IDENTITY / RESOURCE / CONTINUOUS POLICY

Resource-centric access across an existing enterprise

A technical white paper on policy decision points, enforcement, private connectors, identity, and changing trust conditions.

6 September 2026 / Technical edition

Inside this paper

01 Begin with a resource boundary

02 Separate policy, traffic, and evidence

03 A request and a change in trust

04 Write policy around business intent

05 Resilience and evaluation

01 / Begin with a resource boundary

Zero trust removes network location as a sufficient reason to trust a request. NIST SP 800-207 separates policy decisions from enforcement around resources. Translate that principle into a concrete enterprise inventory: application, owner, users, protocols, dependencies, and data sensitivity.

References: NIST SP 800-207

For a finance application, the authorized object is the finance service and its approved dependencies. It is not the entire subnet containing that service. For a workload, the authorized object may be a single service identity and method scope. Start with a narrow application boundary and widen it only when an observed business dependency requires it.

Access as a decision path

01	Identity	User or workload identity plus active enrollment.
02	Context	Device posture, risk, session age, resource sensitivity.
03	Decision	Versioned policy returns scope and constraints.
04	Enforcement	Allow the approved resource and observe the session.

02 / Separate policy, traffic, and evidence

Plane	Responsibility	Failure to avoid
Control	Identity mapping, policy distribution, connector registration.	Treating an administrative login as an end-user access grant.
Data	Carry authorized application traffic through enforcement.	Routing an entire subnet when only one application is approved.
Evidence	Record decisions, session changes, and connection context.	Keeping a deny count without the reason or policy version.

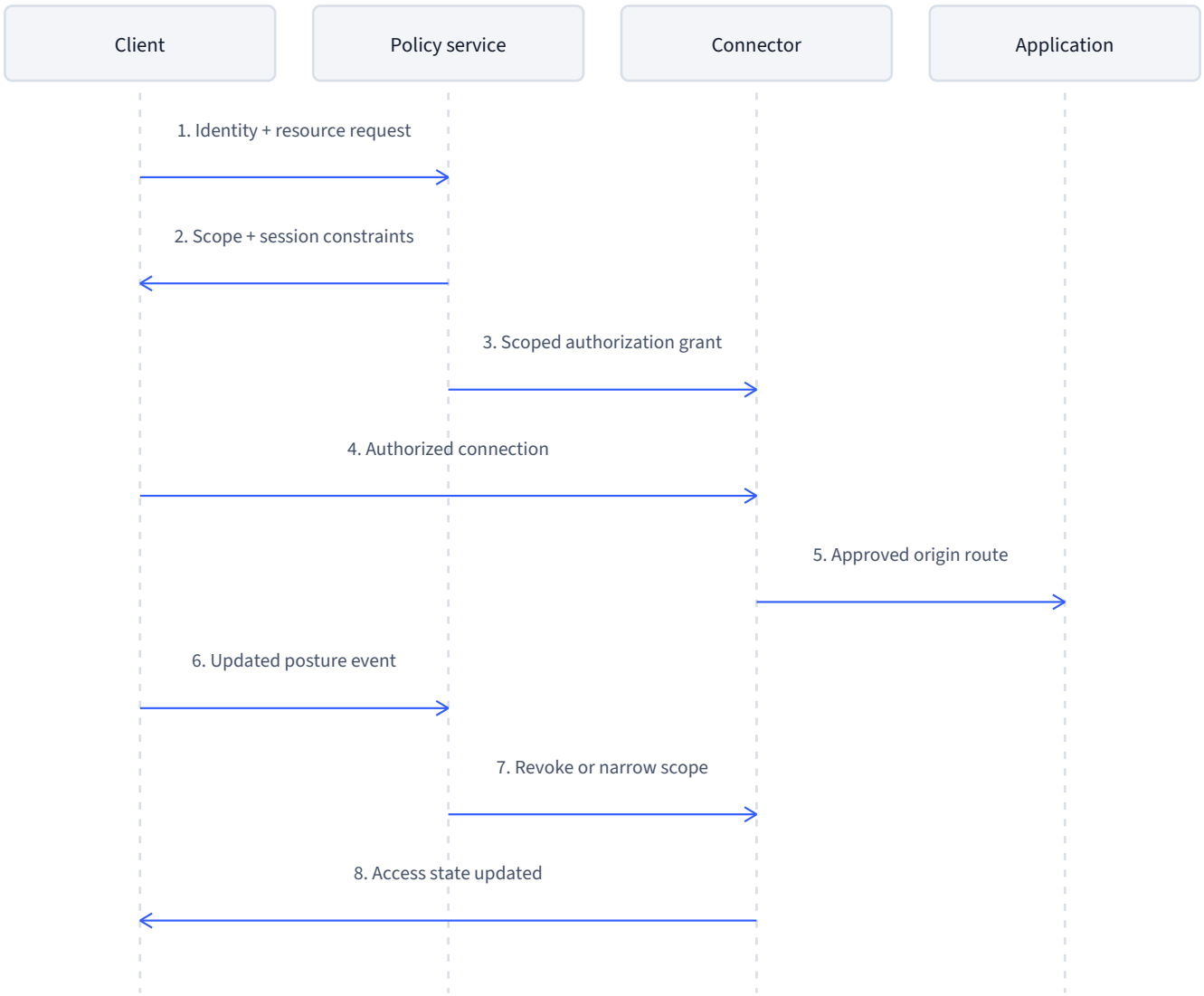
Place private connectors where they can reach the approved origin services. Restrict their egress destinations, origin ports, and management access. Outbound establishment can remove the need for a public application listener, but the connector still has a real network trust boundary and needs patching, credential rotation, and high availability.

Workload identity deserves a distinct lifecycle from human identity. NIST SP 800-207A extends the architectural discussion to cloud-native applications and service identities. Use separate credentials, owners, and authorization scopes for automation.

References: NIST SP 800-207A

03 / A request and a change in trust

Initial access and posture-driven reevaluation



Continuous assessment needs a defined event model. An operating-system patch signal may arrive periodically; an enrollment removal can be event-driven. Set maximum signal age, recheck intervals, and the action for unknown state. Unknown posture should not quietly inherit the same treatment as a fresh healthy result.

Not every change requires dropping every connection. A resource policy can require reauthentication, narrow a session, or terminate it. Publish the behavior to users and support teams, including remediation guidance and a path back to normal access.

04 / Write policy around business intent

Application access intent

```
resource: finance-erp
owner: finance-platform
identities:
  groups: [finance-employees]
device_requirements:
  enrolled: true
  disk_encrypted: true
  posture_max_age_minutes: 5
session:
  reauthenticate_for: [sensitive-export]
  on_enrollment_removed: terminate
network:
  origin: erp.internal.example
  ports: [443]
evidence:
  include: [policy_version, reason, session_id]
```

This is a policy design worksheet, not a product API schema. Its purpose is to make scope, freshness, and enforcement behavior reviewable before mapping them into the deployment. Avoid embedding raw user secrets or permanent credentials in policy files.

Context change	Decision to define	User experience
Device leaves management	Revoke managed-device entitlement.	Explain the enrollment requirement.
Posture expires	Step up, restrict, or deny by resource.	Show the required health refresh.
Role removed	Reevaluate application authorization.	Remove the application entitlement.
Risk rises	Require stronger authentication or end session.	Give an actionable reason where appropriate.

05 / Resilience and evaluation

Design connector redundancy across failure domains with capacity for a member outage. Test DNS failures, loss of an identity provider, stale policy, and application restarts separately. A healthy gateway does not prove a healthy application path. Keep identity availability, control-plane availability, and data-plane continuity visible as separate signals.

- Prove that a permitted identity can reach only the named resource.
- Prove that a removed entitlement affects new and existing access according to policy.
- Prove that an unapproved origin port is unreachable through the connector.
- Measure application completion time as well as tunnel establishment.
- Rehearse connector failure with representative stateful application sessions.
- Give the SOC a reproducible decision trace containing policy version, signal freshness, and resource scope.

References and continued reading

NIST SP 800-207

NIST SP 800-207A

Product overview

Integration guide

Operations and evaluation