SOPHOS
Cybersecurity evolved.

Top Six Advantages of ZTNA

Compared to remote access VPN

A Sophos Whitepaper. October 2021

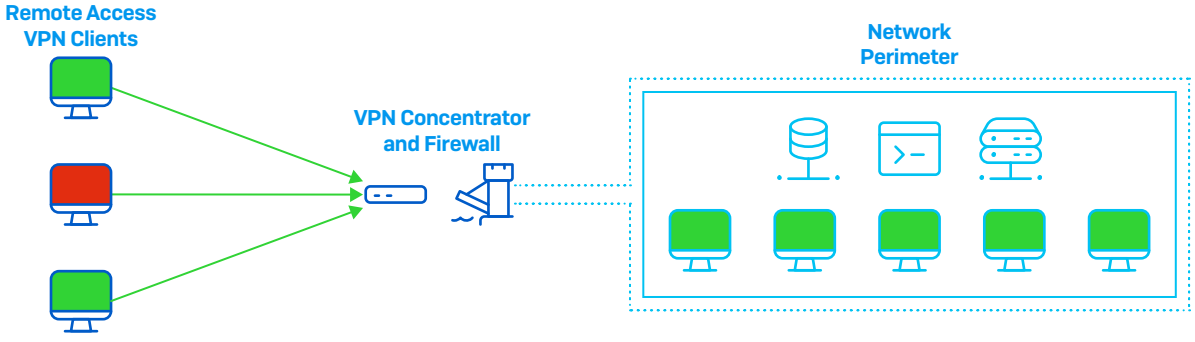
Remote access VPN has long served us well, but the recent increase in remote working has cast a spotlight on the limitations of this aging technology. While some organizations continue to extract every bit of mileage they can from VPN, many are looking for a better alternative – something that addresses the challenges with remote access VPN. Several organizations have already started to fully embrace the next-generation of remote access technology: ZTNA or zero trust network access. ZTNA offers better security, more granular control, increased visibility, and a transparent user experience compared to traditional remote access VPN.

In this ZTNA buyers guide we will examine the limitations and challenges with traditional remote access VPN and the benefits that zero trust network acccess can provide and summarize with a shopping list of critical capabilities you should be looking for in your new ZTNA solution.

Challenges with remote access VPN

Remote access VPN has been a staple of most networks for decades, providing a secure method to remotely access systems and resources on the network. However, it was developed during an era when the corporate network resembled a medieval fortification – the proverbial castle wall and moat that formed a secure perimeter around network resources within. VPN provided the equivalent of a secure gatehouse for authorized users to enter the safe perimeter, but once they were in, they had full access to everything within the perimeter.

Traditional Remote Access VPN



Of course, networks have evolved substantially, being more distributed than ever. Applications and data now live in the cloud, users are working remotely, and networks are under siege by attackers and hackers looking for any weakness to exploit.

Administering a remote access solution based on traditional VPN (IPSec/SSL) in any kind of modern environment can be extremely painful. You have to contend with IP management, traffic flows and routing, firewall access rules, as well as client and certificate deployment and configuration. Anything beyond a handful of nodes and a few dozen users turns this into an unnecessary full-time job - just to keep this running. If that wasn't enough, security becomes an absolute nightmare to monitor and control.

In summary, traditional remote-access VPN has a number of unnecessary limitations and challenges:

1. **Implicit Trust** – Remote access VPN does a good job of getting you through the perimeter and onto the corporate network as if you were physically there, but at that point, you're implicitly trusted and given broad access to the resources on that network which may present unnecessary and enormous security risks.
2. **Potential Threat Vector** – Remote access VPN has no awareness of the state of the device used to connect to the corporate network, creating a potential conduit for threats to enter the network from devices that may have been compromised.
3. **Inefficient Backhauling** – Remote access VPN provides a single point-of-presence on the network, which will potentially necessitate backhauling of traffic from multiple locations, datacenters, or applications through the remote access VPN tunnel.
4. **Lack of Visibility** – Remote access VPN is unaware of the traffic and usage patterns it is facilitating making visibility into user activity and application usage more challenging.
5. **User Experience** – Remote access VPN clients are notorious for offering a poor user experience, adding latency or negatively impacting performance, suffering from connectivity issues, and generally being a burden on the helpdesk.
6. **Administration, Deployment and Enrollment** – Remote access VPN clients are difficult to setup, deploy, enroll new users, decommision departing users. VPN is also challenging to administor on the firewall or gateway side, especially with multiple nodes, firewall access rules, IP management and traffic flows and routing. It quickly becomes a full time job.

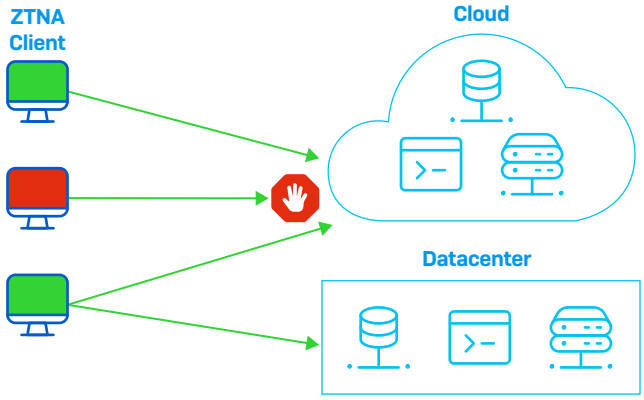
What is ZTNA and how it works

ZTNA or zero trust network access has been designed from the start to address the challenges and limitations with remote access VPN, offering a better solution for users anywhere, to connect securely to the applications and data they need to do their jobs, but nothing more. There are a few fundamental differences that set ZTNA apart from remote access VPN.

As the name implies, ZTNA is founded on the principles of zero trust – or trust nothing, verify everything. Zero trust essentially eliminates the concept of the old castle wall and moat perimeter in favor of making every user, every device, and every networked application their own perimeter and only interconnecting them after validating credentials, verifying device health, and checking access policy. This dramatically improves security, segmentation, and control.

Another key difference in how ZTNA works is that users are not just dropped on the network with complete freedom of movement. Instead, individual tunnels are established between the user and the specific gateway for the application they are authorized to access, and nothing more - providing a much more secure level of micro-segmentation. This has a number of benefits for security, control, visibility, efficiency and performance. For example, remote access VPN provides zero insights into which applications users are accessing, while ZTNA can provide real-time status and activity for all your applications proving invaluable in identifying potential issues and performing licensing audits. The added micro-segmentation that ZTNA provides ensures there's no lateral movement of device or user access between resources on the network. Each user, device, and application or resource is literally it's own secure perimeter and there's no longer any concept of implicit trust.

Zero Trust Network Access



ZTNA is also inherently more dynamic and transparent by nature, working in the background without requiring interaction from the user beyond the initial identity validation. This experience can be so smooth and frictionless that users won't even realize they are connecting to applications via secure encrypted tunnels.

Advantages of ZTNA

Zero Trust Network Access offers enormous benefits in many ways but is primarily being adopted for one or more of these reasons:

- **Working from home:** ZTNA solutions are a much easier solution for managing remote access for staff working from home. They make deployment and enrollment easier and more flexible, turning what may have been a full-time job with VPN into something much less resource intensive. It's also more transparent and simpler for your staff working remote.
- **Application Micro-Segmentation:** ZTNA solutions provide much better application security with micro-segmentation, the integration of device health into access policies, continuous authentication verification and just the elimination of implicit trust and the lateral movement that comes along with VPN.
- **Stopping Ransomware:** ZTNA solutions eliminate a common vector of attack for Ransomware and other network infiltration attacks. Since ZTNA users are no longer "on the network", threats that might otherwise get a foothold through VPN have no where to go with ZTNA.
- **On-board New Applications and Users Quickly:** ZTNA enables better security and more agility in quickly changing environments with users coming and going. Stand-up new applications quickly and securely, easily enroll or decommission users and devices, and get insights into application status and usage.

In summary, the advantages of ZTNA over traditional remote-access VPN solutions include:

1. **Zero Trust** – ZTNA is founded on the principle of zero trust or "trust nothing, verify everything." This provides significantly better security and micro-segmentation by effectively treating each user and device like their own perimeter and constantly assessing and verifying identity and health to obtain access to corporate applications and data. Users only have access to applications and data defined explicitly by their policies, reducing lateral movement and the risks that come with it.
2. **Device Health** – ZTNA integrates device compliance and health into access policies, giving you the option to exclude non-compliant, infected, or compromised systems from accessing corporate applications and data and eliminating an important threat vector and reducing risk of data theft or leakage.
3. **Works Anywhere** – ZTNA is network agnostic, able to function equally well and securely from any network be it home, hotel, café, or office. Connection management is secure and transparent regardless of where the user and device are located, making it a seamless experience no matter where the user is working.
4. **More Transparent** – ZTNA provides a frictionless, seamless end user experience by automatically establishes secure connections on demand behind the scenes as they are needed. Most users won't even be aware of the ZTNA solution that is helping protect their data.
5. **Better Visibility** – ZTNA can offer increased visibility into application activity that can be important for monitoring application status, capacity planning, and licensing management and auditing.
6. **Easier Administration** - ZTNA solutions are often much leaner, cleaner, and therefore easier to deploy and manage. They can also be more agile in quickly changing environments with users coming and going - making day-to-day administration a quick and painless task and not a full-time job.

Buyers guide: What to look for in a ZTNA solution

While looking at the obvious checklist of supported platforms for clients, gateways, and identity providers, be sure to consider these important capabilities when comparing ZTNA solutions from different vendors:

Cloud-delivered, cloud-managed

Cloud management offers tremendous benefits from being able to be up and running instantly, to reduced management infrastructure, to deployment and enrollment, and enable access anywhere. One of the key advantages of cloud management is being able to log in and begin instantly, without adding additional management servers or infrastructure. Cloud management also offers instant secure access from anywhere on any device, supporting the way you want to work. It also makes it easy to enroll new users wherever they happen to be in the world.

Integration with your other cybersecurity solutions

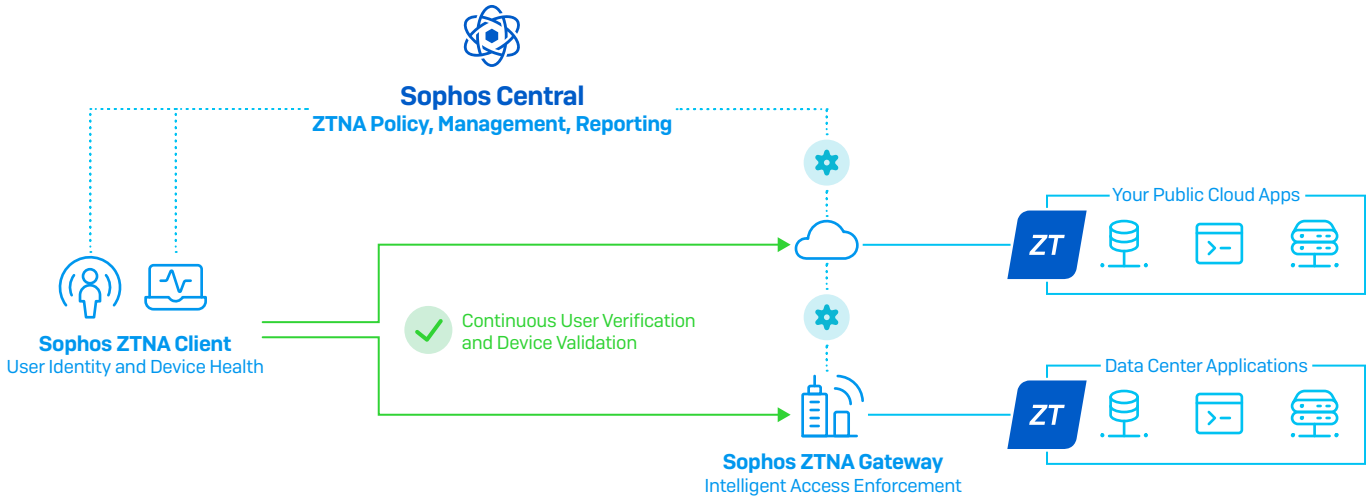
While most ZTNA solutions can work perfectly fine as standalone products, there are significant benefits from having a solution that is tightly integrated with your other cybersecurity products such as your firewall and endpoints. A common, integrated cloud management console can be a force multiplier for you or your team. Using a single pane of glass to manage all your IT security, including ZTNA in one place, can reduce training time and day-to-day management overhead. It can also provide unique insights across your various IT security products, especially if they share telemetry, dramatically bolstering security and offering a real-time response when a compromised device or threat gets on the network. They can work together to instantly respond to the presence of an attack or threat and stop it from moving laterally, spreading, or stealing data.

User and management experience

Ensure the solution you are cnsidering offers both an excellent end-user experience as well as makes administration and management easy. These days, with more users working remotely from all over the world, enrollment and efficient device setup is critical to get new users productive as quickly as possible. Be sure to pay attention to how the ZTNA agent is deployed and how easy it is to add new users to policies. Also ensure the solution you're investing in offers a smooth frictionless experience for end users and provides the visibility you would expect ,like real-time insight into application activity that will help you be proactive in identifying peak load, capacity, license usage, and even application issues.

Sophos ZTNA

Sophos ZTNA has been designed from the start to make zero trust network access easy, integrated, and secure. Sophos ZTNA is cloud-delivered and cloud-managed, integrated into Sophos Central, the world's most trusted cybersecurity cloud management and reporting platform. From Sophos Central, you can not only manage ZTNA, but also your Sophos Firewalls, endpoints, server protection, mobile devices, cloud security, email protection, and so much more.



Sophos ZTNA is also unique in that it integrates tightly with both Sophos Firewall and Sophos Intercept X endpoints. This allows for taking advantage of Synchronized Security and Security Heartbeat to share device health between the firewall, device, ZTNA, and Sophos Central to automatically respond to threats or non-compliant devices. Automatically limit access and contain compromised systems until they are cleaned up.

Sophos customers agree that the time saving benefits of a fully integrated Sophos cybersecurity solution are enormous. They say that using the Sophos suite of products together, managed from Sophos Central, and leveraging Synchronized Security for automatic threat identification and response is like doubling the size of their IT team. Of course, Sophos ZTNA will work with any other vendor's security products, but it is unique in working better together with the rest of the Sophos ecosystem to provide tangible real-world benefits to visibility, protection, and response.

Learn more at

sophos.com/ztna

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

21-10-07 EN (DD)

SOPHOS