Institute of Security Architecture United

ASSOCIATE STANDARD

Firewall Engineering & Rule Management

July 2026

D01-AS-NS-1020

Disclaimer

ISAUnited publishes the ISAUnited Defensible 10 Standards to provide information and education on 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 standard 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 standard, 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 associate standard 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 circumstances, but the full implications must be understood and documented.

Acceptance of Terms

By using this associate standard, 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 Associate-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

Each Associate 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 Associate-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.

Contents

ISAUnited's Defensible 10 Standards
Associate-Standard: D01-AS-NS-1020-Firewall Engineering & Rule Management
Document: D01-AS-NS-1020_v1
Last Revision Date: July 2026
Peer-Reviewed By: ISAUnited Technical Fellow Society
Approved By: ISAUnited Standards Committee

1. Purpose and Scope

This Associate Standard defines mandatory requirements for designing, authorizing, implementing, reviewing, and retiring firewall rules at network enforcement points. It applies to physical, virtual, cloud-native, and software-defined firewalls and is intended to produce least-privilege, default-deny policies that are controlled, testable, logged, and traceable.

Applies to:

- Ingress, egress, inter-zone, cloud, and management-plane firewall enforcement.
- Firewall rule requests, approvals, implementation, testing, review, expiration, and retirement.
- Manual, automated, API-driven, and policy-as-code rule-management processes.

Does not apply to:

- Web application firewall rule development.
- Host-based endpoint firewall configuration.
- Network Access Control or Zero Trust Network Access implementation.

2. Parent Standard Flowdown

Flowdown Item	Source
Parent Standard	D01 — Network Security Architecture & Engineering
Applicable Requirements	§5.3 Firewall and Boundary Security Strategy; §5.7 Logging and Anomaly Detection; §5.8 Change and Configuration Control; §5.9 Baseline Alignment
Applicable Technical Specifications	§6.2 Firewall Engineering and Network Filtering; §6.5 Network Monitoring and Threat Detection
Core Principles	ISAU-RP-01 Least Privilege; RP-03 Complete Mediation; RP-04 Defense in Depth; RP-09 Fail-Safe Defaults; RP-10 Secure Defaults; RP-12 Security as Code; RP-15 Evidence Production; RP-19 Protect Integrity
Foundational Standards Inherited from Parent Standard	D01 §8: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27033, and NIST SP 800-41 Rev. 1
Security Controls Inherited from Parent Standard	D01 §9: CIS Controls v8 4.1–4.3 and 13.5; CSA CCM IAM-09

Flowdown Item	Source
Evidence Pack	EP-01.02

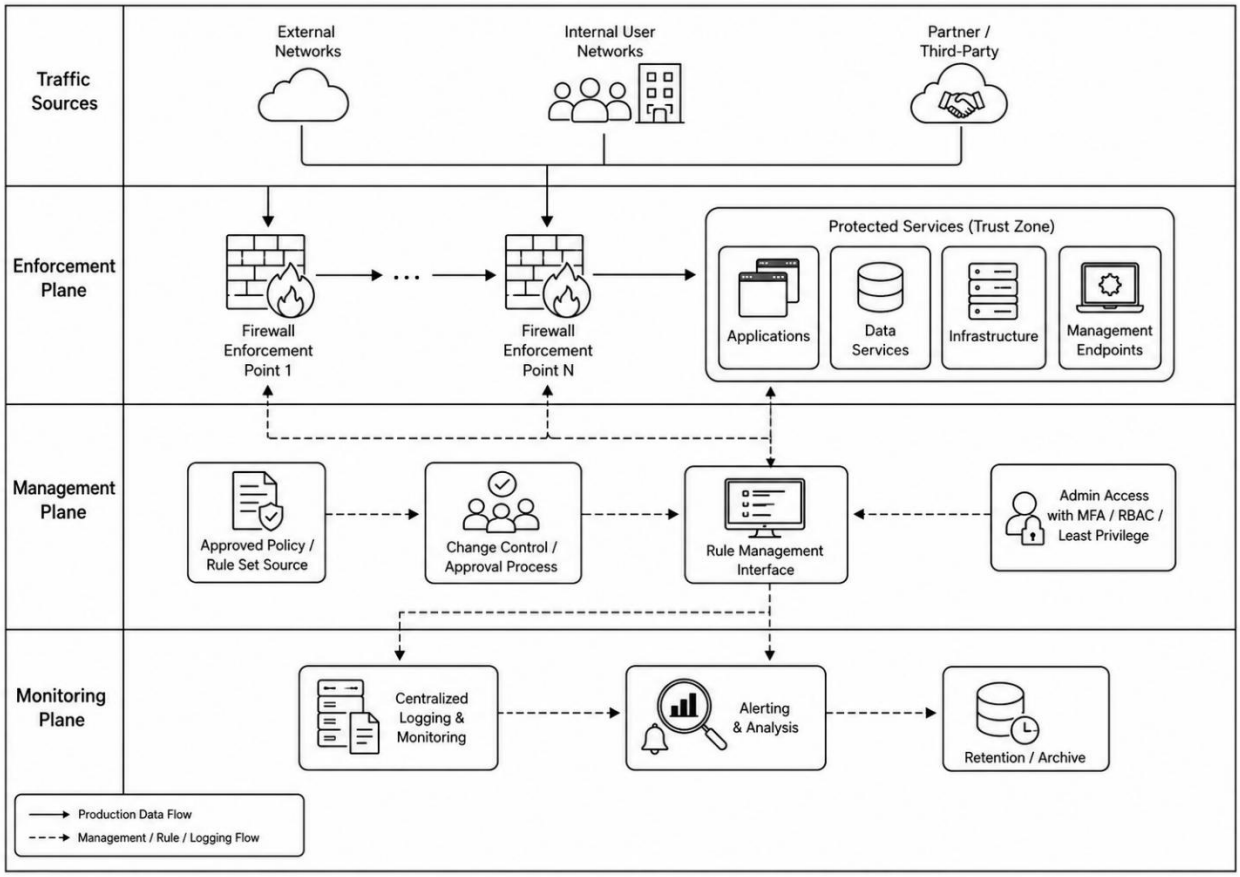
The Associate Standard inherits applicable foundational standards, security controls, definitions, and evidence expectations from the Parent Standard unless otherwise stated.

3. Technical Boundary

The technical boundary includes traffic sources, trust zones, firewall enforcement points, protected zones or services, rule-management interfaces, approved management paths, and centralized logging destinations. Figure 3-1 identifies these components and their primary interfaces.

Figure 3-1. Firewall Technical Boundary and Control Flows:

This figure shows the traffic sources, firewall enforcement points, protected services, management functions, and monitoring components within the technical boundary. Solid lines represent production traffic, while dashed lines represent management, rule deployment, and logging flows.



4. Requirements

ID	Requirement	Parent Flowdown
AS-REQ-01	The organization shall document every in-scope firewall enforcement point and the trust boundaries it protects.	§5.3, §5.9
AS-REQ-02	The organization shall enforce default-deny at in-scope ingress, egress, and inter-zone boundaries.	§5.3; §6.2
AS-REQ-03	The organization shall maintain an approved and traceable record for every permit rule.	§5.3, §5.8
AS-REQ-04	The organization shall validate, approve, test, and provide rollback for firewall rule changes before production deployment.	§5.8; §6.2
AS-REQ-05	The organization shall formally approve and time-bound temporary rules and exceptions.	§5.3, §5.8
AS-REQ-06	The organization shall review the active firewall rule base at an interval not exceeding 90 days.	§5.8, §5.9
AS-REQ-07	The organization shall centrally collect denied traffic decisions, security-relevant permitted traffic, and firewall administrative and policy-change events.	§5.7; §6.5
AS-REQ-08	The organization shall restrict firewall administration to approved roles and management paths.	§5.3; §6.2
AS-REQ-09	The organization shall define and validate firewall failure behavior to prevent uncontrolled traffic from bypassing.	§5.3; §6.2

5. Technical Specifications

ID	Supports	Technical Specification	Acceptance Condition
AS-SPEC-01	AS-REQ-01	Maintain a current inventory showing each firewall, owner, interfaces, protected zones, and enforcement purpose.	All in-scope enforcement points are represented in the approved inventory and Figure 3-1.
AS-SPEC-02	AS-REQ-02	Configure each in-scope policy context to deny traffic that is not explicitly authorized.	Unauthorized test traffic is denied and logged at each tested policy context.
AS-SPEC-03	AS-REQ-03	Record rule owner, justification, source, destination, service, action, approval, and review or expiration date.	All permit rules in the analyzed rule base are traceable to records containing the required attributes. When complete automated analysis is not technically possible, a documented risk-based sample covers every enforcement point and applicable rule class.
AS-SPEC-04	AS-REQ-03	Prohibit unrestricted source-to-destination permit rules unless an approved exception exists.	No unapproved unrestricted permit rule is present.
AS-SPEC-05	AS-REQ-04	Check proposed changes for syntax errors, conflicts, shadowing, excessive scope, and policy violations before deployment.	The change passes all required checks with no unresolved high-severity findings.
AS-SPEC-06	AS-REQ-04	Associate each production change with an approved request, test result, implementation record, and rollback procedure.	Every sampled production change contains the four required records.
AS-SPEC-07	AS-REQ-04	Preserve or restore the last approved policy when a deployment fails.	A failed deployment does not leave an unapproved or incomplete policy active.
AS-SPEC-08	AS-REQ-05	Set temporary rules to expire within 30 days unless renewed through the approved process.	Each temporary rule expires by its approved date or has documented renewal approval.

ID	Supports	Technical Specification	Acceptance Condition
AS-SPEC-09	AS-REQ-06	Review rules for duplicate, shadowed, obsolete, unused, and overly broad conditions.	The review is completed within 90 days and every finding has a recorded disposition.
AS-SPEC-10	AS-REQ-07	Log deny events, administrative actions, policy changes, and permitted traffic identified by the approved monitoring policy. Records shall include the originating firewall, source, destination, service, action, result, and synchronized timestamp.	Required events are centrally available and traceable to the originating firewall.
AS-SPEC-11	AS-REQ-08	Permit interactive firewall administration only through approved management networks, brokers, or controlled out-of-band paths. Require MFA, time-bound elevated authorization, and centralized recording of administrative actions.	Successful administrative access originates only from an approved management path, uses the required authentication and authorization controls, and produces traceable administrative records.
AS-SPEC-12	AS-REQ-04	Compare running firewall policy to the approved policy and alert on unauthorized drift within 24 hours.	Introduced drift is detected and reported within 24 hours.
AS-SPEC-13	AS-REQ-09	Configure each enforcement point to preserve the last approved policy or transition to an approved restricted state upon policy load failure, management plane loss, or failover.	A controlled failure or failover does not permit traffic outside the approved policy.

6. Implementation Sequence

Step 1 — Define the Boundary

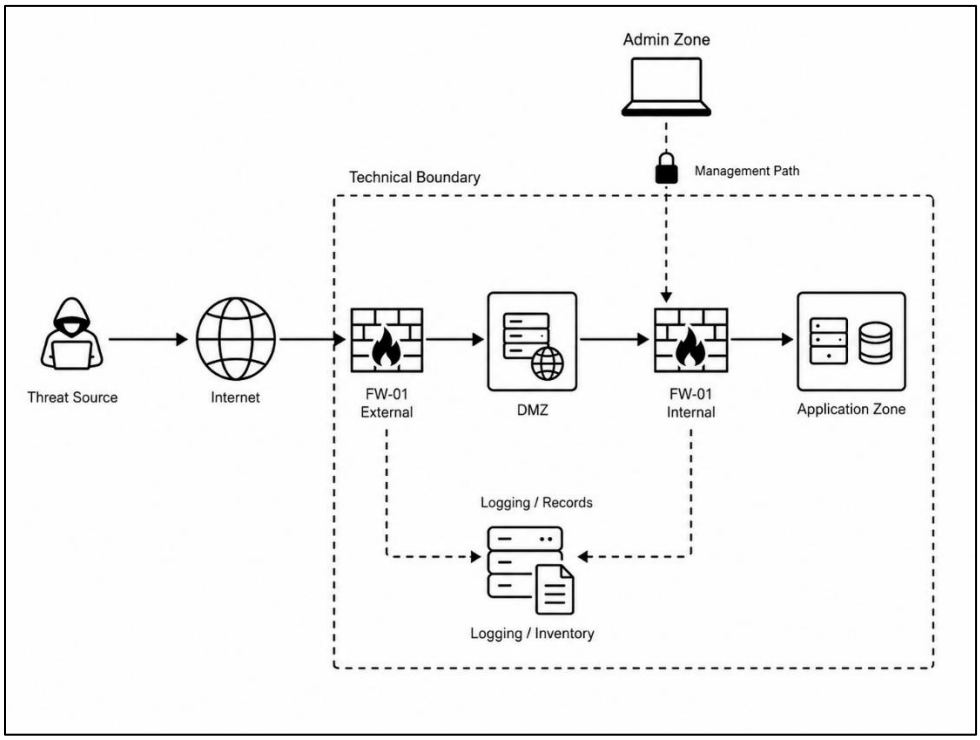
Identify firewall enforcement points, protected zones, interfaces, owners, management paths, and logging destinations.

Output: Approved technical boundary and firewall inventory.

Illustrative configuration example — Boundary inventory

Enforcement Point	Interface / Context	Source Zone	Destination Zone	Purpose
FW-01	External	Internet	DMZ	Public-service ingress
FW-01	Internal	DMZ	Application	Controlled service access
FW-MGMT	Management	Admin Zone	Firewall Management	Administrative access

Figure 6-1. Firewall Boundary Definition:
Shows the identified enforcement points, trust zones, management path, and logging destination that establish the approved firewall technical boundary.



Step 2 — Define the Intended State

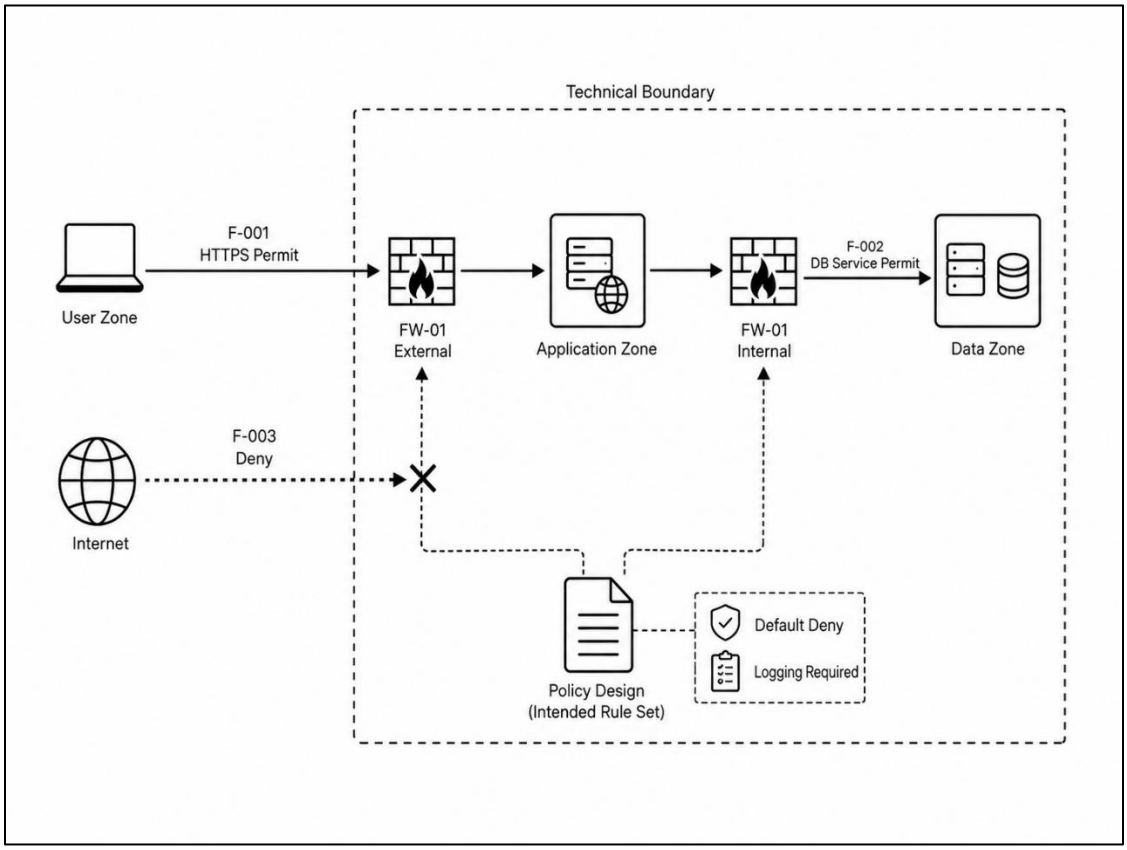
Document default-deny policy contexts, authorized traffic flows, rule attributes, review intervals, exception conditions, and approved firewall failure behavior.

Output: Approved firewall policy design and intended rule set.

Illustrative configuration example — Intended traffic-flow matrix

Flow ID	Source Zone	Destination Zone	Service	Action	Logging
F-001	User	Application	HTTPS	Permit	Session end
F-002	Application	Data	Approved database service	Permit	Start and end
F-003	Internet	Data	Any	Deny	Required

Figure 6-2. Intended Firewall Traffic Flows:
Shows approved and denied traffic paths used to define the intended firewall policy and default-deny behavior.



Step 3 — Configure the Technical Controls

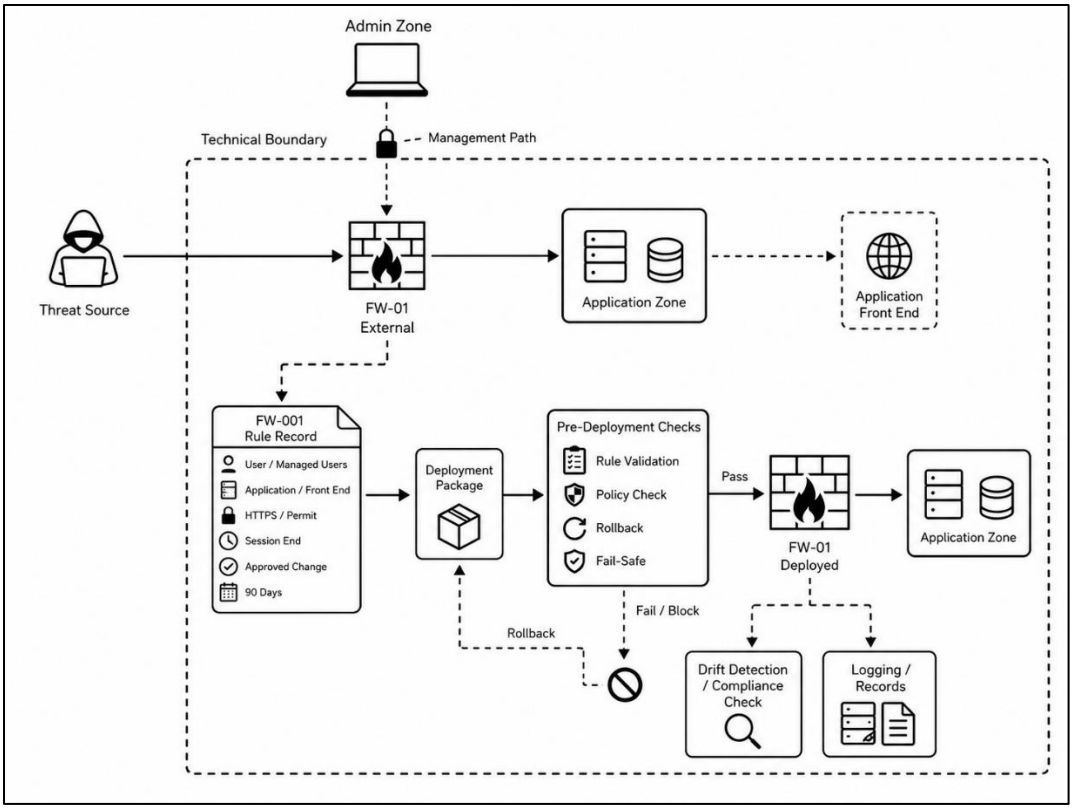
Implement approved rules, management restrictions, logging, pre-deployment checks, rollback controls, drift detection, and fail-safe behavior.

Output: Controlled configuration and deployment package.

Illustrative configuration example — Firewall rule record

Configuration Field	Illustrative Value
Rule ID	FW-001
Source Zone / Object	User / Managed Users
Destination Zone / Object	Application / Application Front End
Service / Action	HTTPS / Permit
Logging	Session end
Owner / Approval	Network Security / Approved change record
Review Interval	90 days

Figure 6-3. Firewall Configuration and Deployment Controls:
Shows how an approved rule record moves through validation, deployment, rollback, logging, and drift-detection controls before becoming active.



Step 4 — Restrict Unauthorized Conditions

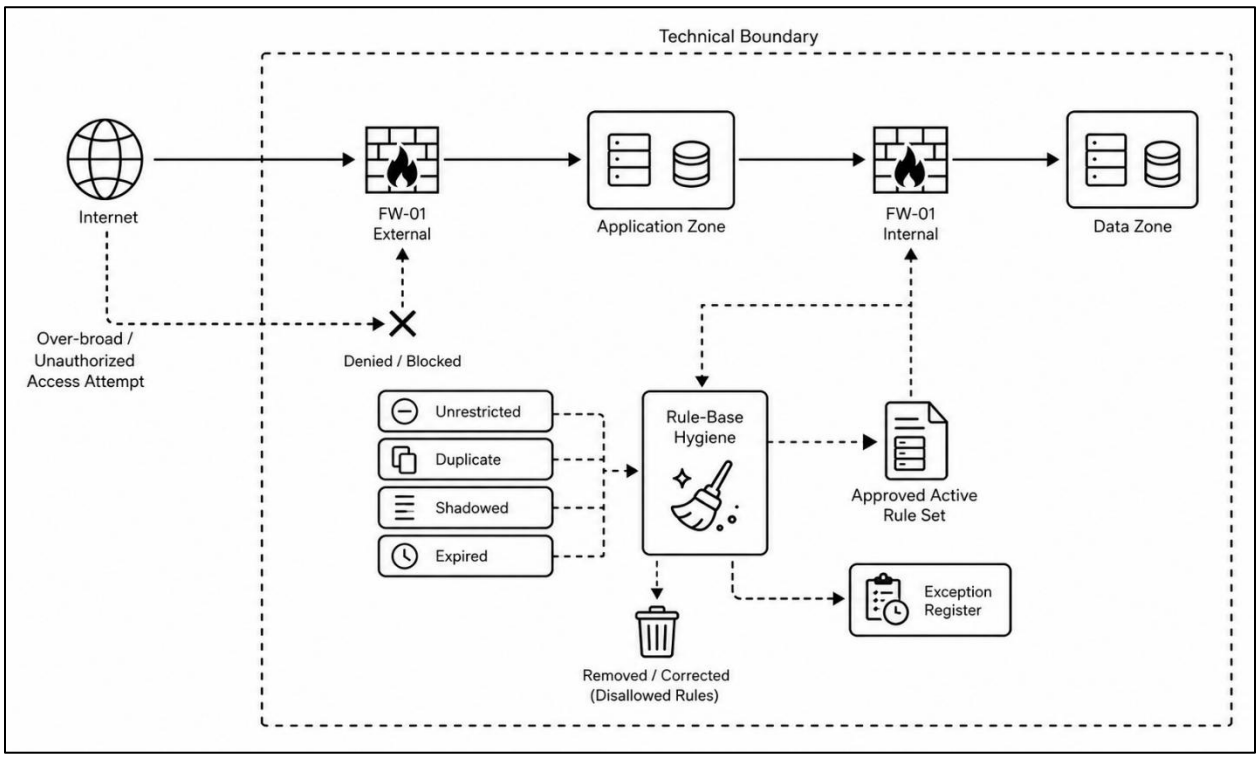
Remove or correct unapproved, unrestricted, duplicate, shadowed, obsolete, and expired rules.

Output: Approved active rule set and exception register.

Illustrative configuration example — Rule base hygiene

Condition	Illustrative Example	Required Disposition
Unrestricted	Any source to any destination using any service	Remove or approve a time-bound exception
Duplicate	Same source, destination, service, and action as another rule	Consolidate or remove
Shadowed	A broader earlier rule prevents a later rule from being evaluated	Reorder, narrow, or remove
Expired	Temporary rule remains active beyond its approval date	Disable or renew through the approved process

Figure 6-4. Firewall Rule Base Hygiene:
Shows how unrestricted, duplicate, shadowed, and expired rules are identified, corrected, removed, or recorded as approved exceptions.



Step 5 — Enable Logging and Monitoring

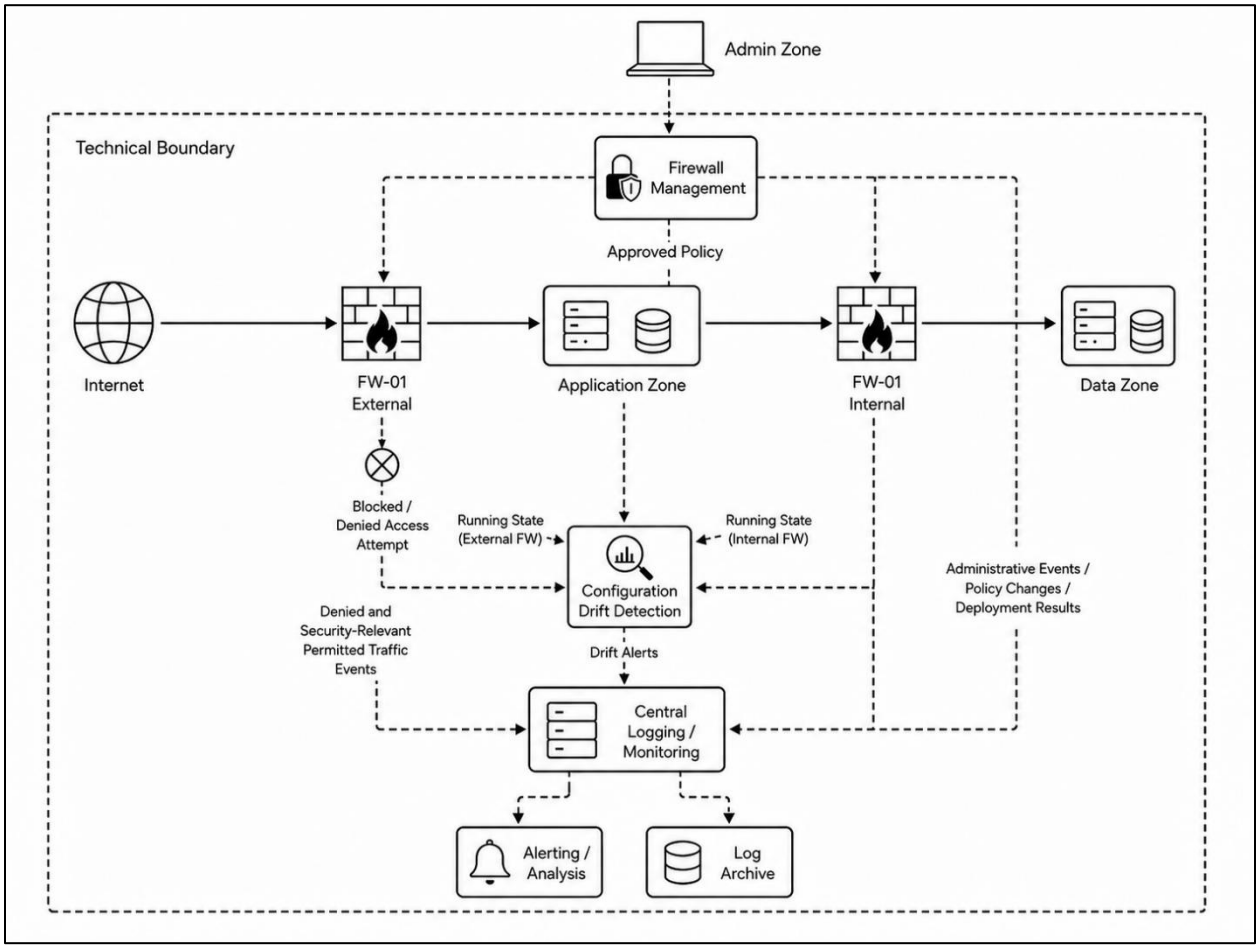
Centralize denied traffic decisions, security-relevant permitted traffic, administrative events, deployment results, and configuration-drift alerts.

Output: Logging configuration and monitoring records.

Illustrative configuration example — Logging profile

Event Category	Expected Configuration
Denied traffic	Logged and centrally collected
Administrative actions	Logged with administrator identity and synchronized timestamp
Policy changes	Logged and traceable to the approved change record
Security-relevant permitted traffic	Logged as defined by the approved monitoring policy

Figure 6-5. Firewall Logging and Monitoring Architecture:
Shows how firewall traffic events, administrative activity, policy changes, deployment results, and drift alerts are centralized for monitoring, alerting, and retention.



Step 6 — Verify the Configuration

Inspect rule records, configurations, approvals, logs, and management controls against Section 5.

Output: Verification results.

Illustrative configuration example — Configuration comparison

Verification Item	Intended State	Running State	Result
Default deny	Enabled	Enabled	Pass
Temporary rule FW-T01	Expired	Active	Fail
Management path	Admin Zone only	Admin Zone only	Pass
Central logging	Enabled	Enabled	Pass

Step 7 — Validate the Operational Result

Exercise authorized and unauthorized traffic, expired rules, management access, deployment failure, rollback, policy-load failure, management-plane loss, and failover.

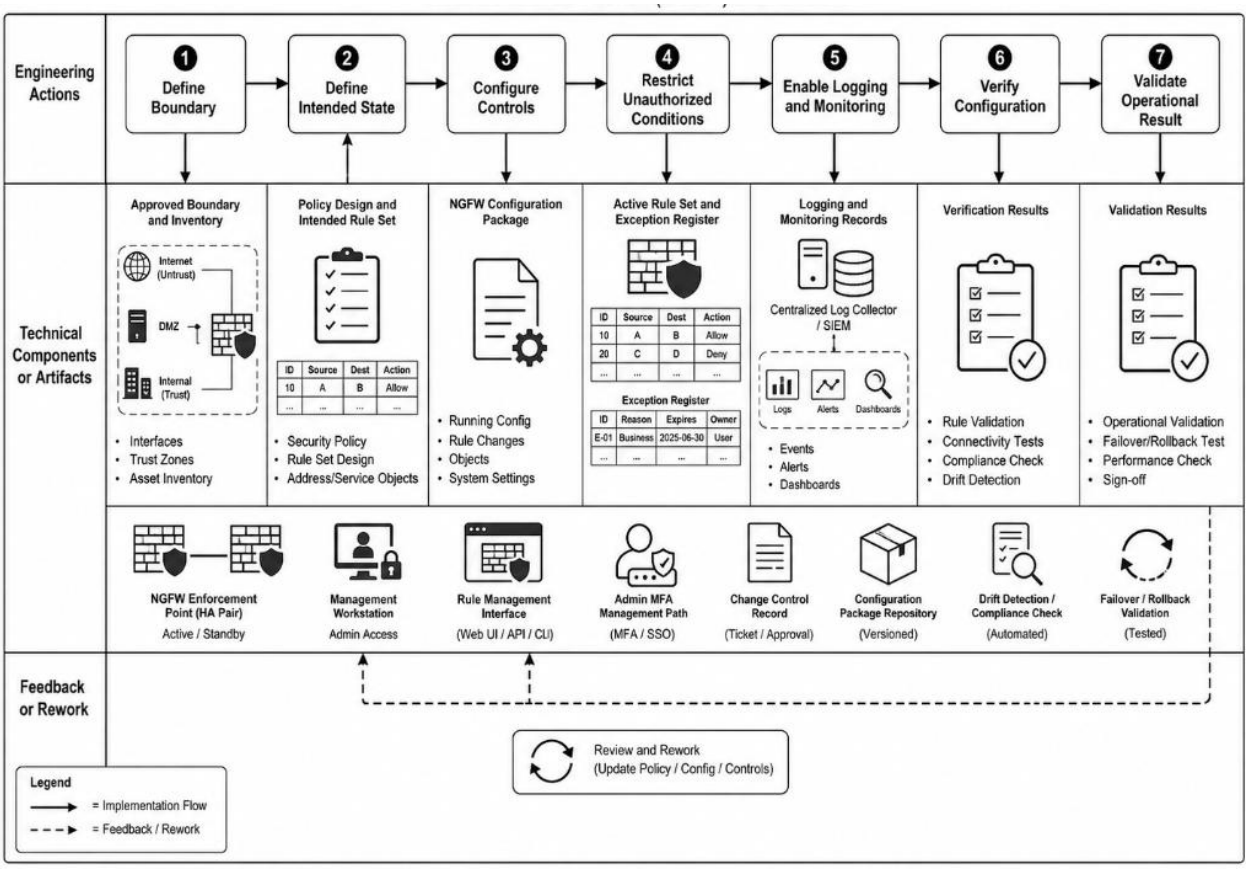
Output: Validation results.

Illustrative configuration example — Operational test vectors

Test	Source	Destination	Expected Result
Authorized flow	User Zone	Approved application	Permit and log
Unauthorized flow	Internet	Data Zone	Deny and log
Expired temporary rule	Approved source	Former temporary destination	Deny
Unauthorized admin access	User Zone	Firewall management	Deny and alert
Failover	Approved source	Protected service	Approved policy remains enforced

Figure 6-1. Firewall Engineering Implementation Workflow:

This figure shows the seven-step implementation sequence for defining, configuring, restricting, monitoring, verifying, and validating an in-scope firewall environment. It also identifies representative technical components, required artifacts, and the feedback path for updating the intended policy and firewall configuration.



7. Verification and Validation

7.1 Verification

Verification confirms that the implementation satisfies the stated requirements and technical specifications.

Test ID	Requirement	Method	Test Activity	Expected Result
V-01	AS-REQ-01	Inspection	Compare the approved boundary diagram and inventory to all deployed in-scope enforcement points.	All in-scope enforcement points, interfaces, owners, and protected zones are represented.
V-02	AS-REQ-02	Test	Review default-deny behavior and send unauthorized test traffic across sampled policy contexts.	Default-deny behavior is active; unauthorized traffic is denied and logged.
V-03	AS-REQ-03	Inspection	Perform complete rule-to-record analysis when supported. Otherwise, use a documented risk-based sample covering each enforcement point and applicable rule class.	All analyzed rules are traceable to records containing the required attributes and approval.
V-04	AS-REQ-04	Demonstration	Process a test change through validation, approval, deployment, and rollback controls.	The change cannot bypass required checks, and rollback is available.
V-05	AS-REQ-05	Analysis	Review temporary and exception rules for approval and expiration.	Each rule is approved, time-bound, and within its authorized period.
V-06	AS-REQ-06	Analysis	Review the latest rule base analysis and disposition records.	The review is current, and all findings have an owner and disposition.

Test ID	Requirement	Method	Test Activity	Expected Result
V-07	AS-REQ-07	Test	Generate denied traffic, security-relevant permitted traffic, administrative actions, and policy-change events and trace them to centralized logging.	Required events are received with synchronized timestamps and are traceable to the originating firewall.
V-08	AS-REQ-08	Test	Attempt administration from approved and unapproved paths, verify MFA and time-bound authorization, and confirm administrative event recording.	Approved access succeeds with required controls; unapproved or expired access is denied, and all attempts are logged.
V-09	AS-REQ-04	Test	Introduce a controlled unauthorized policy change or simulated policy difference and compare the running policy with the approved state.	The drift is detected and reported within 24 hours, and the approved policy is restored or an authorized exception is opened.

7.2 Validation

Validation confirms that the implementation achieves its intended cybersecurity and operational purpose.

Test ID	Intended Outcome	Validation Activity	Expected Result
VA-01	Only approved traffic crosses protected boundaries.	Execute representative authorized and unauthorized ingress, egress, and inter-zone traffic.	Authorized flows succeed; unauthorized flows are blocked and logged.
VA-02	Firewall changes remain controlled and reversible.	Deploy a representative rule change and exercise the rollback path.	The approved change is enforced, and the previous approved state can be restored.
VA-03	Temporary access ends when authorization expires.	Allow a test temporary rule to expire, then repeat the traffic attempt.	The expired rule no longer permits traffic, and the deny event is logged.

Test ID	Intended Outcome	Validation Activity	Expected Result
VA-04	The firewall management plane resists unauthorized access.	Attempt management access from an unapproved source and with expired or unauthorized elevated access.	The attempt is denied, logged, and does not reach the management interface.
VA-05	Firewall failure does not create uncontrolled traffic bypass.	Exercise a controlled policy-load failure, management-plane loss, or failover condition.	The last approved policy remains enforced, or the firewall transitions to the approved restricted state.

8. Evidence and Traceability

One artifact may satisfy multiple evidence expectations when it provides complete and traceable coverage.

Evidence ID	Required Evidence	Supports
E-01	Approved technical boundary diagram and firewall inventory	AS-REQ-01; AS-SPEC-01
E-02	Approved firewall policy design and rule records	AS-REQ-02, AS-REQ-03; AS-SPEC-02–04
E-03	Change, approval, test, deployment, and rollback records	AS-REQ-04; AS-SPEC-05–07
E-04	Temporary rule and exception register	AS-REQ-05; AS-SPEC-08
E-05	Rule base review and finding dispositions	AS-REQ-06; AS-SPEC-09
E-06	Firewall configuration exports, management configuration, logs, drift alerts, and failure-behavior configuration	AS-REQ-07 through AS-REQ-09; AS-SPEC-10 through AS-SPEC-13
E-07	Verification results	V-01 through V-09
E-08	Validation results	VA-01 through VA-05

Traceability Matrix

Requirement	Specification	Implementation Step	V&V Test	Evidence
AS-REQ-01	AS-SPEC-01	Step 1	V-01	E-01
AS-REQ-02	AS-SPEC-02	Steps 2–4	V-02, VA-01	E-02, E-07, E-08
AS-REQ-03	AS-SPEC-03–04	Steps 2–4	V-03	E-02, E-07
AS-REQ-04	AS-SPEC-05–07, AS-SPEC-12	Steps 3, 6–7	V-04, V-09, VA-02	E-03, E-06–E-08
AS-REQ-05	AS-SPEC-08	Steps 2, 4, 7	V-05, VA-03	E-04, E-07, E-08
AS-REQ-06	AS-SPEC-09	Steps 4, 6	V-06	E-05, E-07
AS-REQ-07	AS-SPEC-10	Steps 3, 5–7	V-07, VA-01, VA-03	E-06–E-08
AS-REQ-08	AS-SPEC-11	Steps 1, 3, 6–7	V-08, VA-04	E-01, E-06–E-08
AS-REQ-09	AS-SPEC-13	Steps 2–3, 7	VA-05	E-06, E-08

9. Exceptions

Document only approved exceptions.

Item	Description
Affected Requirement	Requirement or specification identifier
Technical Reason	Documented condition preventing conformance
Risk	Risk introduced by the exception
Compensating Measure	Control used to preserve the intended outcome
Owner	Accountable role
Approval	Authorized approving authority

Item	Description
Review Date	Date the exception must be reviewed or closed

An exception shall not remove the intended cybersecurity outcome.

Change Log and Revision History

Review Date	Changes	Committee	Action	Status
July 2026	Initial publication of D01-AS-NS-1020	ISAUnited Standards Committee	Approved for publication	Complete
April 2026	Associate Standards v 1.0 Submitted for Peer Review	Technical Fellow Society	Peer review	Complete

End of Document

IO