5

— STEPS FOR SUCCESSFUL —

VPN TO ZTNA MIGRATION

Organizations realize it's time to augment or replace their virtual private networks (VPNs). This decades-old technology isn't designed to handle the security challenges of today's globally distributed workforce and escalating threat landscape. Zero Trust Network Access (ZTNA) is the modern industry standard for secure access to anything from anywhere by anyone. While many enterprises understand the value, the reality of migrating away from VPN technology may seem daunting. This eBook provides guidance on the five steps organizations can take to successfully transition from VPN to ZTNA, including best practices that minimize business disruption.

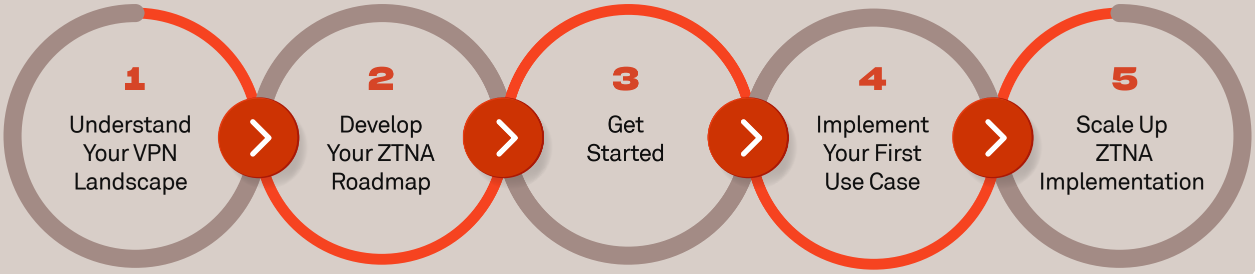

1
Understand Your VPN Landscape
2
Develop Your ZTNA Roadmap
3
Get Started
4
Implement Your First Use Case
5
Scale Up ZTNA Implementation

TABLE OF CONTENTS

Introduction

IT and security teams realize it’s time to enhance remote access strategies by augmenting or replacing their VPN. This shift in thinking arises from the need to address a significant increase in remote workers, accelerated digital transformation initiatives and an advanced threat landscape. VPNs are increasingly deficient and unwieldy for today’s IT ecosystems, resulting in increased risk and complexity. ZTNA is an optimal solution to combat these inherent VPN flaws. However, moving away from VPN can seem daunting, as large investments over the years have deeply ingrained them into the security stack.

This eBook explains how you can smoothly migrate from VPN to ZTNA with a five-step incremental approach that doesn’t disrupt business operations, reduces risk and sets you up for long-term success:

1. Understand your VPN landscape

2. Develop your ZTNA roadmap

3. Get started

4. Implement your first use case

5. Scale up ZTNA implementation

> ***A phased ZTNA approach strengthens and simplifies access controls without disrupting business operations.***

VPN Limitations:
Unfit for Modern Security Challenges

Introduced in the mid-1990s as a remote access solution, VPN architecture is past its prime. Several U.S. government agencies, including the National Security Agency (NSA), have issued warnings about VPN vulnerabilities. They were never designed to be used with hybrid IT infrastructure and a globally dispersed workforce.

INHERENTLY INSECURE

One of the most serious VPN security issues centers around open ports. Without exception, every VPN concentrator is deployed in such a way that it has a presence on the internet with an open, continuously listening port. Malicious actors scan for and enter networks via these open ports, inevitably moving laterally to reach and exploit targets.

The TCP/IP authentication method used by VPNs is another area of weakness. Most VPNs base "trusted" access on the user's IP address. A valid set of login credentials is easy to attain/acquire via social engineering, phishing, smishing, fake websites ... the list goes on. Even two-factor authentication verification codes are easily captured. There are millions of stolen login credentials on the dark web for sale to the highest bidder. Time after time, this legacy approach to authentication is easily manipulated by threat actors and is an absolute miscue given the raw amount of contextual data available to validate user identity.

COMPLEXITY ISSUES

VPN administrators are forced to make an important choice: either create open policies for broad network access or create restrictive policies for limited network access. This is inherently problematic because the easier choice for most is broad network access vs. restrictive policies that are complex, error-prone and hard to manage given the speed of change the business requires (e.g., agility and digital transformation).

All of these issues are further exacerbated by increased distributed workforces and the dynamic IP creation inherent with cloud workloads. It's just entirely too much to manage efficiently and maintain a strong security posture.

Furthermore, VPNs are hardware-bound, siloed solutions that only solve for remote access. This makes it cumbersome and costly to scale while inhibiting the ability to automate processes and integrate with other solutions. At the end of the day, VPNs are a remote access-only solution. They were designed to do one thing and they can't do it securely. These technical limitations and design flaws are just a tiny sampling of why you should strongly consider a VPN to ZTNA migration.

VPNs are hardware-bound and static, while software-defined ZTNA solutions provide the flexibility and scalability demanded by today's businesses.

10 REASONS IT'S TIME TO KICK YOUR VPN TO THE CURB

1. The VPN IP-centric authentication model is weak and lacks identity or contextual awareness.
2. VPNs "trust, then verify" approach results in easily found network entry.
3. VPNs encourage lateral movement within a flat network, increasing the "blast radius" of an attack.
4. VPNs lack the ability to conduct device posture checking as criteria for verifying trust.
5. VPN concentrators create choke points, resulting in poor performance and frustrated workers.
6. VPNs create policy and firewall management complexity.
7. VPNs lack interoperability with IT, security and business systems.
8. VPNs are expensive and time-intensive to scale.
9. Users must switch between VPNs to access distributed and heterogeneous workloads.
10. VPNs offer only active-active or active-passive setups for redundancy, which significantly limits throughput and scalability.

> **"VPNs are antiquated, and while they may have some value for an immediate 'fix,' they need to go away.**
>
> **They are vulnerability aggregators and are a prime target for exploitation."**
>
> **Dr. Chase Cunningham, Dr. Zero Trust**

ZTNA vs. VPN

ZTNA enforces the “principle of least privilege” access to the network that is a leading industry mandate. ZTNA is architected for the realities of today’s IT versus those of the 1990s. It offers significant benefits over VPNs. It’s like comparing the steam engine to a combustion engine. One served its time, while the other reigned supreme because it was more adeptly designed for the times.

These are the key differences ZTNA has to offer over the VPN:

- **Attack surface reduction:**
  While VPN open ports are easily found and exploited, ZTNA architecture uses single packet authorization (SPA) technology to render resources 100% invisible unless authenticated or deemed a trusted identity.

- **Identity-centric authentication:**
  ZTNA uses IP addresses as criteria for authenticating but goes much further in verifying identity. It does this by combining information from any identity store and layering on contextual variables such as time, date, location and device security posture.

- **Least privilege access:**
  Users and machines are only granted trusted, but limited access to the resources necessary to do their jobs. And with SPA technology and fine-grained microsegmentation, threat actors or infected devices are unable to move laterally across the network.

- **Programmable APIs:**
  Unlike the siloed nature of the VPN, ZTNA solutions integrate across business, IT and security systems for heightened network visibility and automation capabilities. The software-defined nature of ZTNA solutions ensures seamless and simultaneous scaling with dynamic infrastructures.

ZTNA and SDP

The ZTNA model was originally known as the software-defined perimeter (SDP). The names are used interchangeably and refer to an updated and more robust network access security posture.

WANT TO LEARN MORE?

Read *Zero Trust Network Access: Everything You Need to Know*

DOWNLOAD NOW

VPN LIMITATIONS VS. ZTNA ADVANTAGES

VPN	ZTNA
Network-centric: "Trust, then verify" model based on a simple IP-to-port relationship.	**Identity-centric:** "Verify, then trust" model based on identity, context and multidimensional profiles.
Open ports: Typically wide-open user access to the authenticated network, enabling uncontrolled lateral movement.	**Cloaked infrastructure:** Authorized users access approved resources only, making everything else invisible to prevent lateral movement.
Hardware-bound: Cumbersome to deploy; static and unscalable as infrastructure changes.	**Software-defined:** Elastic and scalable across all hybrid environments via API integrations.
VPN switching: User access to multiple resources usually requires switching from one VPN to another built on complex, error-prone policies.	**Concurrent connections:** Allows users to access multiple network segments and digital resources via a single connection point.
Siloed and static: Only applicable for remote user access; unable to secure on-premises users or networks.	**Flexible and dynamic:** Versatile and extensible, going beyond remote users to deliver unified, secure access for all.

These are just a few of the reasons you should take an incremental approach to ZTNA implementation. Teams can prove value and ensure success while working strategically with the organization to handle objections, change perspectives and improve policies and procedures along the way.

Overcoming Objections to ZTNA Migration

The desire to protect existing investments and decisions is often a driving force behind why organizations don't move forward with a ZTNA migration plan. The reality is you don't have to boil the ocean all at once. You can augment your aging security technology and make a phased migration plan that delivers improvement over time.

SUNKEN COSTS

VPNs are embedded in tech stacks worldwide, so resistance to change is common. For many, the biggest objection is simply that the investment has already been made in the current technology. Typically, VPNs represent a lot of sunk costs, and your IT/security departments are likely anxious about large-scale "rip and replace" discussions. In fact, in a recent survey we conducted among more than 500 infosec professionals, the number one factor driving decision making was the desire to feel secure about previous technology investments. At the same time, they ranked a technology that creates fast, secure connections between users and applications as most important among purchasing criteria. Unfortunately, VPNs fall short in that area.

We recommend an incremental VPN to ZTNA migration strategy that solves for both of these factors. To start, divert budget earmarked for new secure access initiatives away from VPNs—or other aging technology—to a ZTNA solution. Another avenue is to replace VPNs that are in need of expensive hardware refreshing.

THE KNOWN VS. THE UNKNOWN

VPNs are a known quantity, and end users are accustomed to working with and around them. Retraining staff and fielding service desk calls may be initial objections to adopting ZTNA, but these are short-lived when stacked against benefits that include reduced complexity, improved user experience and performance gains. Born out of a Zero Trust security philosophy, there is a clear argument for the operational benefits achieved via ZTNA solutions.

SOLUTION OVERLOAD

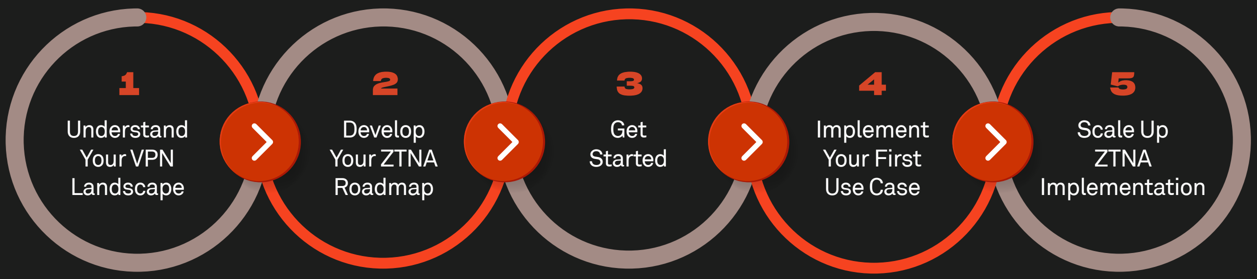
There is the natural objection that tech stack additions could create overtooling vs. consolidation. But, ZTNA actually reduces dependency on VPN, NAC and firewall solutions without a "rip and replace." This is due to the extensibility of a single, private access platform and centralized policy engine overlay that solve the secure access limitations of these legacy tools. So, you can cut the number of firewall rules to manage; end new VPN solution investments and ease VPN concentrator choke points; and eliminate future complex and expensive NAC installments. These operational benefits mean your overburdened security and IT team can focus on needle-moving business initiatives vs. mundane policy management tasks inherent with legacy network security tools.

STATUS QUO VS. CHANGE

Other possible objections include a lack of awareness about cyber risks associated with VPNs and the fear of disrupting business with a new technology implementation. You can counter these by Googling "VPN CVE" to find the latest headlines related to critical VPN vulnerabilities and by surveying your IT team or employees at large regarding help desk tickets and policy management woes related to VPN management. The disruption is already there and must be eradicated to achieve greater efficiencies and a more hardened, highly flexible security posture.

VPN to ZTNA Migration Steps

Getting started can be the most challenging part of a journey to Zero Trust. But if you start small, think big and scale as you go, the process becomes more manageable. Begin by understanding your current VPN landscape, then evaluate it against organizational objectives and areas of severe risk. As the roadmap emerges, teams can identify and prioritize use cases. From there, a phased plan can follow as fast and/or as methodically as your organization desires.



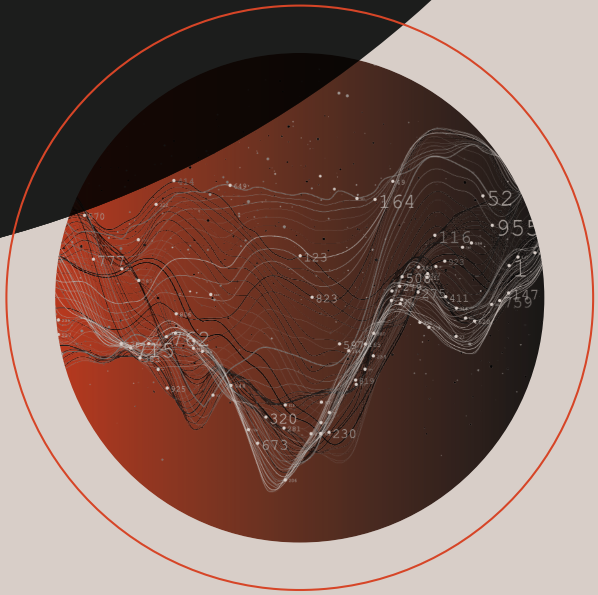
1 Understand Your VPN Landscape

2 Develop Your ZTNA Roadmap

3 Get Started

4 Implement Your First Use Case

5 Scale Up ZTNA Implementation



1 UNDERSTAND YOUR VPN LANDSCAPE

Each organization has its own unique VPN setup and deployment. Before you think about ZTNA migration, you must have a clear sense of your existing VPN landscape. If a map of your VPN framework doesn't exist, now is an excellent time to create one to show where VPNs are used ... by application, network segment and user group.

A VPN baseline assessment should detail how your VPNs are integrated into your tech stack. It defines what and how digital assets need to be secured and considers technological, organizational and financial requirements.

In parallel, it's wise to determine which user groups have access to the most sensitive data or pose the most risk to your organization if compromised. This helps identify trouble spots and how to deal with them before they become larger problems. For example, rather than rolling out a full ZTNA implementation for all remote workers at once, it may be smarter to pilot ZTNA with a smaller user group that poses a high security risk. After achieving a win and reducing your risk posture within that group, you can scale to the broader user population.

Your VPN baseline provides a complete picture of how VPNs work within your organization while also considering all technical, organizational and financial influences.

2 DEVELOP YOUR ZTNA ROADMAP

The next step is to determine your ultimate destination and develop the ZTNA roadmap to get there. It's critical to consider your organization's desired Zero Trust security end state, including your long-term strategy. Remember, ZTNA is far more extensible than VPN – and is just a natural starting point. Your roadmap can extend beyond simply solving for remote access and encompass the broader network access landscape. Ultimately, you can deliver secure access for all users, all devices and all workloads regardless of where they reside.

ZTNA supports many other use cases beyond remote access, so prioritization is entirely dependent on the objectives, risks and desired security posture of your organization.

OTHER COMMON ZTNA USE CASES:

- **Cloud migration:**
  Moving applications and data to the cloud—or multiple clouds—effectively turns all users into remote users but with some stark differences. ZTNA automatically scales with the dynamic resolution of IPs associated with cloud workloads, resulting in dynamic entitlements across multicloud environments without manual intervention.

- **Secure DevOps access:**
  DevOps teams require remote access to sensitive digital assets hosted in multicloud environments and on-premises, which can cause friction and risk within the limited capabilities of VPN. ZTNA can unleash DevOps from those limitations by providing concurrent access to multiple cloud environments accompanied by the bandwidth and performance developers need to do their job. This also provides a prime opportunity for exploring automation capabilities using metadata and integration capabilities (e.g., with IT service management).

- **Third-party access:**
  Third parties, such as vendors, contractors and business partners, can easily expose your business to risks associated with overprivileged access. Third parties are invariably remote in nature, so many organizations rely on VPNs to manage their access. ZTNA can grant trusted access to third-party users without risking exposure to unauthorized resources.

- **Machine-to-machine (M2M):**
  More robust ZTNA solutions can apply the same Zero Trust principles enforced for users to M2M connections. This is just another way ZTNA reduces the attack surface, because it thwarts lateral movement if a machine is compromised.

- **Café-style networking:**
  This is the end game or goal of ZTNA ... an amalgamation of all use cases resulting in a single unified policy model across all users, networks, workloads and devices. It essentially removes the need for varying access models when working remotely or in an office regardless of connecting to the cloud or on-premises workloads.

Using rich APIs, ZTNA can integrate and automate with existing IT, security and business systems, making it an ideal solution for all of your network access use cases. These capabilities should be accounted for in the roadmap, as automation and operational efficiencies likely will become strategic business demands.

3 GET STARTED

Now there's just the detail of selecting a ZTNA provider so you can tackle your first ZTNA use case. You should consider various architectures and features that will meet current and future requirements to avoid a mid-roadmap provider switch or a second ZTNA solution addition to a crowded tech stack.

Key ZTNA vendor selection factors include:

- Ability to handle all protocols, not just web applications
- Latency, compliance and security dependencies for multi-tenant cloud environments
- Capable of working in heterogeneous environments
- Flexibility in choosing deployment options, such as as-a-service or self-hosted ZTNA
- Ability to protect east-west and north-south network traffic
- Integration capabilities for future automation
- Capable of handling multiple and varying identity stores
- Ability to provide a unified policy model that includes IoT and secure branch office

Once you select your ideal ZTNA solution, now it's time to implement:

- **Infrastructure selection – choose between:**
  - Self-hosted ZTNA solutions that require light deployment for gateways and controller (unified policy engine); or
  - "As-a-service" ZTNA solutions that can be quickly deployed and reduce the need for full IT support by relying on the provider's cloud hosting
- **Policy creation:**
  - Your identity store must be unified for user groups due to ZTNA's identity-centric approach for policy creation. So, your ZTNA provider has to support multiple disparate identity providers. Then you can set a few simple policies that can include risk-based context such as time, date, location, MFA, etc.
- **User onboarding:**
  - Your first use case and user group will determine if you need a client installed for device posture checking and protocol support or browser-based access for web applications. A ZTNA solution that can handle both is ideal so you have a choice for future use cases
- **Automation:**
  - Decide where automation will reduce complexity, improve agility and ease admin tasks, which may include automating integration with an ITSM, MFA or business support system

It's also important to plan to measure success. Consider tracking user satisfaction and adoption rates, reduced help desk calls or other points to validate how ZTNA supports business goals. Additional metrics might include user and IT admin productivity gains, open port and firewall rule reduction or time-to-install comparison of ZTNA vs. VPN. Measuring and reporting first use case results to key stakeholders will clear the runway for the final step.

4 IMPLEMENT YOUR FIRST USE CASE

Start by taking a bite-sized chunk out of your most natural first use case, which, as discussed, is migration from VPN to ZTNA. While there is not a “right” or predefined launch point, here are points to consider for upgrading to secure remote access with ZTNA:

- **Risk mitigation:**
  A natural question is “Where does the most risk associated with VPN access reside?” This could be a subset of privileged users who touch sensitive resources on a regular basis. The business case here is about preventative measures and how to avoid the costly nature of a breach, which averages $1.52 million per incident, according to Ponemon’s *2020 Cost of a Data Breach Report.*

- **Productivity gains:**
  Another logical place to start is understanding where you can gain operational efficiencies. This could be a large subset of frustrated users experiencing VPN drawbacks, such as choke points and performance issues, resulting in increased help desk tickets and administrative burdens. And then there are your developers and DevOps, who require the right access to hybrid resources at the right time to deliver on fast-paced application delivery.

- **Budget cycle:**
  This is an excellent time to begin your VPN to ZTNA migration. A major VPN hardware refresh planned for a budget cycle presents an opening for a “replacement vs. upgrade” secure access dialogue. VPN software renewals and maintenance expirations provide similar compelling opportunities for review.

- **New initiatives:**
  New digital transformation initiatives or cloud migration projects also are a prime opportunity to adopt ZTNA. Partnering with business units to accelerate these initiatives—without sacrificing, but rather strengthening, security—positions ZTNA as a catalyst for digital transformation.

5 SCALE UP ZTNA IMPLEMENTATION

After the initial use case has proven out, you can scale up ZTNA implementations across the larger enterprise. Because the solution is software-defined, it's easy to follow your roadmap across all users and all workloads. Simply add more gateways, define new policies and get more users on board.

Ideally, the scale-up process will move horizontally and vertically. Horizontal scaling adds more users. Vertical scaling covers new use cases and adds integration and automation. How this is done and how quickly it is completed will depend on your roadmap. ZTNA solutions can move as fast or as slowly as you require.

Scale up might encompass use cases like DevOps, cloud migration, server-to-server (i.e., east-west traffic), IoT devices or a full-bore café-style network. Successful scaling depends on keeping the policy engine unified and centralized. ZTNA solutions that offer flexible deployment and access options allow you to maintain a unified approach, making slight architectural adjustments to achieve all use cases. For example, third-party vendors may not allow a client install at their endpoint. However, a full-feature ZTNA solution will enable least privilege access from third-party browsers without requiring a new solution or policy management GUI.

Finally, as your deployment matures, you can unlock more features of your solution. This might include:

- **Automate policies:** Leverage data from identity and directory systems and environmental metadata to dynamically create or extend policies and entitlements
- **Automate infrastructure:** Control, build and manage infrastructure-as-code with terraform the GitHub SDP operator
- **Orchestrate workflows:** Integrate with existing enterprise operation or business support systems, such as IT service management or ticketing platforms
- **Enhance posture checking:** Integrate with endpoint solutions to ensure a "trusted device" or user behavior analytics to ensure "trusted user" as risk criteria for access
- **Put data to work:** Push detailed access log activity to other tools and pull intelligence as access criteria from other tools, such as TIPs, SIEMs and UEBAs

Simplify Migration with Appgate's ZTNA Solution

Appgate has helped hundreds of customers make the switch from VPN to ZTNA. We're known for our industry-leading expertise in seamlessly transitioning companies to Appgate SDP, a best-in-class solution that has passed the VPN to ZTNA migration test many times.

Appgate SDP delivers a complete range of ZTNA security capabilities for all users, devices and hybrid workloads:

- **Reduced attack surface** by rendering ports, workloads and applications invisible unless the user is authorized to access them
- **Conditional access permissions** to verify user identity based on context-specific indicators like date, role, location, device posture, etc.
- **Advanced microsegmentation** that limits authorization to protected networks or workloads and is defined by dynamic entitlements that adjust as user and device context changes
- **Improved policy management** by reducing complexity with a single framework for all users, devices, networks and infrastructure for a unified access experience with consistent configuration across heterogeneous IT
- **Concurrent connections** that enhance user experience and support simultaneous direct access to all approved cloud, SaaS and on-premises resources

"Appgate's Zero Trust architecture enabled all of our employees to work remotely from the safety of their homes while maintaining the highest level of security required by our clients."

– Chris Edwards, Founder and CEO, The Third Floor

"Appgate's SDP simplifies a lot of things for us … We were able to trim our firewall policies from about 50 policies to now two or three."

– Deryk Motietall, Sr. Manager of Infrastructure, WW

"As a managed service provider, our customers trust us to secure their data. We are always looking to improve our security posture. Appgate SDP helped us achieve this goal."

– Matthew Staver, CTO, Verdant Services

Make the Move to ZTNA

Now is the time to replace or augment your legacy VPN with the modern security supremacy of ZTNA. The increasingly sophisticated cyberthreat landscape—combined with work-from-anywhere business models—makes it an imperative.

Start small but think big in terms of long-term security goals. By starting with a manageable ZTNA use case, your IT and security team can leverage its knowledge and expertise for incremental enterprise-wide implementation. This ensures stakeholder support, better user adoption and minimal business interruption.

Stop relying on outdated technology to protect and enable today's digital business.

Make the move to ZTNA and begin your journey toward Zero Trust security.

READY TO SEE ZTNA IN ACTION?

GET A DEMO

About Appgate

Appgate SDP is a leading Zero Trust Network Access solution that simplifies and strengthens access controls for all users, devices and workloads. We deliver secure access for complex and hybrid enterprises by thwarting complex threats, reducing costs and boosting operational efficiency.

The full suite of Appgate solutions and services protects more than 650 organizations across government, Fortune 50 and global enterprises. Start your secure access journey with confidence by contacting Persimmon Connections.