterion evaluates whether data sovereignty 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

Science DMZ (HPC) Architecture

SOURCE WEIGHT 15%

4.3.1
High-Throughput Data Transfer

MYTHOS-SEC-0017-EVAL-4.3.1

High-Throughput Data Transfer

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Science DMZ (HPC) Architecture	**4.3.1**	**15%**	**Evidence-led**

How does the network handle massive, multi-gigabit research data transfers without packet loss?

0
All HPC traffic routed through standard stateful firewalls (causes catastrophic latency/loss)

1
Firewalls bypassed, but no dedicated Data Transfer Nodes (DTNs) utilized

2
Dedicated DTNs deployed, but lack proper TCP tuning (e.g., BBR, large window sizes)

3
True Science DMZ: Dedicated DTNs with 100Gbps+ interfaces, routed via dedicated switches with ACL-only (stateless) security

4
Integration with research networks (e.g., Internet2, ESnet); perfSONAR monitoring for multi-domain throughput tuning

5
Leading throughput: formally verified stateless routing, zero packet loss at 400Gbps, mathematical proof of optimal MTU/buffer tuning

ENGINEERING INTERPRETATION

This criterion evaluates whether high-throughput data transfer 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

Industrial DMZ (iDMZ) & Purdue Model

SOURCE WEIGHT 15%

4.4.1
IT/OT Boundary Enforcement

MYTHOS-SEC-0017-EVAL-4.4.1

IT/OT Boundary Enforcement

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Industrial DMZ (iDMZ) & Purdue Model	**4.4.1**	**15%**	**Evidence-led**

How is the corporate IT network separated from the Operational Technology (OT) network?

0
Direct routing between IT and OT networks (catastrophic physical risk)

1
Single firewall between IT and OT (violates Purdue Model)

2
Basic iDMZ (Purdue Level 3.5), but allows direct IP routing

3
Strict iDMZ: No direct routing between IT and OT; all traffic terminates at proxies/gateways in the iDMZ

4
Unidirectional data diodes utilized for OT-to-IT telemetry (physically prevents IT-to-OT inbound attacks)

5
Leading isolation: Formally verified Purdue model enforcement, zero inbound IT-to-OT routing capability, cryptographic attestation of physical boundaries

ENGINEERING INTERPRETATION

This criterion evaluates whether it/ot boundary 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.

4.5 / CAPABILITY FAMILY

Traffic Flow & Unidirectional Enforcement

SOURCE WEIGHT 15%

4.5.1
Connection Directionality

MYTHOS-SEC-0017-EVAL-4.5.1

Connection Directionality

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Traffic Flow & Unidirectional Enforcement	4.5.1	15%	Evidence-led

Are firewall rules configured to prevent reverse connections and lateral movement?

0
Broad "Any-to-Any" rules in the DMZ

1
Rules allow DMZ servers to initiate connections to the internal network

2
Internal network can initiate connections to DMZ, but DMZ is blocked from internal

3
Strict unidirectional flow: Internet → DMZ (external firewall), Internal → DMZ (internal firewall). DMZ cannot initiate outbound to Internal

4
DMZ servers stripped of outbound internet access (prevents reverse shells and data exfiltration)

5
Leading flow: Formally verified unidirectional ACLs, zero ability for DMZ to initiate external or internal connections, mathematical proof of blast radius containment

ENGINEERING INTERPRETATION

This criterion evaluates whether connection directionality 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

- rulebase export, ownership matrix, hit counts, recertification records, and flow logs
- approved architecture or policy record
- current configuration or platform export

ASSESSMENT PROCEDURE

1. test allow, deny, shadowing, expiration, asymmetric flow, and failover scenarios
2. Examine authoritative design, policy, configuration, and lifecycle records.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- orphan rules, broad services, hidden shadowing, stale objects, and weak ownership
- The control exists only in diagrams or policy text.

OPERATIONAL MEASURES

- owned-rule coverage
- stale-rule count
- policy verification pass 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.

4.6 / CAPABILITY FAMILY

Zero-Trust Overlay Integration

SOURCE WEIGHT 15%

4.6.1
DMZ Abolishment

MYTHOS-SEC-0017-EVAL-4.6.1

DMZ Abolishment

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Zero-Trust Overlay Integration	4.6.1	15%	Evidence-led

Is the physical DMZ being augmented or replaced by identity-bound overlays?

0
100% reliance on physical firewalls for perimeter security

1
Basic VPN concentrator in the DMZ (legacy remote access)

2
ZTNA deployed for remote users, but public-facing web servers still use physical DMZ

3
Public-facing services protected by SASE/SSE cloud proxies; physical DMZ footprint reduced to bare metal legacy apps

4
Micro-segmented DMZ: Every app server in the DMZ is wrapped in a WireGuard/mTLS mesh, requiring identity to communicate even within the DMZ

5
Leading integration: Physical DMZ removed from the controlled workflow entirely in favor of identity-bound ZTNA overlays; zero implicit trust based on IP address

ENGINEERING INTERPRETATION

This criterion evaluates whether dmz abolishment 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 Perimeter Suite (MPS)

Traditional benchmarks measure firewall throughput (Mbps). The MPS evaluates lateral movement resistance, HPC packet loss, and IT/OT isolation.

5.1 Suite Composition

5.1.1 MPS-Pivot

- **Web Server Compromise Test:** 100+ tests simulating a reverse shell on a DMZ web server, verifying the internal firewall blocks the connection from reaching the internal database.
- **Exfiltration Test:** 50+ tests attempting to initiate an outbound connection from the DMZ web server to an external attacker IP, verifying egress controls block the transfer.

5.1.2 MPS-Physics

- **HPC Throughput Soak:** 100+ tests pushing 100Gbps of TCP traffic through the Science DMZ for 24 hours, verifying zero packet loss and sub-millisecond latency (no stateful firewall intervention).
- **OT Boundary Test:** 50+ tests attempting to route an IT packet directly to a PLC IP address, verifying the iDMZ physically drops the packet and forces proxy termination.

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.