

TECHNICAL PRODUCT BRIEF

Network segmentation review

Validate that network segmentation works as designed.

Why customers use this service

Compare the intended trust model with routing, firewall policy, management access and representative traffic paths to identify missing boundaries and practical bypass paths.

What we assess

Trust zones	Whether user, server, cloud, OT, guest and restricted environments are separated as intended.
Allowed and denied traffic	Representative permitted and prohibited paths across key boundaries.
Routing and alternate paths	Routes, NAT and alternate forwarding paths that may bypass expected enforcement.
Management access	Administrative paths that cross intended trust boundaries.
Sensitive systems	Whether high-value services are reachable from locations that should not have access.
Exceptions	Temporary or compensating exceptions that weaken the intended model.
Operational usability	Whether monitoring, patching and administration can operate safely.

Engagement outcome

A clear segmentation map, validated traffic-path results, identified bypass conditions and prioritised remediation actions.

How the engagement works

How we test or review

Damocles traces intended trust boundaries through routing and enforcement configuration and attempts approved allowed and denied paths from supplied source hosts. A tested path does not establish every possible route; scanning and traffic volume remain within agreed thresholds.

Testing and review perspectives

Source-zone test user or host

Initiates approved allowed and denied traffic from a representative trust zone.

Included when: Used for live boundary validation.

Access: A source host, identity where required, destination list and protocols.

Limitations: Represents only that source context.

Destination service owner

Confirms the intended consumers, protocols and impact boundaries of sensitive destinations.

Included when: Used to interpret the flow matrix and validation results.

Access: Service inventory, required flows, owners and test endpoints.

Limitations: Business intent is not proof of enforcement.

Routing and enforcement-point reviewer

Traces routes, ACLs, firewall policy, NAT and identity-aware enforcement across each selected boundary.

Included when: Used for configuration-assisted path analysis.

Access: Routing tables, policies, NAT, topology and flow matrix.

Limitations: Unseen alternate paths may remain.

Customer access or evidence typically required

A source host, identity where required, destination list and protocols.; Service inventory, required flows, owners and test endpoints.; Routing tables, policies, NAT, topology and flow matrix.

What you receive

A clear segmentation map, validated traffic-path results, identified bypass conditions and prioritised remediation actions.

Detailed technical coverage

Trust-zone definition

What is assessed	Damocles maps named systems and services to intended trust zones, data classifications and administrative boundaries.
Perspective / access	Routing and enforcement-point reviewer. Assessment requires trust-zone definitions, flow matrix, routing and policy exports, source hosts and destination test services, selected specifically for trust-zone definition.
Evidence	Evidence records the flow, enforcement point, route, NAT, policy, log or allowed/denied connectivity result relevant to trust-zone definition.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Trust-zone definition when the boundary and representative source and destination are authorised.
Limitations	The conclusion is limited to the sampled trust-zone definition; only sampled paths are established; scanning volume and excluded zones remain bounded.

Permitted boundary flows

What is assessed	Damocles compares the approved flow matrix with representative permitted source, destination, protocol and application paths.
Perspective / access	Source-zone test user or host. Assessment requires trust-zone definitions, flow matrix, routing and policy exports, source hosts and destination test services, selected specifically for permitted boundary flows.
Evidence	Evidence records the flow, enforcement point, route, NAT, policy, log or allowed/denied connectivity result relevant to permitted boundary flows.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Permitted boundary flows when the boundary and representative source and destination are authorised.
Limitations	The conclusion is limited to the sampled permitted boundary flows; only sampled paths are established; scanning volume and excluded zones remain bounded.

Rulebase enforcement points

What is assessed	Damocles traces each selected flow through firewall, ACL, host, cloud or identity-aware enforcement points.
Perspective / access	Routing and enforcement-point reviewer. Assessment requires trust-zone definitions, flow matrix, routing and policy exports, source hosts and destination test services, selected specifically for rulebase enforcement points.
Evidence	Evidence records the flow, enforcement point, route, NAT, policy, log or allowed/denied connectivity result relevant to rulebase enforcement points.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Rulebase enforcement points when the boundary and representative source and destination are authorised.
Limitations	The conclusion is limited to the sampled rulebase enforcement points; only sampled paths are established; scanning volume and excluded zones remain bounded.

Routing and alternate paths

What is assessed	Damocles examines routing and alternate paths that could bypass the intended boundary, including asymmetric return traffic.
Perspective / access	Routing and enforcement-point reviewer. Assessment requires trust-zone definitions, flow matrix, routing and policy exports, source hosts and destination test services, selected specifically for routing and alternate paths.
Evidence	Evidence records the flow, enforcement point, route, NAT, policy, log or allowed/denied connectivity result relevant to routing and alternate paths.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Routing and alternate paths when the boundary and representative source and destination are authorised.
Limitations	The conclusion is limited to the sampled routing and alternate paths; only sampled paths are established; scanning volume and excluded zones remain bounded.

NAT effects on segmentation

What is assessed	Damocles accounts for source and destination NAT when correlating observed traffic with segmentation policy.
Perspective / access	Source-zone test user or host. Assessment requires trust-zone definitions, flow matrix, routing and policy exports, source hosts and destination test services, selected specifically for nat effects on segmentation.
Evidence	Evidence records the flow, enforcement point, route, NAT, policy, log or allowed/denied connectivity result relevant to nat effects on segmentation.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to NAT effects on segmentation when the boundary and representative source and destination are authorised.
Limitations	The conclusion is limited to the sampled nat effects on segmentation; only sampled paths are established; scanning volume and excluded zones remain bounded.

Identity-aware access paths

What is assessed	Damocles tests representative identity-aware decisions using supplied users, devices and expected policy context.
Perspective / access	Destination service owner. Named source and destination test points, expected flow matrix and a safe test window; customer inputs must identify the approved identity-aware access paths targets and expected behaviour.
Evidence	Source-to-destination results linked to rule, route or boundary evidence; the record names the tested identity-aware access 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 representative identities and the corresponding permission or ownership boundary are included in scope.
Limitations	Conclusions cover only the supplied identities, roles and records; credential guessing, lockout and privileged changes stop at the agreed thresholds.

East-west administrative protocols

What is assessed	Damocles attempts approved east-west management protocols between representative zones and records allowed and denied outcomes.
Perspective / access	Source-zone test user or host. 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 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.

Representative path validation

What is assessed	Damocles sends approved test traffic from actual source hosts to destination services and records the enforcement point and result.
Perspective / access	Source-zone test user or host. 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 representative path validation 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.

Sensitive-zone reachability

What is assessed	Damocles tests named high-value destinations and forbidden protocols from representative lower-trust zones.
Perspective / access	Source-zone test user or host. 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 sensitive-zone reachability 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.

Logging at boundaries

What is assessed	Damocles confirms whether boundary decisions create usable logs with source, destination, protocol, action and policy identity.
Perspective / access	Routing and enforcement-point reviewer. 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.

Third-party and remote access

What is assessed	Damocles traces third-party and remote-access routes into internal zones and compares them with intended access restrictions.
Perspective / access	Destination service owner. Assessment requires trust-zone definitions, flow matrix, routing and policy exports, source hosts and destination test services, selected specifically for third-party and remote access.
Evidence	Evidence records the flow, enforcement point, route, NAT, policy, log or allowed/denied connectivity result relevant to third-party and remote access.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Third-party and remote access when the boundary and representative source and destination are authorised.
Limitations	The conclusion is limited to the sampled third-party and remote access; only sampled paths are established; scanning volume and excluded zones remain bounded.

Exceptions and compensating controls

What is assessed	Damocles records segmentation exceptions, owners, expiry, compensating controls and validation evidence.
Perspective / access	Source-zone test user or host. Assessment requires trust-zone definitions, flow matrix, routing and policy exports, source hosts and destination test services, selected specifically for exceptions and compensating controls.
Evidence	Evidence records the flow, enforcement point, route, NAT, policy, log or allowed/denied connectivity result relevant to exceptions and compensating controls.
References	Security and Privacy Controls for Information Systems and Organizations Release 5.2.0
Applicability	Applies to Exceptions and compensating controls when the boundary and representative source and destination are authorised.
Limitations	The conclusion is limited to the sampled exceptions and compensating controls; only sampled paths are established; scanning volume and excluded zones remain bounded.

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.

Payment Card Industry Data Security Standard 4.0.1 — Provides contextual PCI DSS 4.0.1 relevance while licensed identifiers remain withheld.

Standards and control mappings

Payment Card Industry Data Security Standard 4.0.1 — contextual

References: Framework-level mapping

Assessed: The scoped technical behaviour relevant to network segmentation review.

Evidence: Scoped observations and coverage status that a qualified assessor may consider.

Applicability: Only when the customer confirms that the framework and environment are applicable.

Limitations: Exact identifiers and licensed text are withheld; this is not certification or a complete framework assessment.

What you receive: report and evidence

Authorised scope and rules of engagement

Records authorised scope and rules of engagement produced from the authorised Network segmentation 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 Network segmentation 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 Network segmentation 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.

Trust-zone and enforcement map

Records trust-zone and enforcement map produced from the authorised Network segmentation 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.

Allowed and denied path results

Records allowed and denied path results produced from the authorised Network segmentation 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.

Segmentation exception register

Records segmentation exception register produced from the authorised Network segmentation 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.