

TECHNICAL PRODUCT BRIEF

Firewall migration and implementation

Move firewall policy without carrying forward avoidable risk.

Why customers use this service

Review the source policy, target design and migration controls so required connectivity is preserved while stale, excessive or mistranslated access is identified.

What we assess

Source policy baseline	Current rules, objects, routing and known dependencies.
Target architecture	Zones, interfaces, routing and intended enforcement points.
Rule translation	Accurate conversion of services, objects and policy behaviour.
Policy cleanup	Stale, duplicate and excessive access before migration.
Management security	Administrative identity, access and secure configuration.
Cutover validation	Representative allowed and denied traffic paths.
Rollback and recovery	Practical restoration steps and decision points.
Operational handover	Logging, monitoring, documentation and ownership.

Engagement outcome

A reviewed target policy, migration risk register, cutover validation record and prioritised follow-up actions.

How the engagement works

How we test or review

Damocles reconciles current and proposed configurations, traces translated zones, objects, rules, NAT, routing and VPNs, and observes approved pre-cutover, cutover and rollback checks. Review does not authorise implementation, and production changes occur only under the customer change plan.

Testing and review perspectives

Current-state reviewer

Captures and reconciles the source firewall configuration, dependencies and observed service intent.

Included when: Used to establish the migration baseline.

Access: Native exports, topology, inventories, tickets and owners.

Limitations: Undocumented external dependencies may remain.

Migration implementation engineer

Reviews translated zones, objects, rules, NAT, routing, VPN and management settings against the source.

Included when: Used during design and pre-cutover assurance.

Access: Target configuration, translation records, platform constraints and test plan.

Limitations: Review does not authorise production implementation.

Validation and rollback owner

Defines acceptance checks, cutover stop conditions and restoration steps and records their execution.

Included when: Used for rehearsals and authorised change windows.

Access: Approved change plan, test endpoints, rollback artefacts and decision authority.

Limitations: No live cutover is claimed unless observed.

Customer access or evidence typically required

Native exports, topology, inventories, tickets and owners.; Target configuration, translation records, platform constraints and test plan.; Approved change plan, test endpoints, rollback artefacts and decision authority.

What you receive

A reviewed target policy, migration risk register, cutover validation record and prioritised follow-up actions.

Detailed technical coverage

Current-state configuration capture

What is assessed	Damocles captures the source platform configuration, software state, interfaces, dependencies and change baseline using native exports.
Perspective / access	Validation and rollback owner. Current configuration export or read-only access, diagrams, owners and representative validation endpoints; customer inputs must identify the approved current-state configuration capture targets and expected behaviour.
Evidence	Configuration excerpts, object or rule identifiers and observed validation results; the record names the tested current-state configuration capture 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 current configuration evidence and a representative endpoint or device are included in the review.
Limitations	A configuration snapshot cannot prove continuous enforcement across excluded nodes; validation avoids changes unless implementation work is authorised.

Zone and interface translation

What is assessed	Damocles maps every in-scope source zone and interface to the target construct and records semantic or platform differences.
Perspective / access	Current-state reviewer. Assessment requires source and target exports, translation records, topology, owners, test plan, change window and rollback artefacts, selected specifically for zone and interface translation.
Evidence	Evidence records the configuration comparison, translated object or rule, test result, decision record or change evidence relevant to zone and interface translation.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Zone and interface translation when the migration component and assurance stage are included.
Limitations	The conclusion is limited to the sampled zone and interface translation; review does not authorise implementation and live outcomes are claimed only when observed.

Object and group translation

What is assessed	Damocles translates and reconciles network, service and identity objects and groups, resolving duplicates and unsupported forms.
Perspective / access	Current-state reviewer. Assessment requires source and target exports, translation records, topology, owners, test plan, change window and rollback artefacts, selected specifically for object and group translation.
Evidence	Evidence records the configuration comparison, translated object or rule, test result, decision record or change evidence relevant to object and group translation.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Object and group translation when the migration component and assurance stage are included.
Limitations	The conclusion is limited to the sampled object and group translation; review does not authorise implementation and live outcomes are claimed only when observed.

Rulebase rationalisation

What is assessed	Damocles compares source and target rules, preserving required intent while documenting removed, consolidated or changed entries.
Perspective / access	Validation and rollback owner. Assessment requires source and target exports, translation records, topology, owners, test plan, change window and rollback artefacts, selected specifically for rulebase rationalisation.
Evidence	Evidence records the configuration comparison, translated object or rule, test result, decision record or change evidence relevant to rulebase rationalisation.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Rulebase rationalisation when the migration component and assurance stage are included.
Limitations	The conclusion is limited to the sampled rulebase rationalisation; review does not authorise implementation and live outcomes are claimed only when observed.

NAT translation

What is assessed	Damocles translates source and destination NAT and validates the resulting address, port, zone and published-service behaviour.
Perspective / access	Current-state reviewer. Assessment requires source and target exports, translation records, topology, owners, test plan, change window and rollback artefacts, selected specifically for nat translation.
Evidence	Evidence records the configuration comparison, translated object or rule, test result, decision record or change evidence relevant to nat translation.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to NAT translation when the migration component and assurance stage are included.
Limitations	The conclusion is limited to the sampled nat translation; review does not authorise implementation and live outcomes are claimed only when observed.

Routing and dynamic protocols

What is assessed	Damocles maps static and dynamic routing, policy routes and dependencies and checks target convergence assumptions.
Perspective / access	Validation and rollback 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 dynamic protocols 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 migration

What is assessed	Damocles translates VPN peers, identities, selectors, cryptography, routing and monitoring and records interoperability dependencies.
-------------------------	---

Perspective / access	Current-state 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; the record names the tested vpn migration 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.

Management-plane hardening

What is assessed	Damocles reviews target management interfaces, AAA, administrator roles, protocols and permitted management sources.
Perspective / access	Validation and rollback owner. Current configuration export or read-only access, diagrams, owners and representative validation endpoints.
Evidence	Configuration excerpts, object or rule identifiers and observed validation results; the record names the tested management-plane hardening 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 current configuration evidence and a representative endpoint or device are included in the review.
Limitations	A configuration snapshot cannot prove continuous enforcement across excluded nodes; validation avoids changes unless implementation work is authorised.

Logging integration

What is assessed	Damocles maps source logging and event fields to target destinations, parsers, alerts and operational ownership.
Perspective / access	Validation and rollback 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.

High-availability configuration

What is assessed	Damocles reviews target HA peers, interfaces, state synchronisation, monitored paths and failure behaviour.
Perspective / access	Validation and rollback owner. Architecture, dependency list, monitoring view, authorised failover window and rollback owner.
Evidence	The relevant configuration excerpt or rule identifier, the expected setting and the observed validation result.

References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Performed only when a customer-approved recovery or failover scenario, observer and rollback window are available.
Limitations	The result covers the exercised failure mode; activity stops at the rollback threshold and does not predict every compound failure.

Pre-cutover validation

What is assessed	Damocles executes or reviews the approved pre-cutover test plan against staged configuration and representative flows.
Perspective / access	Current-state reviewer. Assessment requires source and target exports, translation records, topology, owners, test plan, change window and rollback artefacts, selected specifically for pre-cutover validation.
Evidence	Evidence records the configuration comparison, translated object or rule, test result, decision record or change evidence relevant to pre-cutover validation.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Pre-cutover validation when the migration component and assurance stage are included.
Limitations	The conclusion is limited to the sampled pre-cutover validation; review does not authorise implementation and live outcomes are claimed only when observed.

Cutover sequencing

What is assessed	Damocles checks the ordered cutover plan, dependencies, decision points, communications and acceptance evidence.
Perspective / access	Current-state reviewer. Assessment requires source and target exports, translation records, topology, owners, test plan, change window and rollback artefacts, selected specifically for cutover sequencing.
Evidence	Evidence records the configuration comparison, translated object or rule, test result, decision record or change evidence relevant to cutover sequencing.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Cutover sequencing when the migration component and assurance stage are included.
Limitations	The conclusion is limited to the sampled cutover sequencing; review does not authorise implementation and live outcomes are claimed only when observed.

Rollback criteria

What is assessed	Damocles verifies measurable rollback triggers, decision authority, restoration artefacts and source-platform readiness.
Perspective / access	Current-state reviewer. Assessment requires source and target exports, translation records, topology, owners, test plan, change window and rollback artefacts, selected specifically for rollback criteria.
Evidence	Evidence records the configuration comparison, translated object or rule, test result, decision record or change evidence relevant to rollback criteria.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Rollback criteria when the migration component and assurance stage are included.

Limitations	The conclusion is limited to the sampled rollback criteria; review does not authorise implementation and live outcomes are claimed only when observed.
-------------	--

Post-cutover verification

What is assessed	Damocles records post-cutover configuration comparison, representative flow results, logging, monitoring and unresolved variance.
Perspective / access	Current-state reviewer. Assessment requires source and target exports, translation records, topology, owners, test plan, change window and rollback artefacts, selected specifically for post-cutover verification.
Evidence	Evidence records the configuration comparison, translated object or rule, test result, decision record or change evidence relevant to post-cutover verification.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Post-cutover verification when the migration component and assurance stage are included.
Limitations	The conclusion is limited to the sampled post-cutover verification; review does not authorise implementation and live outcomes are claimed only when observed.

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 migration and implementation 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 migration and implementation 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 migration and implementation 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 migration and implementation 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.

Configuration translation matrix

Records configuration translation matrix produced from the authorised Firewall migration and implementation 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.

Cutover validation record

Records cutover validation record produced from the authorised Firewall migration and implementation 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.

Rollback readiness record

Records rollback readiness record produced from the authorised Firewall migration and implementation 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.