tufin The Security Policy Company.

How to Achieve Audit-Ready SASE in a Complex Hybrid Network

In any fast-moving, distributed enterprise, network and security teams face constant change. New projects kick off. Clients come onboard. Internal teams shift and grow. To keep pace, users need seamless access to the right tools, sometimes for a few days, sometimes for several months. It is fast. It is complex. And it must work without hesitation.

The goal is clear: give people what they need, when they need it, and take it away when they don't. But that goal doesn't stop at access. For firms operating in regulated industries, every access decision must be governed, auditable, and provable, on demand. Without that, compliance gaps become inevitable.

As access demands scale, the process begins to fracture. Teams across regions make changes daily, adding users, deploying applications, and shifting resources. Over time, access rules multiply. Context fades. And sometimes, the unexpected slips through.

Misalignment: When policy isn't managed in one system

Here's an example that's all too common.A security team discovers a former user who still has access long after their project ended. The original policy was correct. A legacy rule, tied to a reused IP space, quietly reopened a path no one intended to leave behind. Nothing looks wrong in isolation. But the result is not secure.

Each control layer—identity, cloud, and firewall—worked as designed. But none of them saw the whole picture before it was too late.

As enterprise networks expand, policies are often implemented through disconnected systems, each with their own logic, enforcement method, and team of owners. Firewall rules and SASE policies are set through different processes with no built-in way to check for alignment.

This disconnect leads to policies that permit access in one layer while restricting it in another. These inconsistencies are difficult to detect without shared visibility. The gaps that emerge weaken enforcement and only increase compliance risk.

When there is no clear view into how policies behave across systems, validation becomes unreliable. The signs of these issues appear earlier than you might think. These four areas reflect where policy inconsistencies and workflow fragmentation begin to introduce measurable risk.

SASE policies get rewritten at every layer

The friction begins when multiple teams manage security policies across disconnected platforms.

In typical environments, cloud, network, and security teams define and enforce access independently. These teams often rely on different tools, naming conventions, and assumptions about trust boundaries. Even when intentions align, policies diverge.

Priority Task	How it manifests in a fragmented environment
Decommission a user’s access when they leave the company	Identity is disabled in Okta, but firewall and cloud rules still allow access
Add a new remote application and ensure secure segmentation	Cloud team builds it in Terraform, but the network team isn’t looped in—no segmentation rules applied
Implement a policy change for new regulatory requirement (e.g., geo-fencing or encryption)	Each team interprets the requirement differently and enforces it inconsistently across tools
Approve a change to allow new app-to-app communication across zones	Risk is assessed manually in spreadsheets, with no consistent method for validation or rollback
Prepare documentation for an ISO 27001 audit	Teams pull access data from Panorama, Prisma Access, and Azure logs, then stitch it together in Excel

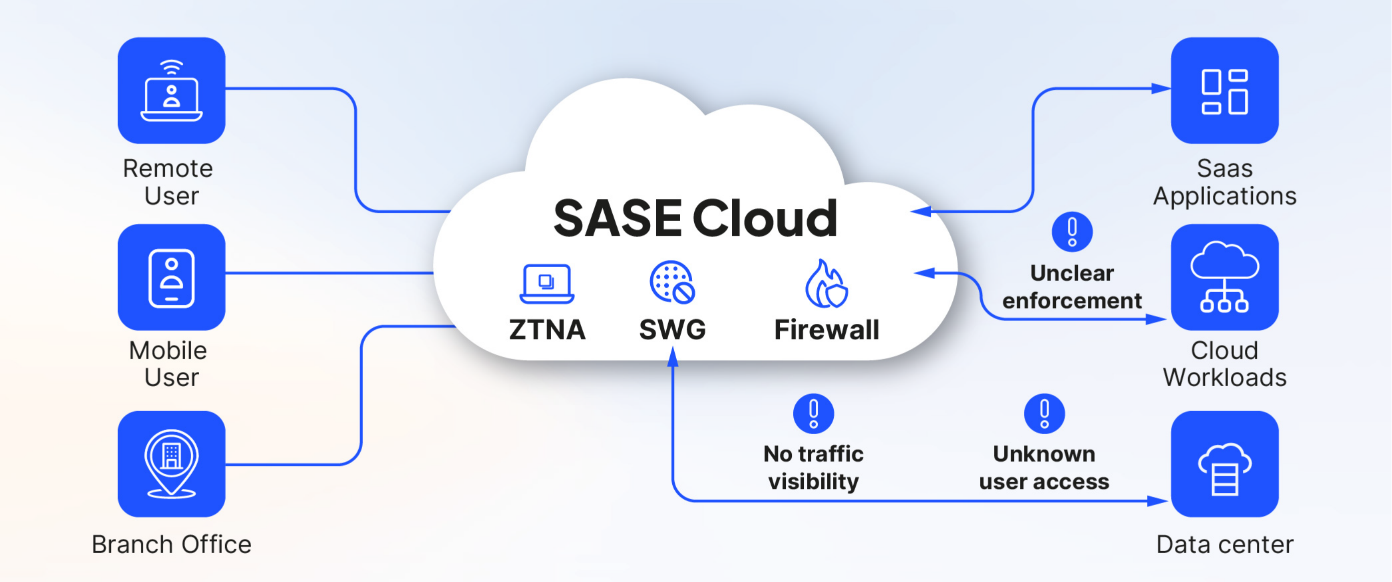
This fragmentation makes it difficult to understand the full scope of access or apply changes consistently. When one team adds a rule for a remote user and another adjusts segmentation for cloud resources, the result is often overlapping, conflicting, or redundant policies that are hard to track and impossible to audit.

This challenge is amplified in environments that use multiple cloud environments, where each platform may operate with its own policy model and enforcement logic.

Visibility breaks down in the most critical places

SASE improves edge-based enforcement but often lacks the observability that data center-based security provides. Remote traffic flows through cloud gateways and access brokers that operate outside of traditional monitoring tools.

As a result, security teams are left without a clear picture of who is accessing what, how policies are being applied, or where coverage gaps may exist.



Without analytics to surface policy usage or traffic intent, stale rules go unnoticed. Policy overlaps remain unresolved. Even well-meaning cleanup efforts become guesswork. Teams lose the context needed to make confident decisions, and that uncertainty slows everything down. It also creates blind spots that make it harder to confirm enforcement, validate access scope, or produce clear audit evidence.

Try This: Internal Visibility Drill

Pick one app or user group.
Can your cloud, security, and network teams all answer:

- Who has access?
- Where is the policy defined and enforced?
- When was it last reviewed?

Manual change management hurts consistency

Despite improvements in tooling, policy change often involves manual handoffs. Even small updates can trigger lengthy workflows involving multiple tools, teams, and handoffs.
In an ideal world, there would be one shared system to validate risk, coordinate actions, or enforce consistency across the stack. Yet, surprisingly, many teams are still using spreadsheets, service tickets, and email to manage changes. Risk is evaluated in silos, and policy updates are inconsistent.

When changes are handled manually and context is scattered, it becomes nearly impossible to trace intent, validate outcomes, or show policy alignment, especially under audit scrutiny. This results in delays in implementing changes, policy misalignment or drift, and slower network and application deployments.

Audit pressure exposes every gap

In many cases, SASE platforms route traffic through global cloud points-of-presence. That routing alone can introduce data residency concerns and jurisdiction-specific compliance obligations.

But the technical setup is only part of the challenge. During audits, many teams struggle to demonstrate who had access, why access was granted, and how enforcement decisions were made. Records are fragmented. Policy history is unclear. Reviews become reactive.

Even frameworks like ISO 27001 or PCI DSS require that enforcement align with documented policy. Without a way to trace decisions across identity, cloud, and network layers, compliance becomes a scramble. Audits that should take hours often take weeks (and even then, gaps are hard to explain).

Making SASE Audit-Ready by Design

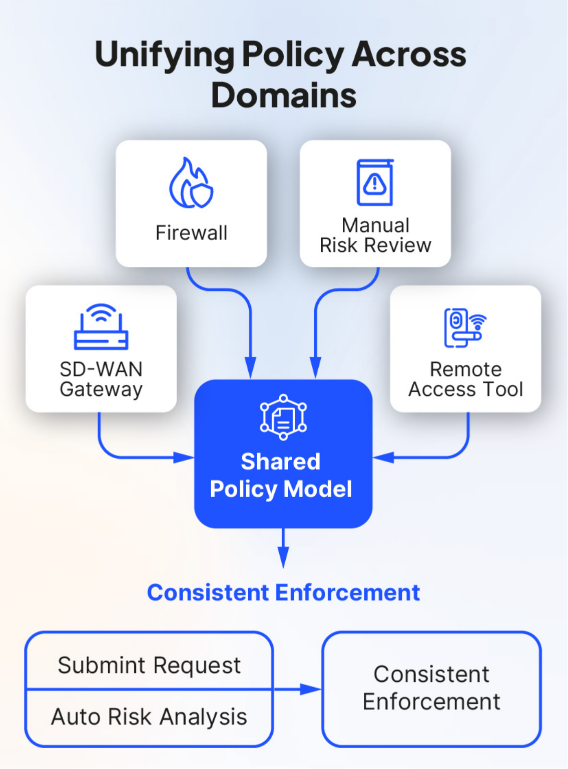
In the previously mentioned scenario,access drift was not caused by a single failure. It came from disconnected teams, legacy rules, and constant change without a shared system to manage it all. That moment forced a shift.

Instead of focusing on adding more tools, the firm began aligning how policy was defined, enforced, and validated. The result was not just cleanup. It marked the beginning of operational maturity.
Organizations that succeed with SASE don't just unify tools. They unify the way policies are built, enforced, and changed. They connect teams, standardize workflows, and use orchestration to ensure visibility and control across every layer.

1. Unify policy across domains

The foundation of compliance is consistent enforcement. But in most environments, policies live in too many places (e.g., firewalls, cloud security groups, SD-WAN gateways, and remote access tools). Each layer works on its own logic, managed by different teams. Organizations that close the compliance gap start by creating a shared policy model that spans all domains. That model needs to normalize syntax, scope, and segmentation logic, so policy is defined once and applied everywhere.

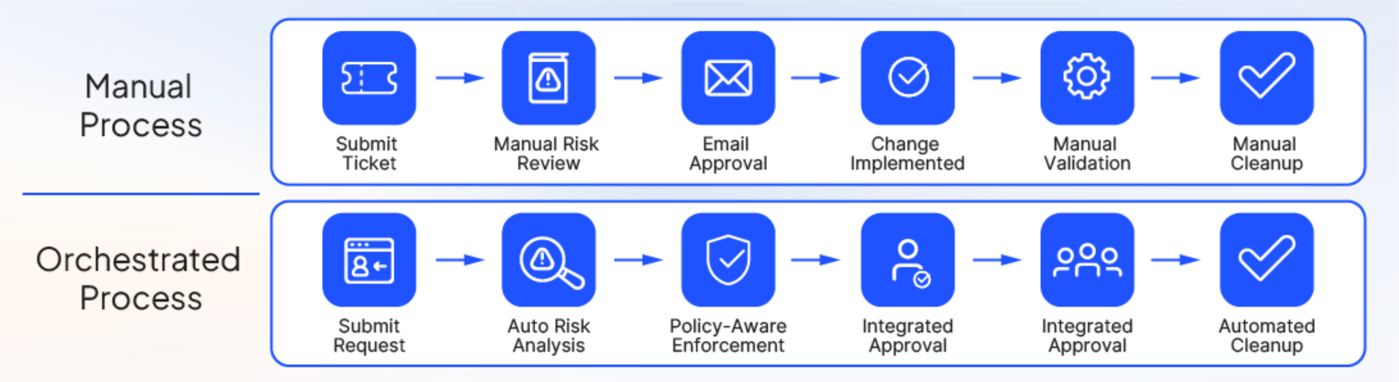
Tufin provides the orchestration layer that connects these enforcement points. Through a central console, policies are aligned and enforced across firewalls, cloud-native controls, SD-WAN, and SASE environments.



2. Automate Change with Confidence via Context

Managing access is not just about approving a request. It's about proving that the change is safe, intentional, and aligned with policy, especially when audits come around.
Mature organizations use automation to enforce this standard at scale. Every change flows through a shared workflow, where risk is evaluated, enforcement is consistent, and cleanup happens by default.

Start by identifying friction points in your current process: approvals, risk validation, and post-change follow-through. From there, apply automation where it creates the most confidence. Tufin orchestrates change management across platforms. Risk checks, rule recommendations, access provisioning, and decommissioning are all part of one connected flow. That means fewer delays, cleaner policy, and stronger audit posture.



3. Validate Policy Usage Before It Becomes Risk

You can't enforce what you can't see. And you can't defend a policy if you don't know whether it's being used, ignored, or exposing your network to unnecessary risk.
Organizations that stay audit-ready make policy usage measurable. They track which rules are enforced. They flag segmentation violations. They surface policies that have drifted from their intent.

With Tufin, teams gain full visibility into usage, exposure, and violations across SASE, firewalls, and cloud. They can pinpoint which rules to keep, which to clean up, and where policies no longer match access needs. This insight is what turns policy visibility into compliance evidence.

4. Foster Collaboration Between Domains

Access decisions span multiple disciplines. Cloud engineers provision resources. Network teams route and segment traffic. Security teams govern policy and risk. In many environments, these domains work from disconnected tools and operate on incomplete information.

One team opens a path. Another blocks it. A third raises a concern after the fact. Without a shared view of posture, intent is lost, and rework follows. In this sense, collaboration becomes reactive.

Organizations that close the compliance gap build cross-functional alignment into daily operations. That starts with a shared system of record: one place to see proposed changes, assess risk, enforce policy, and track access intent.

With Tufin, cloud, network, and security teams work from the same policy baseline. When a rule is proposed, it's validated against segmentation requirements, policy intent, and audit expectations, all in context. Approvals are coordinated, not siloed, and gaps are flagged early. This kind of alignment leads to faster decisions, fewer escalations, and clearer ownership of policy integrity.

Cross-Team Alignment in Action

In mature environments, cloud, security, and network teams work from the same visibility layer.

A cloud engineer opens a port for an application. The network team sees the intent, checks it against segmentation policy, and aligns enforcement. The security team confirms the change is consistent with risk posture and access controls. Audit trails are created automatically and enforcement reflects policy intent, not assumptions.

5. Bake Compliance into Daily Workflows

Compliance should not rely on last-minute checklists or manual evidence gathering. Compliance becomes a constant effort when it is built into how access is approved, how policy is enforced, and how changes are tracked.

Policy justification, access intent, and enforcement validation are captured as part of the workflow. That means audit data is always current and available when needed, not recreated during review cycles.

In mature environments, rule changes are automatically logged with business context. Approvals are tied to user or application need. Access removals are scheduled during the initial request. The result is a security posture that is not only enforced but provable at any moment.

Ask Yourself: Who Owns Policy Consistency?

If you don't have an answer that includes all three (cloud, security, and network) then no one owns it. And that's a governance risk

Conclusion: Orchestration Adds Built-in Governance to SASE

The promise of SASE is real. But that promise only becomes reality when organizations align their access, policy, and enforcement under a shared system. When they build connected processes that standardize change, track outcomes, and validate controls continuously.
Orchestration makes this possible. It brings together the teams, tools, and workflows that shape policy. It ensures that every decision, from access to segmentation to cleanup, can be traced, measured, and aligned to business and regulatory goals.

In this way, compliance becomes part of how security operates day to day. Not an extra step, but an outcome of the way the system is designed. Tufin helps teams maintain consistency, visibility, and audit readiness at scale.

Learn more about Tufin at tufin.com.

Run a Compliance Readiness Check

How aligned is your SASE environment to your internal policy and external regulatory requirements? (Rate from 0–5)

	0	1	2	3	4	5
Access controls are consistently enforced across cloud, firewall, and remote gateways	□	□	□	□	□	□
Policy intent and enforcement logic are documented and traceable	□	□	□	□	□	□
Change requests trigger automated risk validation and cleanup steps	□	□	□	□	□	□
Audit artifacts (who, what, when, why) are generated by default, not manually	□	□	□	□	□	□
You have a shared source of truth for policy across all security domains	□	□	□	□	□	□

Scoring Guidance

5/5 = You're operating with built-in governance
3–4 = Progress made, but still risk of audit gaps or misalignment
0–2 = Policy and compliance are fragmented across tools and teams