

TECHNICAL PRODUCT BRIEF

Firewall security review

Validate that firewall policy enforces the intended trust model.

Why customers use this service

Compare rulebases, objects, administration and logging with required traffic flows to identify excessive access, stale policy and control gaps.

What we assess

Policy intent	Whether rules align with current business and security needs.
Excessive access	Broad sources, destinations, services and permissive actions.
Rule hygiene	Unused, duplicate, shadowed and expired rules.
Objects and groups	Accuracy and maintainability of referenced network objects.
Administrative access	Management-plane exposure, identity and privilege controls.
Change and exceptions	Ownership, approval and expiry of policy changes.
Logging and visibility	Useful records for denied, permitted and administrative activity.

Engagement outcome

A prioritised firewall review with rule-level evidence, risk context, cleanup actions and validation outcomes.

[How the engagement works](#)

How we test or review

Damocles reviews rulebase, objects, NAT, routing, VPN, management and logging evidence, then validates representative permitted and denied paths where test hosts are supplied. Configuration conclusions remain point-in-time and production changes or disruptive traffic require separate authorisation.

Testing and review perspectives

Rulebase and configuration reviewer

Examines zones, rules, objects, NAT, routing, VPN, management and logging configuration.

Included when: Used for the complete firewall configuration review.

Access: Current native export, diagrams, rule owners and intended flow matrix.

Limitations: A configuration snapshot cannot prove all live traffic outcomes.

Authorised traffic-path validator

Sends approved traffic from supplied sources to representative allowed and denied destinations.

Included when: Used to corroborate selected rule and segmentation decisions.

Access: Source and destination test hosts, protocols, window and expected result.

Limitations: Only tested paths are established; load and denial-of-service testing are excluded.

Firewall or service owner

Provides rule intent, ownership, last-use and change context for ambiguous or high-risk entries.

Included when: Used where technical configuration lacks sufficient business context.

Access: Named owners, tickets, usage evidence and exception approvals.

Limitations: Owner statements do not replace configuration or traffic evidence.

Customer access or evidence typically required

Current native export, diagrams, rule owners and intended flow matrix.; Source and destination test hosts, protocols, window and expected result.; Named owners, tickets, usage evidence and exception approvals.

What you receive

A prioritised firewall review with rule-level evidence, risk context, cleanup actions and validation outcomes.

Detailed technical coverage

Security zones and trust model

What is assessed	Damocles maps interfaces and zones to the intended trust model and identifies ambiguous, overlapping or unintended boundary relationships.
Perspective / access	Firewall or service owner. Assessment requires native configuration exports, diagrams, flow intent, rule owners, usage evidence and approved test points, selected specifically for security zones and trust model.
Evidence	Evidence records the zone, rule identifier, object, NAT, route, VPN, log or traffic-path result relevant to security zones and trust model.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Security zones and trust model when the firewall function and supporting evidence are included.
Limitations	The conclusion is limited to the sampled security zones and trust model; configuration is point-in-time and only selected live paths are proven; no production change is authorised.

Rulebase intent and enforcement

What is assessed	Damocles reviews each sampled rule for source, destination, service or application, action, logging, owner, justification and last-use evidence.
Perspective / access	Firewall or service owner. Assessment requires native configuration exports, diagrams, flow intent, rule owners, usage evidence and approved test points, selected specifically for rulebase intent and enforcement.
Evidence	Evidence records the zone, rule identifier, object, NAT, route, VPN, log or traffic-path result relevant to rulebase intent and enforcement.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Rulebase intent and enforcement when the firewall function and supporting evidence are included.
Limitations	The conclusion is limited to the sampled rulebase intent and enforcement; configuration is point-in-time and only selected live paths are proven; no production change is authorised.

Network and service objects

What is assessed	Damocles resolves network and service objects and groups, identifying overly broad, stale, duplicate, recursive or misleading definitions.
Perspective / access	Rulebase and configuration reviewer. Assessment requires native configuration exports, diagrams, flow intent, rule owners, usage evidence and approved test points, selected specifically for network and service objects.
Evidence	Evidence records the zone, rule identifier, object, NAT, route, VPN, log or traffic-path result relevant to network and service objects.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Network and service objects when the firewall function and supporting evidence are included.
Limitations	The conclusion is limited to the sampled network and service objects; configuration is point-in-time and only selected live paths are proven; no production change is authorised.

NAT and published services

What is assessed	Damocles traces source and destination NAT for published and outbound services and compares translated flows with intended exposure.
Perspective / access	Rulebase and configuration reviewer. Assessment requires native configuration exports, diagrams, flow intent, rule owners, usage evidence and approved test points, selected specifically for nat and published services.
Evidence	Evidence records the zone, rule identifier, object, NAT, route, VPN, log or traffic-path result relevant to nat and published services.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to NAT and published services when the firewall function and supporting evidence are included.
Limitations	The conclusion is limited to the sampled nat and published services; configuration is point-in-time and only selected live paths are proven; no production change is authorised.

Routing and asymmetric paths

What is assessed	Damocles reviews static and dynamic routes, return paths and policy routing for asymmetric or bypass conditions affecting enforcement.
Perspective / access	Firewall or service owner. Named source and destination test points, expected flow matrix and a safe test window.
Evidence	Source-to-destination results linked to rule, route or boundary evidence; the record names the tested routing and asymmetric paths object, path or control and its observed result.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Performed when both ends of the network path and the enforcing device are owned or expressly authorised for testing.
Limitations	Results cover the tested source, destination, protocol and route; testing stops on instability and does not authorise third-party or denial-of-service activity.

VPN policy interaction

What is assessed	Damocles traces site-to-site and remote-access VPN traffic through zones, routes and rules to identify unintended policy interaction.
Perspective / access	Rulebase and configuration reviewer. Current configuration export or read-only access, diagrams, owners and representative validation endpoints.
Evidence	Configuration excerpts, object or rule identifiers and observed validation results.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Performed when both ends of the network path and the enforcing device are owned or expressly authorised for testing.
Limitations	Results cover the tested source, destination, protocol and route; testing stops on instability and does not authorise third-party or denial-of-service activity.

Administrative access

What is assessed	Damocles examines management interfaces, permitted sources, administrator authentication, protocols and separation from data-plane access.
-------------------------	--

Perspective / access	Authorised traffic-path validator. Assessment requires native configuration exports, diagrams, flow intent, rule owners, usage evidence and approved test points, selected specifically for administrative access.
Evidence	Evidence records the zone, rule identifier, object, NAT, route, VPN, log or traffic-path result relevant to administrative access.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Administrative access when the firewall function and supporting evidence are included.
Limitations	The conclusion is limited to the sampled administrative access; configuration is point-in-time and only selected live paths are proven; no production change is authorised.

Logging and alerting

What is assessed	Damocles checks rule logging, event fields, destinations, alert coverage and sampled event receipt for material security decisions.
Perspective / access	Firewall or service owner. Log-source inventory, representative event identifiers, workflow records and responsible contacts.
Evidence	Source-health state, event timestamps, investigation timeline and linked action or escalation record.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Performed when the relevant telemetry and analyst or customer workflow can be observed during the review window.
Limitations	Absent or delayed telemetry prevents a detection conclusion, and observation of one event cannot prove continuous detection of all attacks.

Unused and shadowed rules

What is assessed	Damocles identifies unused, shadowed, redundant and conflicting rules using configuration, hit-count and ownership evidence.
Perspective / access	Firewall or service owner. Named source and destination test points, expected flow matrix and a safe test window.
Evidence	Source-to-destination results linked to rule, route or boundary evidence; the record names the tested unused and shadowed rules object, path or control and its observed result.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Performed when the affected component and representative input are explicitly included in the engagement coverage matrix.
Limitations	The conclusion is limited to the sampled unused and shadowed rules; configuration is point-in-time and only selected live paths are proven; no production change is authorised.

Change validation and rollback

What is assessed	Damocles reviews proposed validation, change controls, acceptance criteria and rollback artefacts for material firewall changes.
Perspective / access	Rulebase and configuration reviewer. Assessment requires native configuration exports, diagrams, flow intent, rule owners, usage evidence and approved test points, selected specifically for change validation and rollback.

Evidence	Evidence records the zone, rule identifier, object, NAT, route, VPN, log or traffic-path result relevant to change validation and rollback.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Change validation and rollback when the firewall function and supporting evidence are included.
Limitations	The conclusion is limited to the sampled change validation and rollback; configuration is point-in-time and only selected live paths are proven; no production change is authorised.

Methodologies and standards

Security and Privacy Controls for Information Systems and Organizations Release 5.2.0 — Provides Release 5.2.0 control context only where a verified mapping is declared.

Information Security Manual June 2026 — Provides ASD ISM control context only for the declared mapping and observed behaviour.

Standards and control mappings

Security and Privacy Controls for Information Systems and Organizations Release 5.2.0 — contextual

References: Framework-level mapping

Assessed: The engagement produces point-in-time technical evidence about the configured and observed security behaviour within the authorised Firewall security review scope.

Evidence: Coverage status, procedure results and findings can inform the customer’s control assessment and risk treatment records.

Applicability: Framework-level context is provided when the customer uses NIST SP 800-53 to organise its security control program.

Limitations: No individual NIST control is published as verified; organisational implementation, continuous operation, governance and complete catalogue coverage remain outside the engagement.

What you receive: report and evidence

Authorised scope and rules of engagement

Records authorised scope and rules of engagement produced from the authorised Firewall security review work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Coverage matrix

Records coverage matrix produced from the authorised Firewall security review work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Retest and residual-risk record

Records retest and residual-risk record produced from the authorised Firewall security review work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Rulebase and object findings

Records rulebase and object findings produced from the authorised Firewall security review work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Traffic-path validation record

Records traffic-path validation record produced from the authorised Firewall security review work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Firewall configuration excerpts

Records firewall configuration excerpts produced from the authorised Firewall security review work.

Included when: Included in the final deliverable when the relevant procedure is performed. **Limitations:** Contains only evidence gathered from authorised systems, identities and review material.

Scope and safety limitations

- Only expressly authorised assets, identities, locations and activities are assessed.
- Higher-risk, disruptive, destructive and third-party activity requires separate written authority.
- Point-in-time evidence cannot establish continuous operation or conditions outside the engagement.

Assurance boundary

Damocles maps assessed coverage and observations to agreed objectives as traceable technical evidence. The review is not a certification, does not establish complete compliance, and does not confirm controls outside the authorised scope.

Review metadata

Owner: Technical Assurance

Last reviewed: 2026-08-10

Next review due: 2026-12-10

Scope this engagement with Damocles Security
damocles.com.au/contact

Assurance boundary

Damocles maps assessed coverage and observations to agreed objectives as traceable technical evidence. The review is not a certification, does not establish complete compliance, and does not confirm controls outside the authorised scope.

This brief supports engagement scoping. The authorised scope, rules of engagement and applicable agreement govern delivery.