netskope

White Paper

Delivering on the Promise of 100% Legacy VPN Retirement

DELIVERING ON THE PROMISE OF 100% LEGACY VPN RETIREMENT

As demand for remote working has increased, the security and performance limitations of virtual private network (VPN) technology have become apparent. Cloud-delivered ZTNA is viewed as the modern alternative to remote access VPN. However, enterprises upgrading to modern ZTNA often face application compatibility issues, and as a result, enterprises must keep a small remote access VPN footprint until they can modernize their application infrastructure, which sometimes takes years. In this paper, we will examine an innovative method that enables organizations to complete the move from VPN technologies and embrace a new architecture that's better able to meet the needs of remote working.

THE LIMITATIONS OF VPNS

Remote access VPN creates an encrypted tunnel that connects endpoint devices to the network and assigns a network IP address for the device, virtually placing the device on the network. Most commonly, remote user traffic is terminated at the private data center. From there, through complex network routing, the user's traffic is then connected to the public cloud infrastructure and other data centers. Although remote access VPN can be integrated with a third-party identity provider and leverage multi-factor authentication, VPNs operate on a "connect first verify later" basis. There are several significant drawbacks to VPNs that can leave enterprises at greater risk of security threats, including:

- **Public-facing services.** VPN concentrators are exposed to the internet and are often unpatched, misconfigured, and not well protected, making them a tempting target for threat actors. In a recent survey, 44% of cybersecurity professionals report an increase in exploits targeting their organization's VPN since the shift to remote and hybrid work.[1]
- **Outside-in traffic flows.** For a VPN to function, the network security must "poke a hole" in the enterprise firewall that allows traffic to come in from outside the perimeter. This represents an opportunity for hackers to breach a company's defenses. Studies suggest that attackers are targeting vulnerabilities in a wide range of VPN appliances.[2] To mitigate this threat, organizations need to invest heavily in VPN concentrators to apply security policies to create safe tunnels.
- **Delayed authentication.** Although some VPNs can leverage multi-factor authentication, the protection this provides is weakened by the fact that traffic is granted access to the network prior to authentication taking place. This provides an opportunity for cybercriminals to gain a foothold on the network.
- **Permit unauthorized lateral movement.** Remote access VPN technology, using IP-based routing, virtually places devices onto the network and assigns each device with an IP address. In most cases corporate networks are coarsely segmented with VPN connected devices able to move laterally, free to explore and discover other assets, and have more access than necessary.

[1] "Cybercriminals are after VPNs – don't make it easy for them," Cybernews, September 26, 2022

[2] "Attackers Heavily Targeting VPN Vulnerabilities," Dark Reading, April 2021

Legacy remote access VPNs can provide decent performance if the concentrator and workload are hosted in the same data center. However modern enterprise infrastructures require complex deployment and traffic routing, creating a range of issues:

- **Latency from backhauling.** When applications are hosted outside of the corporate network, associated traffic must first be backhauled through the company's data center before getting to the end user. Depending on where the user is physically located in relation to the data center, this can add latency.
- **Complexity of multi-cloud access.** VPNs are poorly suited in a world where 76% of companies have adopted a multi-cloud approach.[3] For DevOps professionals, using a VPN in a multi-cloud environment is a choice between navigating the complexities of multiple VPN concentrators, or manually connecting multiple VPN clients and destinations, a time-consuming and costly approach.
- **Complexity of access management.** Although VPNs can block access to certain sites and applications, the process requires the security team to use outdated and time-consuming network routing tables.

THE LIMITATIONS OF ZTNA

Built with zero trust principles, zero trust network access (ZTNA) emerges as a modern alternative to remote access VPN. Using a cloud-hosted broker between users and enterprise resources, cloud-delivered ZTNA services authenticate and validate a user's authorization before connectivity. The user and application traffic meets in the middle, creating a secure connectivity that is an isolated user-to-application segment.

Cloud-delivered ZTNA has many benefits: scalability of the cloud service, simplified network connectivity, and most importantly, performance and enhanced security thanks to direct, logical connectivity and zero trust principles. It is not a surprise that two-thirds of enterprises view ZTNA as key to mitigating "work-from-anywhere" risks.[4]

As with any technology upgrade project, enterprises upgrading their remote connectivity to ZTNA often have it co-exist with legacy VPN during the transition. However, many have learned that legacy applications can have a very long tail. As a result, many enterprise IT operations teams realize that they are now maintaining two connectivity solutions for much longer than originally planned—without a clear timeline for eliminating legacy VPN.

[3] "Why 76% of companies are adopting multicloud and hybrid cloud approaches," Oracle

[4] "2 Out of 3 Companies See Zero Trust Network Access as Key to Mitigate Work-From-Anywhere Risks, According to New EMA Report," Dark Reading, 12 October, 2022

This is because most cloud-delivered ZTNA architectures use an "inside-out connectivity." An application gateway fronts private applications and the application makes an outbound-only connection to the ZTNA broker. This architecture shields private resources from discovery on the public internet.

Modern ZTNA is inherently more secure than legacy VPNs because a ZTNA system delivers specific application access and not network access. And it only connects authorized users AFTER they have been authenticated and proper device posture checked. Modern ZTNA, while reducing the digital attack surface and minimizing unauthorized lateral movement, also posts challenges and compatibility issues with how legacy applications were designed.

With the "inside-out" connectivity, cloud-delivered ZTNA only permits client-initiated application traffic, thus challenging for applications that require server-initiated traffic flow, such as on-premises hosted Voice over Internet Protocol (VoIP) applications. With legacy applications, the approach comes up against two key challenges:

1. **Traffic direction is client-initiated.** Cloud-delivered ZTNA requires client-initiated application traffic and does not permit server-initiated traffic, which means it cannot serve legacy applications such as VoIP and peer-to-peer connectivity.

2. **Endpoint IP addresses are masked.** This means that ZTNA does not work for applications that require direct access to the endpoint using its public IP address, such as legacy forensic tools.

As a result, many organizations are using ZTNA and VPNs in tandem until they can upgrade their application infrastructure. In effect, this has meant that organizations' legacy applications cannot be free of the security risks and performance challenges associated with VPNs.

COMPLETING THE VPN REPLACEMENT JOURNEY

Finally, enterprises have a new option to accelerate the journey to zero trust access and enable secure remote working, one that will allow them to complete the migration away from outdated and insecure VPN technologies.

ZTNA NEXT - Unifying ZTNA and SD-WAN technologies

Delivered as a single solution, ZTNA Next integrates ZTNA/SD-WAN architecture, enabling the complete retirement—not just partial replacement—of remote access VPNs for all relevant application access use cases, while enhancing security posture and boosting remote worker productivity with seamless and optimized application access.

The unified Netskope SASE client sits in front of a converged architecture comprising ZTNA for access to private and cloud-based applications, and software-defined wide-area networking (SD-WAN) capabilities to securely connect applications that require bi-directional, server-to-client traffic.

In this model, the virtual client automatically routes application data to the appropriate infrastructure based on whether it is a modern (private access) or legacy/bi-directional (SD-WAN) application as defined by the company's application policies.

REMOTE WORKING USE CASES SOLVED			
USE CASE	**VPN**	**ZTNA**	**ZTNA NEXT**
Online traffic encrypted and secured	☑	☑	☑
Zero trust access to private applications	☒	☑	☑
Direct access to public clouds	☒	☑	☑
Simplified IT ops	☒	☑	☑
Stops lateral movement	☒	☑	☑
Streamlined DevOps access	☒	☑	☑
Inside-out connectivity	☒	☑	☑
Visibility of users, apps, and devices	☒	☑	☑
Supports bi-directional apps (e.g., VoIP, peer-to-peer, UCaaS, remote assistance tools)	☑	☒	☑
Supports direct access to endpoint (i.e., endpoint IP addresses are not masked)	☑	☒	☑
Intelligent, automated traffic routing	☒	☒	☑

THE BENEFITS OF SASE-GRADE REMOTE WORKING

Now, with the availability of a single client for unified ZTNA and SD-WAN, the full potential of a SASE-based approach to remote working can be realized. The solution unlocks a range of benefits for organizations including:

- **Accelerated ZTNA adoption** by enabling organizations to identify their bi-directional apps and create a transformation roadmap
- **Improved security** by replacing VPNs with end-to-end encryption across an organization's networks
- **Reduced complexity** for legacy apps in multi-cloud environments, as SD-WAN enables more flexible traffic routing compared to VPNs
- **Improved user experience** with routing to ZTNA/SD-WAN taking place behind the scenes, providing users with seamless and immediate access to their applications
- **Reduced costs**, as with no VPN holes into the corporate firewall there's less of a need for multiple expensive security appliances
- **Enhanced performance** for video and voice traffic, which can be routed via the SD-WAN for reduced latency

KEY CAPABILITIES TO LOOK OUT FOR

When deploying a new technology architecture, it's important to find solutions that perform as required and can deliver the full range of capabilities. When deploying a converged ZTNA/SD-WAN remote working capability, look for a solution that:

- Reduces overall cost and complexity, preventing technology sprawl and successfully consolidating separate products into a modern solution using a single agent—no hardware required
- Addresses legacy application compatibility issues with ZTNA
- Extends the longevity of legacy applications such as on-premises VoIP by optimizing performance
- Unlocks AI-driven operations with automated troubleshooting and insights into traffic flows, policy violations, and anomaly detection
- Connects users anywhere, using any device, to corporate resources everywhere, continuously evaluating context and adapting in real time to protect data

Organizations looking to finally move once past the era of VPNs can get started right away with two key foundational steps:

1. **Audit your private applications.** Perform an application discovery process to uncover whether your enterprise applications are ready for ZTNA, or whether they require the broader access capabilities of SD-WAN.

2. **Firm up your upgrade path.** Are you simply looking to replace your VPN, or are you specifically planning to replace your VPN with ZTNA? There are different approaches depending on your drivers.

SUMMARY

Remote working is here to stay, and organizations of all sizes need to find a secure and high-performance mechanism to connect users to the resources they need regardless of location. Soon, enterprises will be able to embrace ZTNA across all their applications, but while legacy applications are still in use, there is a requirement to combine ZTNA with broader access technology. A single solution integrating Netskope Private Access with SD-WAN is the most secure, optimized, and efficient approach yet.

FOR MORE INFORMATION

Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply Zero Trust principles to protect data. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and secures people, devices, and data anywhere they go. To learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com

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