VERSA NETWORKS

WHITE PAPER

Why Legacy VPNs are Obsolete: The Future of Secure Private Access

Table of Contents

How the pandemic exposed the limits of legacy VPNs

Prior to the pandemic, the dominant remote networking model revolved around Virtual Private Network (VPN) appliances that had a fixed capacity and were implemented in enterprise data centers. Historically, most enterprises only allowed around 10 to 20 percent of their workforce to use a VPN connection to access resources in their data center. With the sudden closure of offices everywhere, the surge in work-from-home traffic faced serious bandwidth constraints at the VPN concentrator locations. As enterprises attempted to expand the capacity of their traditional VPN solutions, they discovered that hardware was in short supply, wait times for new hardware to ship rarely met the timelines needed to support their workforce, without even factoring in the additional time needed to install, configure, and test the multiple hardware components, and pricing was becoming an issue during a time when organizations faced uncertainty around budgets.

These struggles led many enterprises to explore cloud-delivered options to augment the VPN solutions already implemented, thus offloading administrative and management pain points. The migration to an "as-a-service" model accelerated the delivery of secure private access because it met the immediate remote working needs caused by the COVID-19 pandemic.

The legacy VPN architecture

In addition to capacity limitations revealed when the demand for remote access exploded, the traditional VPN architecture also suffers from inherent limitations in terms of route connectivity optimization and – ironically – security. A typical VPN solution is composed of a VPN concentrator appliance installed on the enterprise network (normally at a data center) and a VPN client installed on an employee's device to create a secure connection.

For redundancy and capacity planning, multiple VPN appliances are usually installed at different locations inside the enterprise network. The user then drives the selection of which appliance at which location is used for the connection, using a drop-down selector, or alternatively some form of global auto-select mechanism is utilized. This is in theory an improvement, but usually this fails to actually identify the optimal path and connection, since normally the connection decision is based on DNS and not on the actual performance of the VPN appliance.

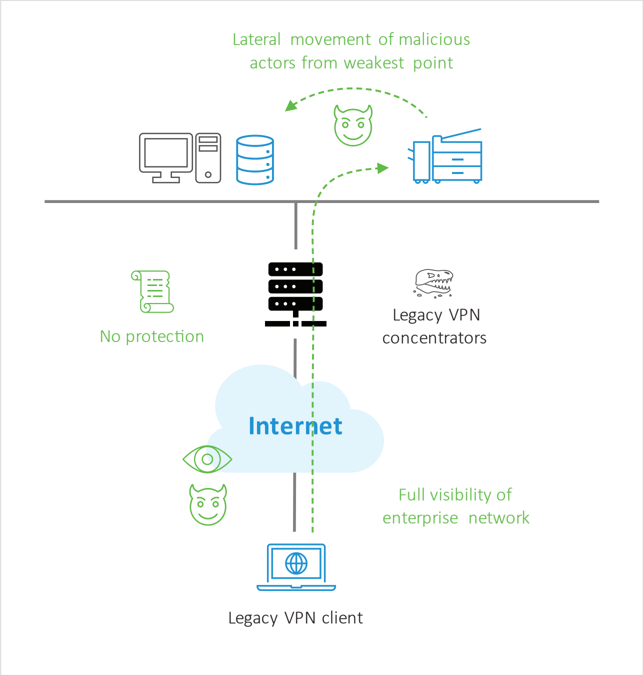
Lateral movement of malicious actors from weakest point
No protection
Legacy VPN concentrators
Internet
Full visibility of enterprise network
Legacy VPN client

Fig. 1 - Traditional VPN clients can access resources and be left exposed to vulnerabilities and threats.

The above-mentioned security limitations are introduced by the VPN model's typical use of L3 authorization. The access policy applied by a traditional VPN authorizes an authenticated user access any or all network resources. Since the application servers are responsible for authenticating and authorizing users for individual applications, this makes the system vulnerable to scanning attacks and other forms of attacks that exploit any existing vulnerabilities in the applications.

The transition to zero trust

Secure private access generally refers to user access solutions for private applications that apply “zero trust” principles of least privilege control and continuous trust evaluation, frequently referred to as Zero Trust Network Access (ZTNA) solutions. Such solutions remove network location and the hosting environment as implicit trust parameters, and focus instead on establishing explicit identity-based trust in a manner that is adaptive, granted dynamically per access attempt, restricted to a need-to-know basis, and based on verified identity and context. This approach significantly reduces a network’s attack surface.

In the ZTNA model, as shown in Figure 2, the secure gateway replaces the VPN appliance. Unlike the VPN appliance that is installed on the enterprise’s premises, the secure gateway is instantiated in the cloud, which allows for flexibility, scalability, and elasticity, with the ability to also instantiate multiple secure gateways in different availability zones or regions around the world.

Secure private access connections

A secure private access solution includes a client that is installed on the employee device and will connect to any of multiple secure gateways anywhere in the world when accessing corporate resources, with numerous security and performance benefits. The connection provides an encapsulated and encrypted path to the secure private access service, and is resilient because it does not have to re-establish a connection to the service in the event of a network failure, allowing optimal up-time. The best secure gateway connection can be selected at any given moment based upon performance metrics of the network connectivity to a given secure gateway and the performance of the secure gateway itself. The client also acts as a policy enforcement point, capturing data regarding the connecting device and the user requesting access. Based upon appropriate corporate policy, the client will determine what applications are connected to via the service and which applications can go directly to the internet.

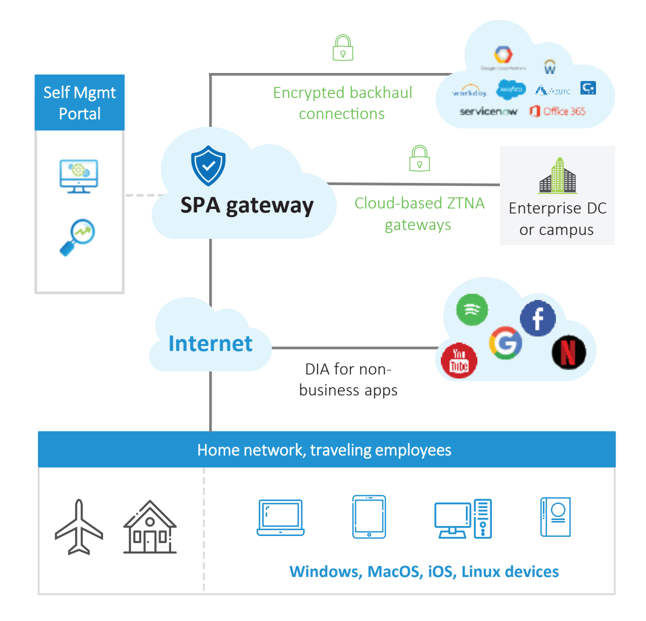
Self Mgmt Portal
Encrypted backhaul connections
SPA gateway
Cloud-based ZTNA gateways
Enterprise DC or campus
Internet
DIA for non-business apps
Home network, traveling employees
Windows, MacOS, iOS, Linux devices

Fig. 2 - Traditional VPN clients can access resources and be left exposed to vulnerabilities and threats.

In terms of a connection to the enterprise network, in a traditional VPN solution this was always a direct connection to the enterprise data center, but in an SPA service this is a network connection, usually with an IPSec tunnel or a private network connection to the enterprise. For redundancy, multiple enterprise network connections can be established.

If the SPA service is part of a SASE service, the SASE service can also provide an integrated suite of SSE security services either at the secure gateway or in the SASE cloud. This set of security services may be extensive, including network firewall, Cloud Access Security Broker, malware detection and response, data loss prevention, intrusion detection and prevention, domain name filtering, URL filtering, and full forward IP proxy. Each of these security services is necessary to ensure that the access and data that are entering and leaving the enterprise network and cloud services are protected. In this new model, the SPA solution is an evolution of the traditional VPN.

Leveraging gateway deployment

The cloud gateways can be deployed in numerous cloud services such as AWS, Equinix, and Microsoft Azure. Having a global, dispersed network of cloud service points of presence (PoPs) provides greater flexibility and fault tolerance, which equates to a better customer experience because the connection can be determined by the best performance path through a cloud gateway.

If the solution utilizes a full forward proxy, the enterprise private networks are obscured from the public and do not expose the actual IP addresses of the enterprise resources. This network obfuscation should extend to the enterprise cloud instances. Any SPA solution should also allow the enterprise to establish multiple network connections either over a public internet or via a private network access method, such as a SCI (AWS) or Express Track (Azure). This flexibility provides a better customer experience as the traffic would not need to be back-tunneled to the enterprise data center but could still be secured by the SASE service.

In addition, if the SPA service is integrated with SD-WAN capabilities, or is part of a multi-cloud SASE service, it has the ability to connect to an enterprise's private virtual cloud instances and can arbitrate over the private cloud enterprise connection or utilize an encrypted path via the public internet, thus providing a built-in secure failover for the public or private cloud instances.

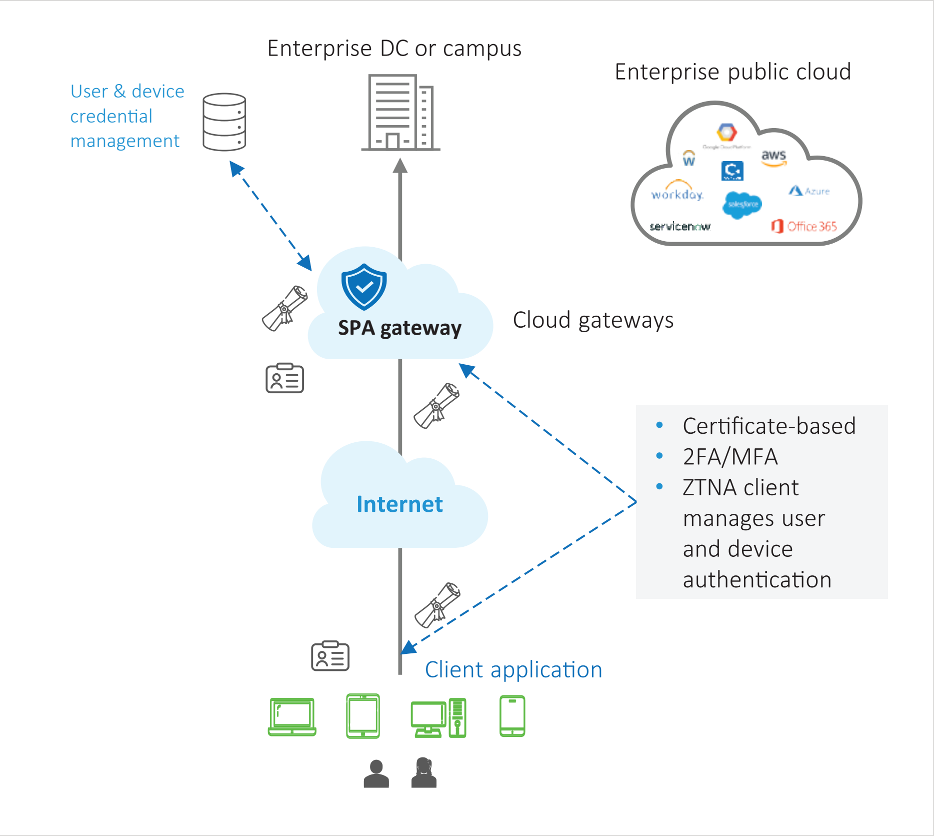

Fig. 3 - Secure private access applies per-user policies to ensure that users who are authorized to access specific applications are only allowed to reach the application in question.

Policy enforcement, authentication, and obfuscation

Policies for secure private access are broken into two parts: 1) the authentication and authorization of the user to use the service and 2) the authorization of the user to actually perform an action through the service. As seen in Figure 3, the client should authenticate the user based on multiple methods per the corporate policy. For example, this policy could require that the authentication be issued via SAML, LDAP, or SSO and just include a traditional login-password combination, multi- factor authentication, one-time password, or certificate authentication. Based on the policy, different authentication methods could also be triggered based on the contextual access of the user: geolocation, time, device health, and more. For example, an LDAP authentication is required when accessing from the employee's home, but multi-factor authentication is required when the employee is traveling and accessing from new locations.

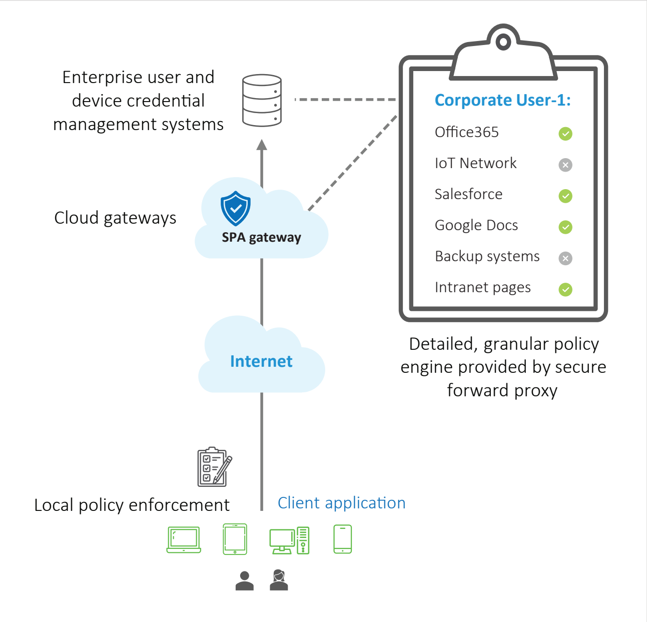

Fig. 4 - Corporate access policies can be narrowed to include a specific user and a specific application flow within a specific set of contextual parameters.

A secure private access service protects the clients as well as applications by:

- Applying per-user policies to ensure that users who are authorized to access specific applications are only allowed to reach the application.
- Applying policies that hide the network topology of the applications from the users, and vice versa.

SPA intelligently applies a combination of forward proxy, CGNAT, ALGs and DNS proxy to ensure that the end user clients are not exposed to the actual IP address space where the applications are hosted. Thus, a malicious actor who may have access to the device will not be able to glean more information about the network internals, creating a barrier for further attacks. The solution works seamlessly with a variety of applications including FTP, voice, and video.

The client has the ability to enforce device compliance based upon many different factors like:

- the anti-virus version
- the anti-virus signature version
- operating system type and version
- operating system patch
- if it's a corporate device or personal device
- specific software installed on the device

By inspecting parameters on the device, the granularity of the context allows organizations to establish an Endpoint Information Profile (EIP) when devices are connecting to the enterprise network. Included in the EIP are additional checks such as a compliance check and reporting about the remote access.

The EIP must also authenticate and authorize a user when they are accessing via their compliant device and, once authenticated, the corporate polices will determine if the user is allowed to actually perform the requested actions. Corporate policies can be applied at the application level to give a wide granularity of control such as requiring session authentication or restricting access within an application. In addition, corporate policies can be further narrowed to include a specific user and a specific application flow with a specific set of contextual parameters such as not allow a remote, traveling user to access sensitive HR files within an application.

For bring-your-own-device (BYOD) scenarios, connections to an SPA service should be able to be made without the installation of a client. The full-forward IP proxy would provide a captive portal for these devices to register, get authorization, and then get access granted. Where a client is not utilized, the secure connection typically can only send traffic to the cloud gateway, and at that point the SASE service would be the enforcement point to implement the corporate security policies.

The next frontier: Zero trust access for a hybrid workforce

While protecting a surging number of remote workers during the pandemic was the use case that lit a fire under the transition from legacy VPN to secure private access solutions, the post-pandemic reality of hybrid workers – workers that move between home, mobile, and office locations, often switching between them in the same week, if not the same day – has led many users and security teams to ask how they can apply zero trust to their branch offices and campus sites as well. Many organizations have learned that the ZTNA solutions they implemented, while effective for remote work, face limitations in their architecture when applied to corporate work environments. For 2024 and beyond, Gartner predicts significant movement from the current dominant ZTNA use case, remote workers, to what it terms “universal ZTNA,” covering office workers and devices as well, using new “next gen” ZTNA solutions that are integrated with SD-LANs to provide a seamless user experience and improved security independent of location.

About Versa Networks

Versa Networks, the leader in single-vendor Unified SASE platforms, delivers AI/ML-powered SSE and SD-WAN solutions. The platform provides networking and security with true multitenancy, and sophisticated analytics via the cloud, on-premises, or as a blended combination of both to meet SASE requirements for small to extremely large enterprises and Service Providers. Thousands of customers globally with hundreds of thousands of sites and millions of users trust Versa with their mission critical networks and security. Versa Networks is privately held and funded by Sequoia Capital, Mayfield, Artis Ventures, Verizon Ventures, Comcast Ventures, BlackRock Inc., Liberty Global Ventures, Princeville Capital, RPS Ventures and Triangle Peak Partners. For more information, visit https://www.versa-networks.com or follow Versa Networks on X (Twitter) @versanetworks.

Versa Networks, Inc, 2550 Great America Way, Suite 350, Santa Clara, CA 95054
+1 408.385.7660 | info@versa-networks.com | www.versa-networks.com