Zscaler Zero Trust Gateway for GCP



©2026 Zscaler, Inc. All rights reserved.

TECHNICAL BRIEF

Table of Contents

Introducing the Next Evolution in GCP Security 3

What is GCP Network Security Integration (NSI)? 5

- The producer—consumer model 5
- How it chains together 6

Introducing Zero Trust Gateway as a Zscaler–Managed Service 7

- What Zscaler manages for you 7

Adaptable Deployment Architectures 8

- Use Case 1: Single VPC Project Enforcement 8
- Use Case 2: Multi–VPC Environments within a Single Project 9
- Use Case 3: Shared VPC with Host and Service Projects 10
- Use Case 4: Simplified Ingress Security 11
- Configuring NSI for Zscaler Zero Trust Gateway 12
- ZTGW Policy Enforcement 14

Benefits at a Glance 15

What's Next 16

©2026 Zscaler, Inc. All rights reserved.

Introducing the Next Evolution in GCP Security

The trade-off is over. For years, securing cloud workloads has forced teams into a difficult corner: either accept the heavy operational burden of managing complex security infrastructure or settle for lightweight controls that leave dangerous security gaps. If you've been running workloads on Google Cloud Platform (GCP), you know that compromise all too well.

Today, that changes. Zscaler is proud to announce a major breakthrough for our Zero Trust Cloud offering: a native, fully managed integration with Google Cloud Platform leveraging its Network Security Integration (NSI) service.

We're introducing the Zero Trust Gateway (ZTGW)—a transformative deployment model where Zscaler handles the infrastructure and management so you can focus entirely on security outcomes.

©2026 Zscaler, Inc. All rights reserved.

Why is this a game-changer for your cloud architecture?

Zero Infrastructure: Say goodbye to managing VMs, scaling fleets, or patching appliances.

Zero Compromise: Get full deep-packet inspection, SSL/TLS decryption, and threat prevention without redesigning your network.

Native Simplicity: Utilizing Network Security Integration (NSI), traffic interception occurs at the hypervisor layer, eliminating the requirement for traffic steering to a centralized security Virtual Private Cloud (VPC).

Curious how this works seamlessly within your existing VPCs? Or perhaps you're wondering how to achieve consistent policy enforcement across shared projects without the administrative overhead? The secret lies in our new producer-consumer model.

Read on to discover how you can stop managing infrastructure and start securing your GCP environment with unprecedented speed and depth.

The ZTGW Advantage

Zscaler deploys and manages all Zero Trust Gateway infrastructure for you in GCP. Your projects connect via Google Cloud Network Security Integration (NSI) Security Profiles, which transparently steer workload traffic—including default egress—through the Zscaler Zero Trust Exchange for deep, real-time inspection.

©2026 Zscaler, Inc. All rights reserved.

What is GCP Network Security Integration (NSI)?

Understanding NSI is key to appreciating why ZTGW represents a significant advancement in security architecture. By leveraging Google Cloud's native framework for service insertion, NSI transforms your security model from a complex, infrastructure-heavy burden into a streamlined, high-performance capability.

THE NSI ADVANTAGE FOR YOUR SECURITY STRATEGY:

- **Seamless Operational Simplicity:** NSI intercepts traffic transparently at the hypervisor layer. This eliminates the need for managing complex traffic steering, manual route-table updates, or fragile overlay tunnels. You gain robust protection without modifying your existing network architecture.

- **High-Performance Enforcement:** Unlike traditional approaches that redirect traffic through external appliances, NSI uses GCP's native primitives. By utilizing in-band interception, ZTGW can inspect and enforce policies in real-time, blocking threats before they ever reach your workloads.

- **Native Reliability:** Because traffic is encapsulated via GENEVE and delivered to Zscaler directly by GCP, source and destination addresses are fully preserved. This ensures full visibility and seamless routing, providing the security of an inline appliance with the performance of a native cloud service.

In short, NSI allows you to stop managing the 'plumbing' of security infrastructure and focus purely on the security outcomes that matter to your business.

The producer—consumer model

NSI is built on a clean division of responsibility: a **producer** operates the inspection service, and a **consumer**—the workload owner—steers traffic to it. In this integration, Zscaler is the producer and you are the consumer. Understanding which NSI resources live on which side is what makes "zero infrastructure" clear.

Producer side—created and operated by Zscaler

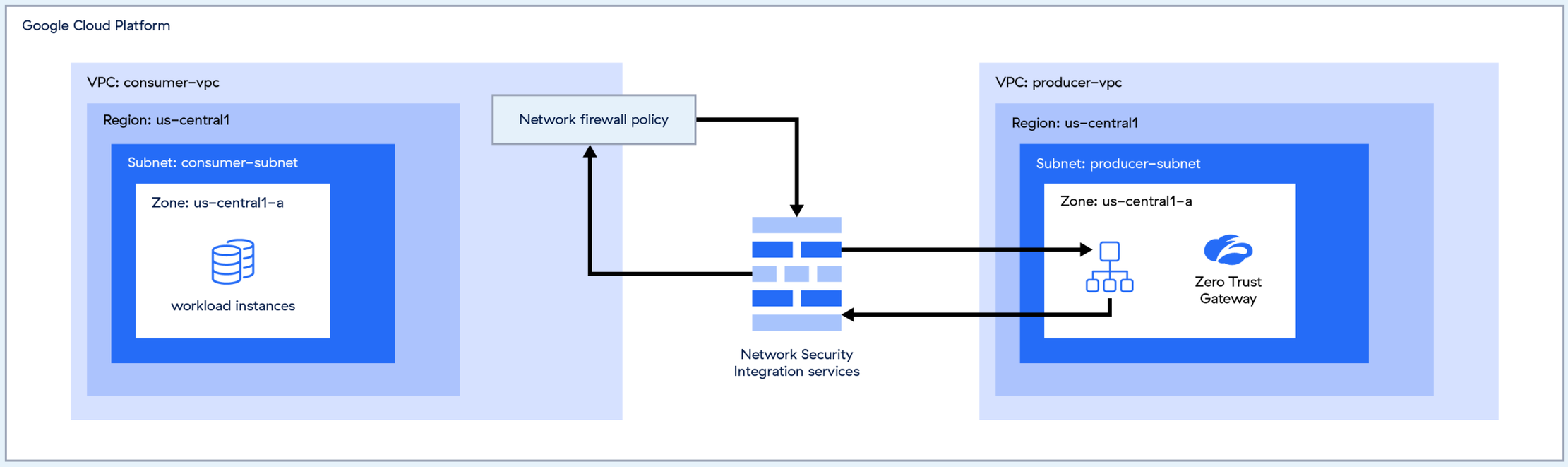
Intercept Deployment

A zonal resource representing the inspection service in a given zone. It points at an internal load balancer that fronts the ZTGW inspection fleet.

Intercept Deployment Group

A global resource that aggregates the zonal Intercept Deployments into a single service offering. This is the only producer resource you ever reference—the VMs, load balancers, scaling, and zonal coverage behind it are invisible to you by design.

©2026 Zscaler, Inc. All rights reserved.



Consumer side—created by you, in your project

Intercept Endpoint Group

A global, per–project resource that references Zscaler's Intercept Deployment Group. It declares your intent to consume the ZTGW inspection service.

Intercept Endpoint Group Association

Connects the Intercept Endpoint Group to one or more of your VPC networks. Only associated VPCs can steer traffic to ZTGW.

Security Profile

An organization–level resource of type custom intercept that references your Intercept Endpoint Group and defines inspection behavior for matched traffic.

Security Profile Group

Aggregates one or more Security Profiles, and is what your firewall rules actually reference—giving you room to apply different inspection profiles to different flows, or start with one and evolve.

Firewall Policy rules

Rules in a global network firewall policy (or hierarchical firewall policy) using the `apply_security_profile_group` action. These are your steering controls: any traffic they match—egress, ingress, or east–west—is intercepted and sent to ZTGW.

How it chains together

Firewall rule → Security Profile Group → Security Profile → Intercept Endpoint Group → Zscaler's Intercept Deployment Group → ZTGW. Every link on your side of that chain is a lightweight reference object—configuration, not infrastructure. Everything that carries, scales, and inspects packets sits on the producer side, where Zscaler builds and runs it.

©2026 Zscaler, Inc. All rights reserved.

Introducing Zero Trust Gateway as a Zscaler-Managed Service

Deploying and managing traditional virtual firewalls creates a massive operational burden. Teams are often forced to manually provision appliances, handle endless lifecycle updates, apply critical patches, and wrestle with scaling requirements just to keep traffic moving. This approach turns security into a high-maintenance administrative drain—one that grows increasingly fragile and complex as your cloud footprint expands.

With the Zero Trust Gateway (ZTGW) on GCP, Zscaler assumes full responsibility for this infrastructure. This shifts your operational role from managing appliances to managing policy, allowing your team to focus exclusively on security outcomes.

What Zscaler manages for you

- **Infrastructure Management:** We fully provision and operate the ZTGW environment, including all load balancers and service attachments. You gain a turn-key solution without the burden of cloud resource administration.
- **Dynamic Auto-Scaling:** The service automatically scales capacity in real-time based on traffic demand, ensuring consistent, high-performance security without manual intervention.
- **Maintenance-Free Security:** Zscaler handles all updates, patches, and feature releases. You benefit from continuous security innovation without downtime or maintenance windows.
- **Proactive Monitoring & High Availability:** We provide 24/7 health monitoring and built-in redundancy. You receive reliable, enterprise-grade uptime without needing to manage service availability.
- **Centralized Visibility:** Gain instant insights into threats and traffic patterns directly within the Zscaler Admin Portal, removing the need for manual, complex logging configurations.
- **Predictable Cost Efficiency:** By shifting infrastructure and scaling responsibilities to Zscaler, you benefit from a streamlined, service-based cost model that eliminates hidden overhead.

What you manage is simply your GCP Firewall Policies and your Zscaler security policy configuration in the Admin Portal. Everything else is Zscaler's responsibility.

©2026 Zscaler, Inc. All rights reserved.

Adaptable Deployment Architectures

The Zero Trust Gateway (ZTGW) is designed to integrate seamlessly into your existing environment. Unlike traditional security appliances that demand disruptive network overhauls, the GCP NSI integration respects and adapts to the architectures enterprises already use. You can strengthen your security posture immediately, without the need for a complex network redesign.

Explore the primary deployment patterns below to see how ZTGW leverages NSI Security Profiles to provide transparent traffic steering across the most common GCP topologies.

Use Case 1: Single VPC Project Enforcement

In this deployment model, a single consumer GCP project with one VPC is fully instrumented for Zero Trust traffic enforcement through Zscaler Zero Trust Gateway. All NSI configuration is scoped to this project, steering every traffic flow outbound internet, private application access, and east-west lateral movement to the Zscaler Project hosting the Zero Trust Gateway. No additional hub VPC is required.

This pattern is ideal for organizations adopting Zero Trust incrementally, starting with a single project before scaling the model across their broader GCP environment. It also serves as the reference architecture for validating all three enforcement paths in a contained, repeatable setup.

How traffic flows:

Intelligent Interception: Workload traffic matching your GCP firewall rules—whether destined for the internet, private apps, or other internal workloads—is automatically identified by NSI.

Direct Steering: Packets are steered transparently to the ZTGW endpoint, maintaining original IP headers for full visibility.

Deep Inspection: Zscaler enforces your Zero Trust policies and performs real-time threat prevention at scale.

Policy-Driven Delivery: Approved traffic is forwarded securely based on its destination:

- **External Access (ZIA):** Secure internet egress with full SSL/TLS inspection, advanced threat protection and DLP.
- **Lateral Movement (East-West):** Intra-VPC traffic is subject to the same rigorous security standards as external flows.

©2026 Zscaler, Inc. All rights reserved.

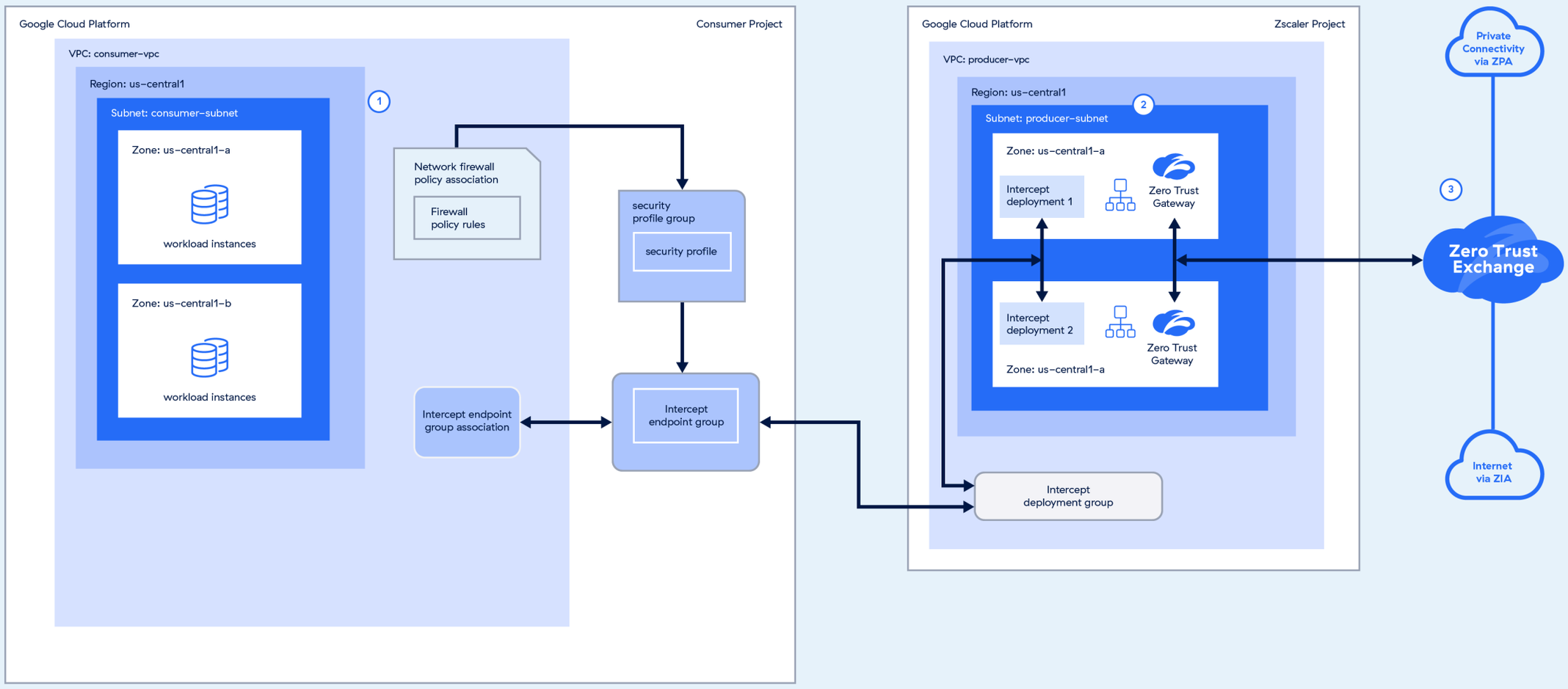


Figure 2: Traffic from the workload are intercepted and forwarded to Zscaler ZTGW for inspection

Use Case 2: Multi-VPC Environments within a Single Project

Organizations with multiple VPCs in a single project—segmented by environment (Dev, Test, Prod) or function—need consistent Zero Trust enforcement without the complexity of a shared hub. This model empowers you with:

- **Granular Control:** Apply unique security profiles to each VPC based on specific workload needs.
- **Unified Security:** Funnel all traffic through a single, Zscaler-managed ZTGW for deep inspection.
- **Operational Efficiency:** Eliminate the "hub-and-spoke" tax by steering traffic directly from each VPC.

Traffic flow:

1. A workload generates traffic within its specific VPC.
2. The VPC's Network Firewall Policy matches the flow and triggers NSI interception.
3. NSI steers the packet to the ZTGW for real-time inspection and policy enforcement.

Configuration Tip: Every VPC requires an independent endpoint group association. Use shared Security Profile Groups to maintain common policies across VPCs while keeping enforcement boundaries separate.

©2026 Zscaler, Inc. All rights reserved.

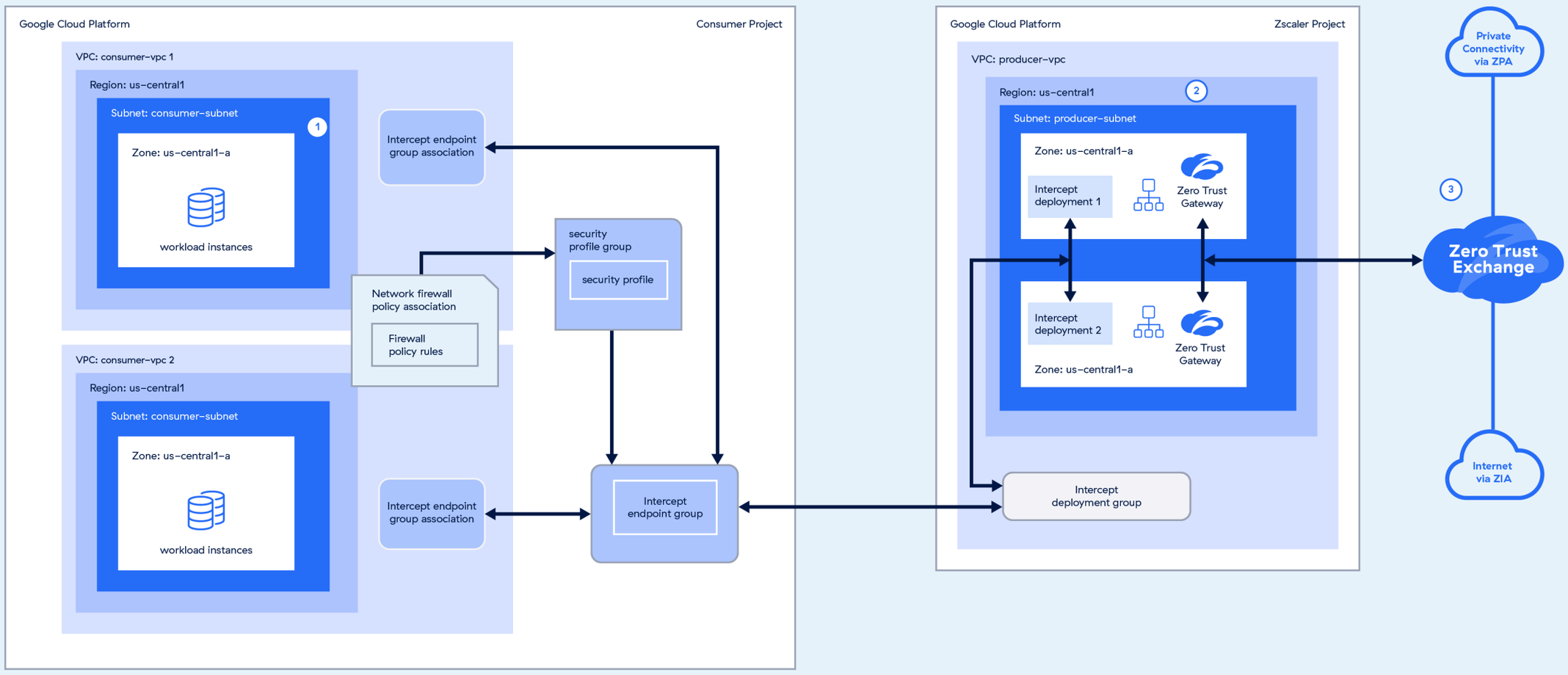


Figure 3: Multiple VPCs connected to Zscaler ZTGW via NSI

Use Case 3: Shared VPC with Host and Service Projects

In complex enterprise environments, the Shared VPC model separates network management (Host Project) from workload ownership (Service Projects). ZTGW integrates into this hierarchy to provide:

- **Centralized Security Governance:** Platform teams define inspection rules once in the Host Project, ensuring compliance across all service projects.
- **Reduced Operational Overhead:** Service project teams focus on their apps, inheriting robust security automatically without managing NSI or ZTGW configurations.
- **Seamless Integration:** Security follows the subnet; any workload deployed into the shared network is instantly protected.

Traffic flow:

1. A workload in a Service Project generates traffic within a shared subnet.
2. The Host Project's Network Firewall Policy intercepts the traffic at the hypervisor layer.
3. NSI steers the traffic to the ZTGW for inspection based on Host-defined security profiles.

For **Shared VPC**, the host project should own the endpoint group association and firewall policy association because it owns the VPC/subnets.

©2026 Zscaler, Inc. All rights reserved.

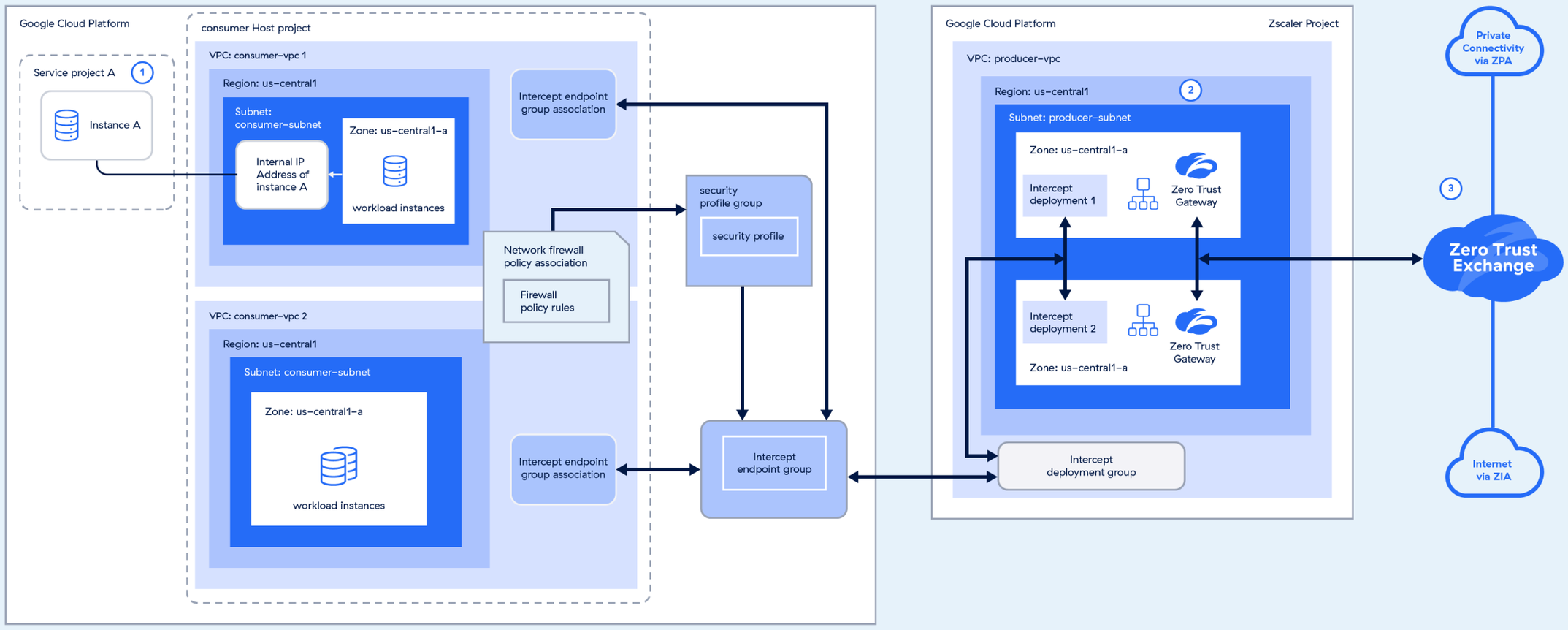


Figure 4: Shared VPC – NSI Security Profiles connecting directly to ZTGW

Use Case 4: Simplified Ingress Security

Securing inbound traffic often forces organizations into complex, high-maintenance network architectures. With the Zero Trust Gateway (ZTGW) on GCP, you can secure ingress traffic natively and transparently. This model decouples your workload environment from the security inspection layer, allowing you to enforce robust inspection without the administrative overhead of VPC peering, NAT, or complex proxy configurations.

KEY CUSTOMER BENEFITS:

- **Transparent Enforcement:** Workloads receive traffic as if no inspection were in the path, with full preservation of original client IPs and packet headers.
- **Clean Separation of Duties:** Clearly delineate the security provider (Zscaler) from the workload owner, simplifying governance and reducing configuration errors.
- **Architecture Agility:** Secure inbound traffic without needing to redesign your network, establish VPC peering, or manage complex shared subnet structures.
- **Consistent Security Posture:** Apply the same enterprise-grade threat protection to inbound traffic that you use for internal and outbound flows.

Traffic flow:

1. **Arrival:** External traffic enters through the Passthrough External Network Load Balancer, preserving original packet headers.
2. **Interception:** The Network Firewall Policy matches incoming packets and triggers NSI redirection before they reach the workload.
3. **Steering:** The Intercept Endpoint Group securely routes packets from the consumer VPC to Zscaler's producer VPC.
4. **Inspection & Delivery:** ZTGW inspects the traffic and returns approved packets to the consumer VPC for transparent delivery to the destination.

©2026 Zscaler, Inc. All rights reserved.

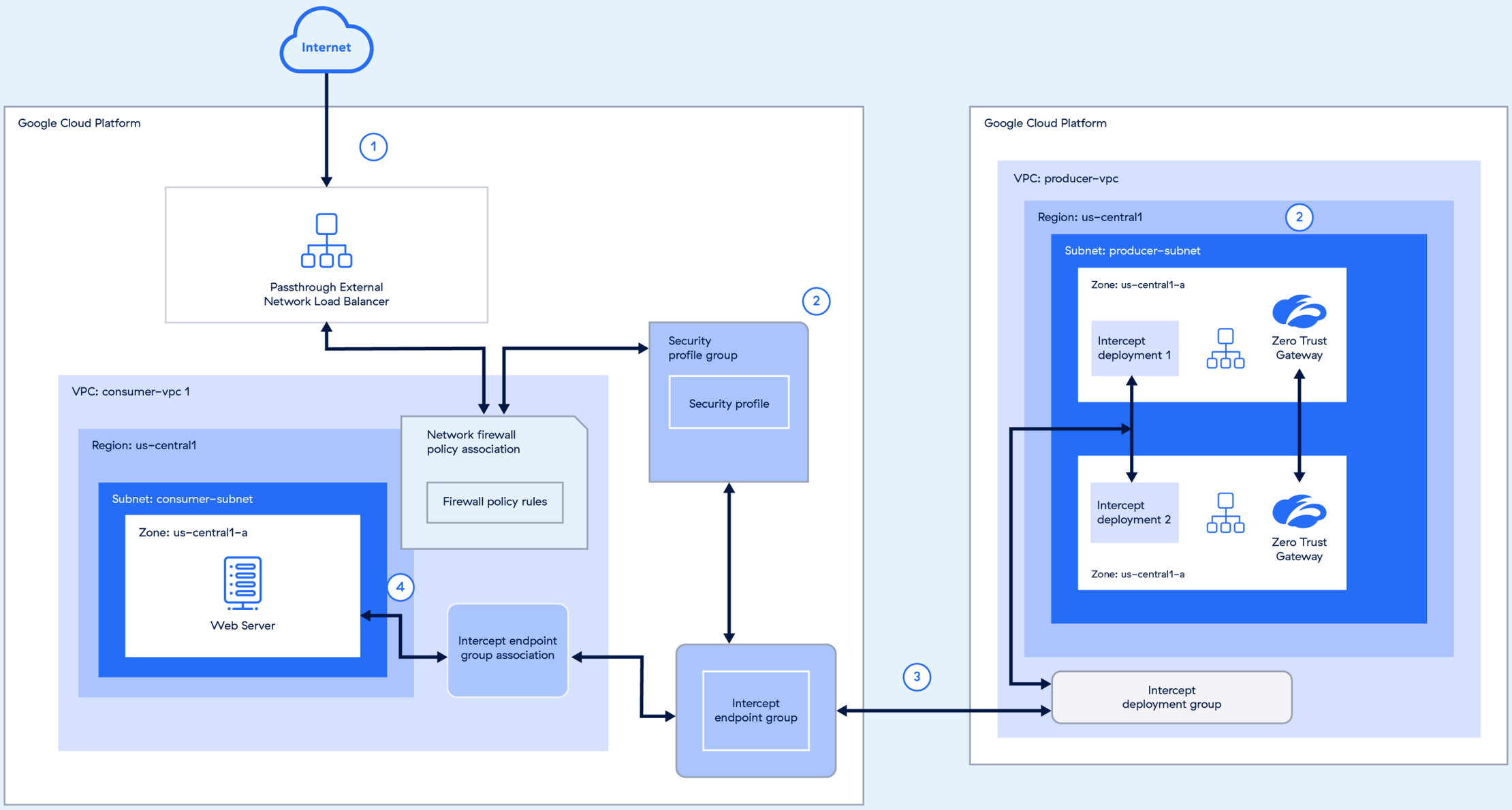


Figure 5: Ingress traffic is intercepted by NSI and redirected to ZTGW for inspection

Steering default traffic

Zscaler recommends configuring a low-priority default-egress rule (0.0.0.0/0) in your Firewall Policy to ensure all workload egress traffic is inspected. Higher-priority 'allow' or 'deny' rules can then be placed above it to selectively exclude specific internal or management flows from inspection—giving you full control without all-or-nothing enforcement.

Configuring NSI for Zscaler Zero Trust Gateway

Transitioning to a Zero Trust architecture on Google Cloud is a streamlined experience. By offloading the "producer" side—the entire inspection infrastructure—to Zscaler, your team can focus exclusively on the "consumer" side: defining the traffic you want to secure. This two-part workflow ensures a rapid deployment with minimal operational friction.

©2026 Zscaler, Inc. All rights reserved.

Step 1: Obtain the Zscaler Service Reference—Connects Your Environment to the Zscaler Cloud

Receive the Intercept Deployment Group reference from Zscaler. This single object represents the entire Zscaler-managed inspection service, making it available as a native resource within your GCP environment.

Step 2: Create an Intercept Endpoint Group—Declares Your Intent to Secure Traffic

Establish a local endpoint group in your project that points to Zscaler. This serves as your project's private "on-ramp" to the Zero Trust Gateway, ensuring traffic is routed through a trusted path.

Step 3: Associate the Endpoint Group with Your VPC—Activates Security for Your Network

Create an Intercept Endpoint Group Association for each VPC whose traffic should be inspected. In a single-VPC deployment, this association is created in the workload project. In a Shared VPC deployment, it is created in the host project that owns the network.

Step 4: Define a Custom Intercept Security Profile—Specifies the Inspection Path

Create a Security Profile that targets your Intercept Endpoint Group. This tells GCP exactly where to send packets for deep inspection without requiring manual routing updates.

Step 5: Assemble a Security Profile Group—Simplifies Policy Management

Create a Security Profile Group and attach the custom intercept Security Profile to it. Firewall policies reference the Security Profile Group, not the individual profile.

Step 6: Configure Firewall Policy Rules—Implements Precise Traffic Steering

Create global or hierarchical firewall policy rules that match the traffic you want inspected and set the rule action to `apply_security_profile_group`. Rules can be broad, such as inspecting default egress, or narrow, such as inspecting only traffic from production workloads, specific subnets, secure tags, protocols, or destinations.

©2026 Zscaler, Inc. All rights reserved.

Step 7: Bind the Policy to the VPC—Initiates Transparent Protection

Finalize the setup by associating the firewall policy with your VPC. Once active, traffic is intercepted at the hypervisor level, providing robust security with zero impact on network performance.

Step 8: Validate Enforcement—Confirms Visibility and Security Outcomes

Monitor the active associations and traffic logs in the Zscaler Admin Portal. This validation ensures that your security policies are being enforced exactly as intended across your cloud resources.

The beauty of this integration lies in its transparency. When a firewall rule triggers, Google Cloud handles the heavy lifting by securely encapsulating and delivering packets to Zscaler via NSI. Because this process happens at the hypervisor layer, your workloads remain entirely unaware of the inspection path—requiring no changes to your application code, IP addresses, or complex route tables. You get enterprise-grade security without a single network redesign.

ZTGW Policy Enforcement

Upon arrival at the ZTGW, traffic is subject to the security policies configured within your Zscaler Admin Portal. These tenant-scoped policies leverage metadata forwarded by NSI, such as network tags and GCP resource labels, to allow for granular refinement.

Consequently, you can easily implement tailored controls, such as strict DLP parameters for workloads tagged as ‘environment:prod’ or distinct URL filtering criteria for development versus staging environments. This integrates your GCP resource structure directly into the Zero Trust policy engine rather than keeping it isolated.

©2026 Zscaler, Inc. All rights reserved.

Benefits at a Glance

Here's a summary of what the Zscaler ZTGW on GCP delivers out of the box:

CAPABILITY	WHAT IT MEANS FOR YOUR BUSINESS
SSL/TLS INSPECTION	Full decryption and inspection of encrypted traffic—no blind spots in HTTPS flows, even at scale. All handled in the Zscaler cloud.
ADVANCED THREAT PROTECTION	Real-time defense against malware, ransomware, and zero-day exploits, powered by Zscaler ThreatLabz threat intelligence updated continuously across the Zero Trust Exchange.
DATA LOSS PREVENTION	Inline DLP scanning prevents sensitive data from leaving your GCP environment through any protocol—including cloud storage, API calls, and SaaS uploads.
CLOUD SANDBOX	Unknown files and payloads are detonated in an isolated environment before they're allowed to reach their destination—stopping zero-day threats before they land.
GCP-NATIVE POLICY CONTEXT	GCP resource labels and network tags are forwarded as policy metadata, enabling context-aware Zero Trust enforcement tied directly to your cloud resource hierarchy.
NO INFRASTRUCTURE TO MANAGE	Zero VMs, zero scaling configuration, zero patching. Zscaler runs the entire ZTGW service. You connect, configure policy, and focus on your business.
UNIFIED MULTI-CLOUD VISIBILITY	Centralized logging and policy management across GCP, AWS, Azure, and on-premises—through a single Zscaler Admin Portal with real-time threat and traffic intelligence.

©2026 Zscaler, Inc. All rights reserved.

What's Next

The Zero Trust Gateway on GCP offers the most streamlined, high-performance path to enterprise-grade workload security on Google Cloud. By eliminating infrastructure management, scaling, and maintenance, we allow you to focus entirely on your security outcomes, not your plumbing.

Key benefits of the Zscaler Zero Trust Gateway include:

- **Operational Simplicity:** Zero VMs to manage, zero scaling configuration, and zero patching.
- **Deep Security:** Full-stack protection, including SSL/TLS inspection, advanced threat protection, and inline DLP.
- **Native Integration:** Transparent traffic steering via GCP NSI with no network redesign required.
- **Context-Aware Policy:** Granular enforcement using native GCP metadata.

Ready to transform your cloud security? Stop managing infrastructure and start securing your workloads with unprecedented speed and depth. Reach out to your account team today or visit Zero Trust Cloud to see how we can secure your GCP environment.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at **zscaler.com/legal/trademarks** are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Act Fast.
Stay Secure.