HPE aruba networking

# Fully replace VPN with HPE Aruba Networking

## The modern workplace calls for a new approach to remote access

Created in April of 2019 by Gartner®, the term Zero Trust Network Access (ZTNA) represents a set of new technologies designed for secure access to private applications. Also referred to as Software-defined perimeter (SDP), ZTNA technologies use granular access policies to connect authorized users to specific applications, without the need for access to the corporate network, and establish least-privileged app-level segmentation as a replacement for network segmentation, without exposing the application location to the public internet.

### Accelerating to a modern workplace means saying goodbye to VPN

Spurred by the need to ensure business continuity during the pandemic and outpace competition, every organization is in a race to adopt the right digital solutions to keep their users happy, motivated, and productive. They've adopted new collaboration apps like Zoom and Microsoft Teams, doubled down on scalable public cloud services, implemented for more flexible work environments. With this modernization underway, many IT leaders are considering better ways of providing remote access to private applications for their employees and third parties and moving away from VPN.

Prior to the pandemic, a mere 30% of employees worked from home. Today, 77% of businesses plan to embrace hybrid work to retain top employees who now prefer to work from home and to access new, less expensive talent pools. However, VPNs tend to hinder productivity and frustrate employees.

Partners, suppliers, vendors, and customers also play a key role in driving revenue for the business. One out of every three users who require access to resources are third parties, and they rarely allow a VPN client to be deployed on their devices.

As you can imagine, this modern workplace also comes at a cost. IT spending is estimated to reach $2 trillion in 2022 — much of which will be to modernize IT infrastructure and support this new work environment. Yet, this only represents a 4% increase in average IT budgets — so continuing to spend heavily on legacy remote access technologies is not an option.

HPE GreenLake

Even in the midst of enabling work from anywhere, securing third-party access, and modernizing infrastructure, companies must protect their resources and reputation. With every user, device, and application connecting over the Internet, the potential attack surface increases exponentially — and placing users onto the corporate network via a VPN has become the biggest risk of all.

To support this new environment, 60% of businesses will replace their VPN with ZTNA by 2023.

## The difference between VPN and ZTNA

### Remote access VPN

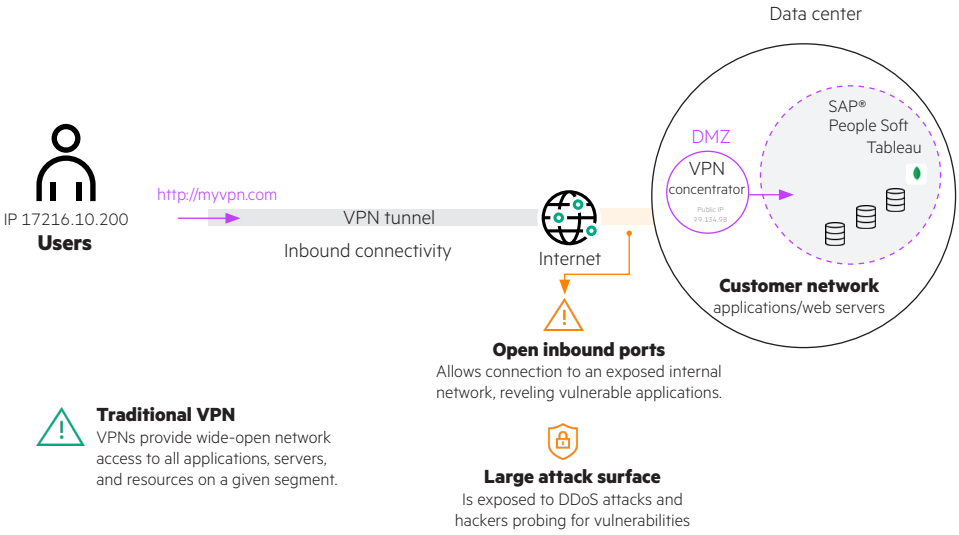


**Figure 1.** Traditional VPN

Over the past 20 years, VPN has allowed remote employees and third parties to access the network and the private resources running within it. VPN concentrators listen for inbound calls from VPN clients and serve as a beacon for the clients — providing an entry point into the corporate network. To minimize the risk of this flawed architecture, organizations require firewalls, load balancers, DDoS prevention, and VPN concentrators to connect remote users to private applications, leading to increased complexity, costs, and risk. Over the past few years, popular VPN services from well-known companies have been exploited due to this architecture.

**ZTNA**

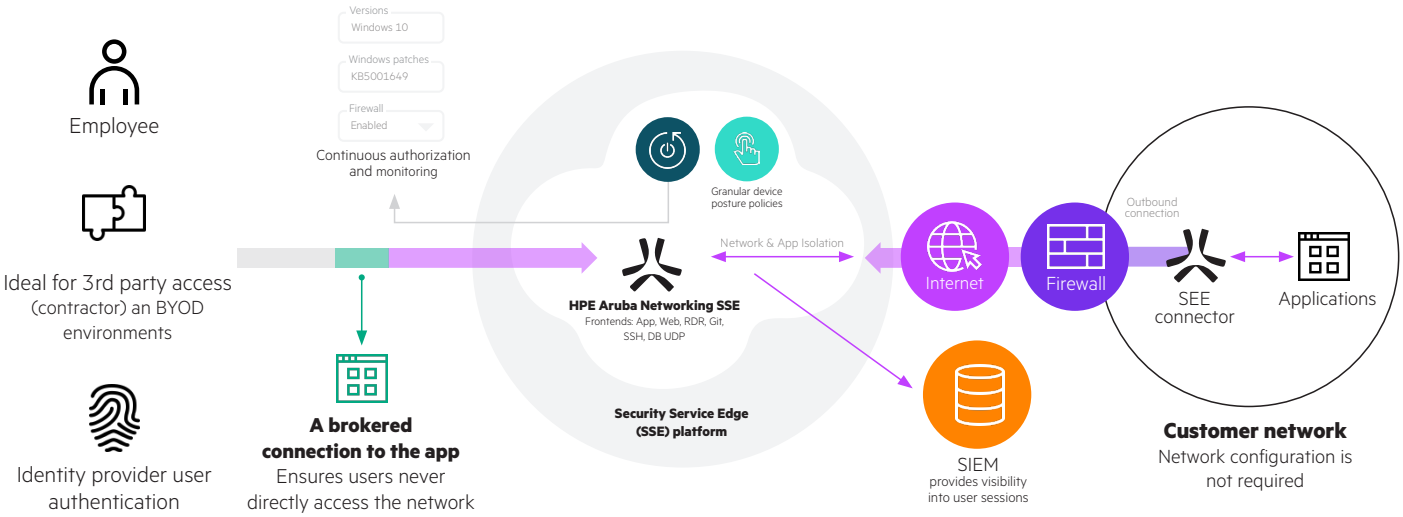


**Figure 2.** HPE Aruba Networking's ZTNA service within the SSE platform

With 500+ edge locations across the globe, the HPE Aruba Networking SSE platform is one of the most reliable, available, and scalable zero trust solutions designed for secure connectivity to business resources.

Our ZTNA service provides users with fast, secure, reliable access to private resources. Here's what's happening in real time when connecting through clientless functionality.

1. The user requests access to an internal application, such as: hr-app-tenant.axisapps.io
2. If the user is not actively logged into an HPE Aruba Networking-managed application, the user is redirected to the associated application identity provider.
3. Our ZTNA checks the user's access request against the customer's defined policies.
4. The user is continuously authorized according to their identity, group, and other contextual criteria. NOTE: The HPE Aruba Networking SSE platform can actively inspect traffic and closes the session if a security event occurs.
5. ZTNA checks for an existing connection to the application for potential reuse.
6. When a new connection occurs, the closest SSE connector identifies the authorized application and responds with an outbound connection to the HPE Aruba Networking SSE cloud via a specified port.
7. The HPE Aruba Networking SSE cloud returns the new connection to the dedicated front end.
8. The front-end web establishes a connection to the application.
9. Access to the requested internal application is then extended to the user via browser-based connectivity.

HPE Aruba Networking's ZTNA ensures that application access is granted without requiring access to the corporate network. This decoupling reduces network security risks — like insider threats or ransomware spreading — by minimizing lateral movement through application-level segmentation.

Unlike a VPN concentrator, our ZTNA service uses a service-initiated architecture to leverage what we call outbound-only connections. This connection type ensures that the network infrastructure and business applications are masked from the Internet and cannot be located or verified because they do not listen for any inbound pings. They sit behind the SSE connector, which exclusively speaks with the HPE Aruba Networking SSE platform. Think of the SSE platform as the intermediary between the entity (user or app) and the application.

HPE Aruba Networking treats the Internet as the new corporate network and ensures that dynamic Internet-based encrypted micro-tunnels replace traditional network connections like always-on VPN, MPLS, and dedicated site-to-site connections for public cloud. This reduces costs and frees up time for network and security teams to focus on more strategic projects instead of managing expensive appliances, updating versions, deploying hardware, and planning renewals.

**Table 1.**

| | VPN | vs. | ZTNA |
|---|---|---|---|
| **User experience**<br>Users expect accessing private applications to feel like accessing SaaS applications. | **Poor user experience**<br>VPNs force users to deploy a client on their device and reconnect to the corporate network every time they change location. Because VPN gateways have limited points or presence, suboptimal flows add latency, cutting into user productivity. | **vs.** | **Seamless user experience**<br>HPE Aruba Networking SSE offers both client and clientless access methods. A single Zero Trust policy follows the user and ensures they only have access to the specific resources they need. The always on user experience allows customers to simply work and not worry about reconnecting to a network. Cloud-delivered ZTNA services offer global PoPs that securely extend connectivity out to every user locations — via the Internet. |
| **Security**<br>The business must protect data from cyberattacks at all costs | **Increased risk**<br>Cyber criminals are actively targeting VPN and VDI technologies with internet-based attacks. These network-centric access methods place users onto the corporate network and expose infrastructure to the open Internet. With a simple port scan, an adversary can target infrastructure with an outdated posture, steal credentials, and access the corporate network as if they were a legitimate user. | **vs.** | **Zero attack surface**<br>HPE Aruba Networking SSE is designed to never inherently trust anything. Only after proper inspection, and validation, does the ZTNA service connect users to specific resources. These 1:1 connections are outbound-only from the resource to the authorized user — without placing users on the corporate network. This least-privilege access design ensures that users and threats cannot propagate laterally across the environment. HPE Aruba Networking also protects resources by placing them behind the ZTNA service — making them invisible to the Internet. Access rights then auto-adapt based on changes in context, such as relationship with company, device posture, location etc. |
| **Ease of use**<br>As the business grows, and continues cloud adoption, simplicity and scale become a priority. | **More complexity and costs**<br>Scaling VPN services requires adding capacity to the entire inbound gateway including purchasing, deploying, and managing more appliances. Often times, load balancers, external and internal firewalls, DDoS service, and other appliances are necessary. This increase in appliances is challenging to manage and increases costs the roof when you consider both CapEx and OpEx spend on maintaining the entire gateway. | **vs.** | **Simple to manage**<br>The cloud-delivered services require no appliances and are maintained by the vendor themselves. The services are designed for reliability, availability, scalability as traffic demands increase. They ensure the fastest experience possible without disruption to the business. API integrations with key ecosystem services like IDP, endpoint security, and SIEM, help expedite the deployment process. These services charge on a per user, per year basis, so capacity and appliance costs are no longer a factor. IT can spend less time and money on connectivity services and instead focus on the strategic projects that are key to their modern workplace initiatives. |

## Unique capabilities of our ZTNA

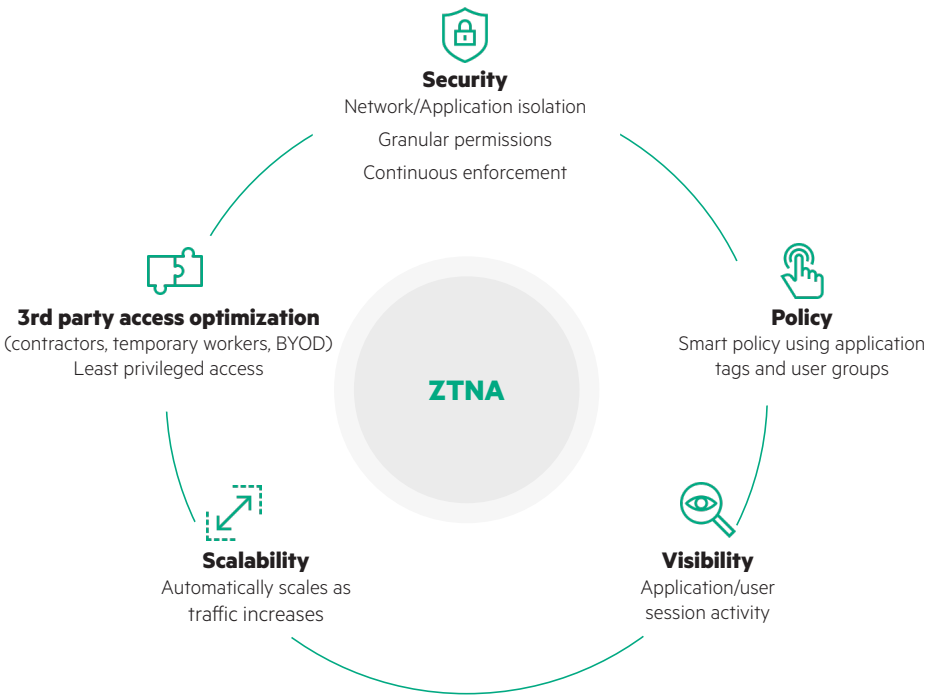


**Figure 3.** Unique ZTNA differentiators

**Enables granular app-level segmentation, without network segmentation**
Reduce the potential attack surface by only allowing access to specific resources. This limits lateral movement across the network, removes the need for complex network segmentation efforts, and reduces the potential attack surface of the business.

**Supports seamless access to apps from any device with or without a client**
Enable authorized remote employees and third parties to securely access business resources from the device of their choice in the most seamless way possible. The clientless method also supports browser-based RDP sessions reducing the need for VDI.

**Adapts access based on API-powered, contextual controls**
Automatically adapt access rights based on changes in key criteria, including user location, identity, and device posture. This continuous adaptive risk assessment helps better protect business data.

**Replaces legacy VPN technology**
HPE Aruba Networking ZTNA has the broadest support of private applications in the market. The ZTNA service not only supports all TCP and UDP traffic, including VOIP, peer-to-peer, and server-to-client workflows (which are difficult for most ZTNA vendors), but also all modern web apps like SSH, RDP, Git, DB, etc. Now IT teams can fully replace their VPN for good.

**Simplifies security with 100% cloud-delivered architecture across 500 global edges**
IT can stop spending time on managing VPN appliances. With HPE Aruba Networking SSE, every connection is brokered in the SSE edge location best suited to provide the connection — even in the case of a disaster. IT can rest assured that they'll be able to minimize disruption and maximize uptime.

**Inspects all traffic flowing to and from private resources**
For the first time, gain deep visibility into what employees and third parties are accessing. View user activity, file downloads, record brushstrokes, and commands used during a session, and block any malicious actions.

## Get Started

Learn more about HPE Aruba Networking's ZTNA and how you can use it as an alternative to your VPN by connecting with one of our SSE experts! Or experience the power of HPE Aruba Networking yourself with our free SSE Test Drive.

**Make the right purchase decision.**
**Contact our presales specialists.**

**Chat now (sales)**

**Call now**

Visit **ArubaNetworks.com**

**Get updates**

Hewlett Packard Enterprise



SB_VPNWithHPEArubaNetworkingZTNA_LP_091724 a00136658ENW