netskope

Whitepaper

Secure Access to Private Applications in AWS

A Zero Trust approach is needed to modernize connectivity and reduce business risk for the hybrid workforce

Introduction

Organizations have been focusing on modernizing their IT infrastructures for more than a decade now, chiefly by migrating private applications and workloads out of physical data centers protected by a "castle and moat" assortment of security appliances, to public cloud providers such as Amazon Web Services (AWS). Reasons given for migration to cloud-based Infrastructure-as-a-Service (IaaS) platforms are varied; however, they often include advantages such as flexibility, scalability, faster app deployment, and cost savings. The change has been so dramatic that Gartner predicts around 51% of IT spending will have shifted from traditional solutions to the public cloud by 2025—compared to just 41% in 2022. And by 2026, 75% of organizations will adopt a digital transformation model based on the cloud as their underlying platform.

With 40% market share, AWS is the largest IaaS provider, serving some of the largest enterprises across the globe. While AWS is responsible for security of the underlying infrastructure and services they provide, security of applications and data is solely the customer's responsibility. Rightly, organizations pay a great deal of attention to protecting apps and data from an infrastructure perspective. Yet when it comes to providing hybrid workers with access to cloud-based private apps, traditional approaches such as virtual private networks (VPNs) can create security gaps that unnecessarily expose sensitive data and resources to threats and attacks. This is where Zero Trust Network Access (ZTNA) can be used to augment or replace VPNs, providing workers with a more secure way to access private apps from anywhere, and reducing risk for organizations embracing the migration to public cloud.

CHALLENGES TO PROVIDING SECURE ACCESS FOR HYBRID AND REMOTE WORKERS

IT departments have historically connected workers to cloud-based applications through the corporate network. When in the office, workers simply log on to the local area network (LAN), and when working remotely, they connect to the corporate network over an encrypted VPN connection. A VPN gateway or concentrator appliance is used to terminate the VPN connection (see Figure 1). This approach is adequate when a small percentage of workers are remote and latency associated with backhauling traffic through the security stack in the corporate data center can be tolerated. Site-to-cloud connections then carry traffic on its final leg between corporate offices and the cloud provider, typically over another VPN connection, or a cloud provider service such as AWS Direct Connect.

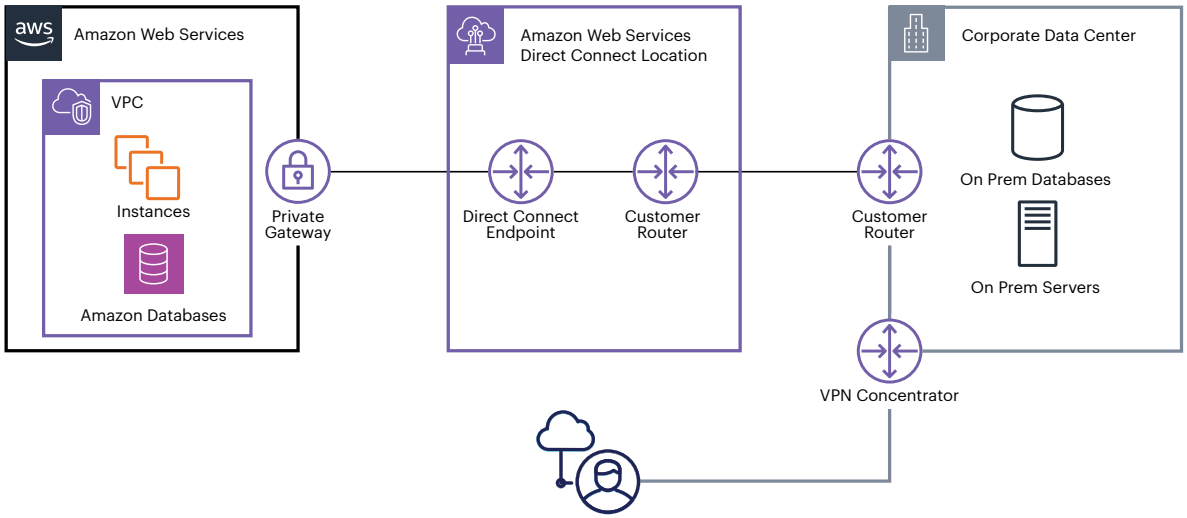

Figure 1: Remote access to AWS-based resources via an on-premises VPN concentrator.

Today, remote workers constitute a much larger percentage of the workforce. A recent Pew Research Center survey states that 35% of workers who have jobs that can be performed remotely work from home all the time. In addition, contractors, consultants, suppliers, and other third parties often need access to specific internal or private resources using devices that are not managed by the organization.

As more people work and connect remotely, more VPN appliances are necessary, imposing additional maintenance demands on already stretched IT teams. Backhauling traffic from remote workers through the corporate data center also becomes less appealing as latency increases and begins to impact worker productivity.

> "Around 51% of IT spending will have shifted from traditional solutions to the public cloud by 2025."
>
> – Gartner

VPN gateways also create security concerns. By design, they must expose their IP addresses to the public internet to allow user connectivity which leaves them open to discovery by port scanners. Once the IP address is known, attackers can probe for vulnerability exploits that can be used to gain a foothold. And, most alarmingly, remote VPN users are often given full access to the corporate network—

along with all applications and resources—automatically exposing these resources to any attackers who manage to gain access to the VPN gateway appliance. This outdated arrangement increases risk and can create headaches for security teams, especially when multiple appliances are under management.

Some organizations address traffic backhauling latency issues by deploying a VPN concentrator virtual appliance in the cloud. This setup can reduce latency for remote workers by connecting them more directly to cloud resources (see Figure 2). However, cloud-based VPN concentrator IP addresses must also be exposed to the public internet to allow connectivity, and bypassing the security stack only further compounds security and compliance issues. Scalability and maintenance issues also remain.

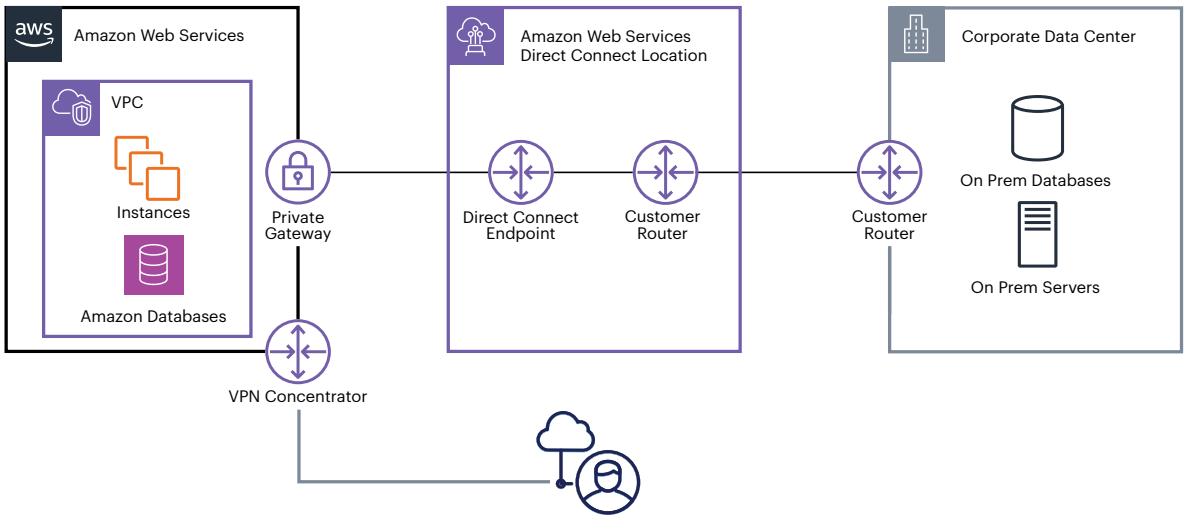

Figure 2: Remote access to AWS resources via a cloud-based VPN concentrator.

With myriad problems inherent in VPN solutions, it's clear that a modern, cloud-native approach is needed to connect remote and hybrid workers to cloud-based apps and resources

THE SOLUTION: A ZERO TRUST NETWORK ACCESS (ZTNA) APPROACH

Forward-thinking organizations are increasingly turning to Zero Trust Network Access (ZTNA) for a more secure and flexible way to connect their workforce, leaving behind legacy VPNs.

ZTNA flips the traditional approach to remote access by taking a default deny posture and providing only the access to an application or service that a user has been explicitly authorized. This challenges the "connect first, verify later" approach of VPNs, where users are implicitly trusted with broad access to the network and resources, creating security risks and gaps in visibility.

> "By 2025, at least 70% of new remote access deployments will be served predominantly by zero trust network access (ZTNA) as opposed to VPN services."
>
> – Gartner

ZTNA, on the other hand, takes the approach of "verify first, connect later." Applications are registered with a ZTNA gateway and then connected to a ZTNA trust broker. When a user attempts to connect to an application, they are required to authenticate with the ZTNA trust broker which verifies their identity, the security posture of their device, and the applications they are authorized to use, before they are allowed to establish a connection to the application they need (see Figure 3). This approach ensures that users are denied access by default and only granted least-privilege access, reducing the attack surface, limiting unauthorized lateral movement, and thus improving overall security posture.

It's important to understand the difference between ZTNA and zero trust. ZTNA is a category of products that provides secure access to applications and services using granular identity- and context-based access control policies. ZTNA is built on the principles of zero trust and is a key component of a zero trust architecture.

Meanwhile, zero trust is a security framework and strategy that operates on an "never trust, always verify" paradigm and seeks to prevent unauthorized access by implementing three key principles: 1) always assume breach, 2) explicitly verify all requests and 3) strictly enforce least-privilege access. Instead of assuming that everything within the network (i.e., behind the corporate firewall) can be inherently trusted, zero trust is premised on the idea that threats can originate from anywhere – both inside and outside the network – and therefore, no entity should be trusted.

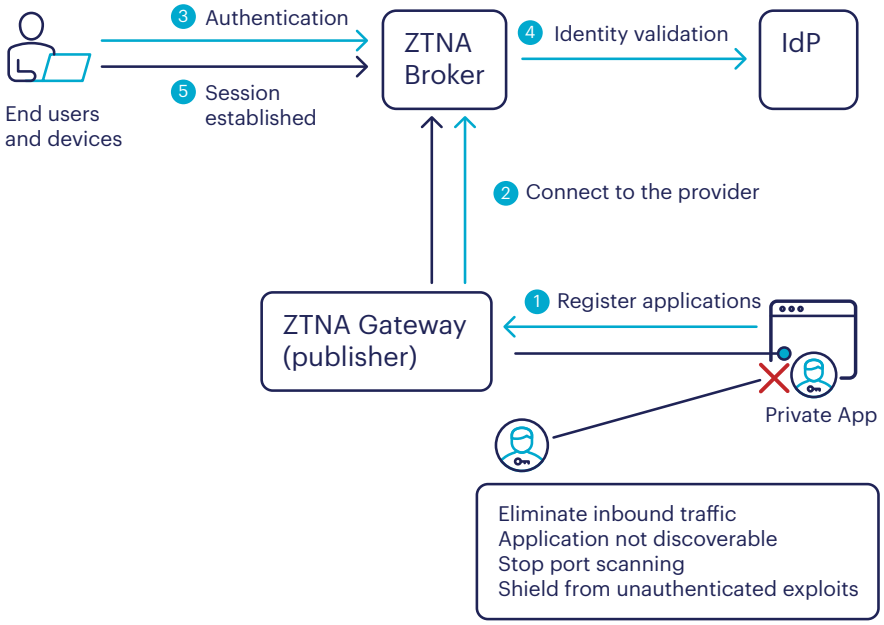

Figure 3: How ZTNA works.

Here are the key benefits of using a ZTNA approach to connect hybrid workers to cloud-based apps:

- **Least-privilege access:** ZTNA enforces the principle of least privilege, ensuring that users and devices only have access to the specific resources they need to perform their tasks. This reduces the potential impact of a security breach and limits unauthorized access.
- **Secure remote connectivity:** ZTNA allows secure access to resources regardless of the user's location, ensuring that security is maintained when accessing resources from outside the corporate network.

- **Dynamic trust:** ZTNA evaluates trust dynamically based on various factors, such as user identity, device posture, location, and behavior. Trust is not assumed based solely on being inside the network perimeter, but rather continuously verified throughout the user's session.
- **Improved security posture and compliance:** By adopting ZTNA, organizations can enhance their overall security posture by reducing the risk of lateral movement within the network, helping organizations meet compliance requirements.
- **Secure cloud migration:** With organizations migrating to cloud services, ZTNA provides a more secure way to connect users and applications to cloud resources without exposing them directly to the public internet.

NETSKOPE PROVIDES ZTNA AND MORE FOR AWS CUSTOMERS

Netskope Private Access (NPA)—Netskope's ZTNA solution and modern alternative to legacy VPNs—provides remote and hybrid workers with secure, highly scalable access to private apps running on AWS. NPA can replace VPNs for workers across the organization. For example, it can also provide access to private apps running on-premises in physical data centers, or in multi-cloud scenarios it can provide access to apps running on other cloud provider platforms such as Microsoft Azure and Google Cloud. With NPA, organizations can finally retire outdated VPN appliances and replace them with a modern, secure, cloud-native alternative.

NPA allows authenticated users to access authorized applications on an app-by-app basis, instead of the entire corporate network. It's easy to see how NPA would also be useful in scenarios such as providing controlled access to apps for partners and contractors. With NPA, administrators can grant and revoke access to both workers and third parties as needed, whether or not they have a Netskope client installed on their user device. Also, user groups can be created to simplify access to authorized apps and resources for different categories of users.

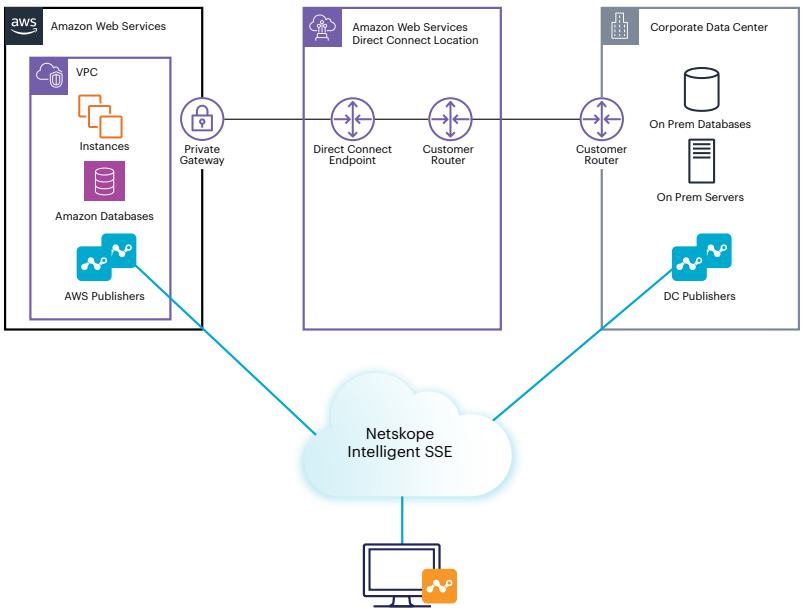

Figure 4: Netskope Private Access providing secure connectivity to AWS and on-premises private applications and resources.

Organizations using NPA to provide access to apps and resources in AWS benefit from an in-depth understanding of risk exposure. They can inventory assets, detect misconfigurations, enforce compliance standards, and also protect against insider threats and malware.

NPA provides seamless and direct access to AWS for authenticated users, supporting any application and protocol. It delivers direct connectivity that is secure, flexible, highly scalable, and protects data and resources through automation, with application-level access control based on user identity and device security posture.

KEY BENEFITS:

Delivers a fast, seamless end-user experience: Netskope connects users directly to AWS-hosted private applications without a VPN. Eliminates the need to backhaul remote user traffic to the data center for security, thereby avoiding performance bottlenecks.

Reduces the overall attack surface: By hiding private applications behind Netskope's Security Cloud, VPNs, protocols, and services are no longer exposed to the public internet, making them undiscoverable to potential attackers.

Limits lateral threat movement: With granular, application-level access control policies, Netskope enforces least-privilege on resources and grants only the minimum level of access to applications – not the network.

Protects data and mitigates insider risk: Netskope detects sensitive data movement and insiders' anomalous behaviors with user and entity behavior analytics (UEBA) and advanced data loss prevention (DLP).

Simplifies operations: Secure hybrid workforces with Netskope's Secure Access Service Edge (SASE), a single unified solution that fully converges network and security capabilities including ZTNA, SWG, CASB, FWaaS, and SD-WAN. Consolidates multiple point products and reduces complexity, while increasing agility (see Figure 5).

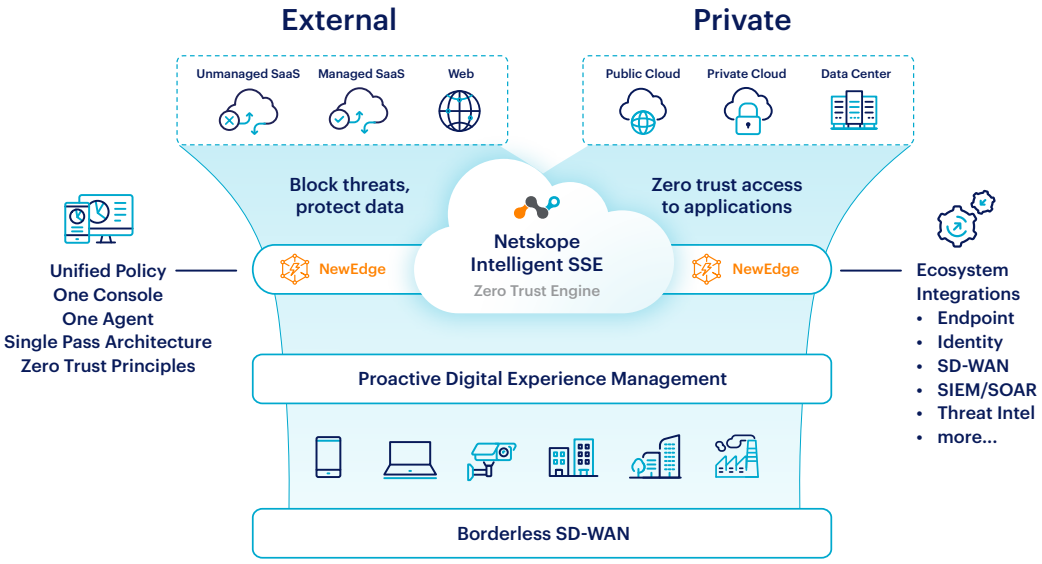

Figure 5: The Netskope SASE platform.

NPA can accommodate a variety of needs, including broad application support, third-party and bring your own device (BYOD) access, granular access control, app discovery, private infrastructure management, analytics and reporting, API automation, and data protection. Pre-logon enables quick onboarding of new employees with self-service provisioning on a new PC. Administrators can leverage enterprise device certificates to ensure that only sanctioned devices have access to internal applications.

To simplify administration, NPA is tightly integrated into the Netskope SASE platform with a single policy engine and user interface for app configuration, policy, analytics, and reporting across all Netskope services.

COMPELLING USE CASES FOR VPN REPLACEMENT

Getting started with ZTNA doesn't have to be difficult or overwhelming. Here are six common use cases that represent the biggest application access challenges organizations are facing today:

- **VPN Replacement:** Simplify connectivity and improve security outcomes by eliminating exposed IP addresses and maintenance issues associated with multiple VPN appliances and concentrators.
- **Hybrid Workforce:** Enable fast, seamless access to applications for all users - no matter where they're located – to boost workforce productivity and reduce the time spent managing separate policies.
- **Cloud Migration:** Provide native access to resources hosted in AWS virtual private cloud (VPC) environments, removing the need to hairpin remote user traffic through the data center, for faster transition to the cloud.
- **Third Party Access:** Give external collaborators, such as contractors, vendors and partners, a frictionless user experience through clientless browser access to private applications, eliminating the need for additional client installation.
- **M&A Integration:** Enable day-one access to mission-critical internal resources, bypassing the need for complex VPN setup and eliminating the complexity of merging networks.

CONCLUSION

As organizations worldwide continue to navigate evolving business needs, including those of a hybrid workforce, traditional approaches to connect workers to business-critical private applications on AWS are clearly no longer sufficient.

Instead, successful organizations will be the ones that choose to adopt a modern remote access solution based on zero trust principles that minimize risk and modernize cloud connectivity, and Netskope is the best choice for organizations looking to maximize the benefits of migrating private apps to AWS.

Netskope's zero trust security solutions are available for purchase on the AWS Marketplace.

Learn more about Netskope for AWS

aws PARTNER Security Software Competency

aws Available in AWS Marketplace

Interested in learning more?

Request a demo

Netskope, a global SASE leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. Fast and easy to use, the Netskope platform provides optimized access and real-time security for people, devices, and data anywhere they go. Netskope helps customers reduce risk, accelerate performance, and get unrivalled visibility into any cloud, web, and private application activity. Thousands of customers, including more than 25 of the Fortune 100, trust Netskope and its powerful NewEdge network to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements.

Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.