WHITE PAPER

Zero Trust Security

Discussion of a "de-perimeterized future" in networking was initiated by the now-disbanded Jericho Forum as far back as 2004. The character of **what exactly constitutes a security perimeter** of a network is the foundation of a Zero Trust Network Architecture (ZTNA).

The networks of yesteryear had hard perimeters following fixed building, location or organizational boundaries. Traffic and devices "inside" the perimeter were implicitly—by default—trusted and allowed any-to-any access. The fixed perimeter was secured with choke points comprising stacks of firewalls and VPN aggregators where untrusted traffic from "outside" the perimeter was routed and forced to enter to be scrutinized before being allowed "inside". Long ago, traffic originating "outside" the hard perimeter of the typical enterprise was minimal: all users and all applications resided inside the perimeter, in fixed geographic locations, with only occasional access via VPN by a remote worker or a partner organization.

The security approach of implicitly trusting all traffic "inside" the network perimeter offers a field day to bad actors. If hackers could only manage to breach the VPN or Remote Desktop (RDP) controls, and thereby gain "inside" access to the network, they had almost unlimited opportunity for damage and lateral movement.

By contrast to this strict, heavily-guarded network perimeter of enterprise and government networks, the internet was designed to connect things, not to block things. With only an IP address and a DNS server, anything can connect to anything else. Authentication of credentials, if any, was the responsibility of the destination application or server, after the connection was already allowed.

In recent years the fixed enterprise network perimeter has stretched and contracted into a fluid, amorphous, ambiguous "edge" due to several foundational trends in the industry. These trends immensely expanded the attack surface of corporate assets.

- Cloud migration: Large and small organizations have migrated to cloud-based assets, enabling significantly increased business agility, cost-reduction, time-to-market, market change or seasonal adjustments, architectural flexibility and enabling digital business models.
- Direct Internet Access (DIA): By leveraging ubiquitous internet connections rather than fixed-circuit MPLS, branch offices reaped many advantages in improved cloud application performance, reduced transport costs and better HA architecture.
- Work-from-anywhere (WFA): A gradual upward trend in work-from-home and mobile users was accelerated beyond all expectations by the covid-19 pandemic. Seemingly overnight the vast majority of knowledge workers were WFA, using internet transport connections shared with non-employee household members to access on-prem and cloud corporate assets.
- Unmanaged BYOD devices and IoT: User devices that are strictly issued, prescribed and controlled by IT is no longer a viable operational solution. Users have a multitude of their own devices with disparate OSs, unknown levels of patching and mixed corporate and personal use information and applications. Burgeoning IoT devices are everywhere, and

many of these are low-end with embedded protocol stacks and software of unknown provenance that cannot be tracked or patched. Any user, or hacker, can connect a new device to the network.

In today's era of client-to-cloud and WFA, there is a dire need to upgrade organizational security architecture: not just the architecture, but also the approach to the architecture.

- The home has now become part of the office.
- The internet has become part of your corporate network.
- The perimeter to defend has become software-defined (SDP)

The "perimeter" to be secured often exists transiently between a WFA user device connected via the internet to a dynamic cloud location. Securing an SDP requires precise and dynamic security measures based on identity and context to deliver a secure, reliable, and dynamic user, customer, and application experience that can be enhanced, measured, monitored, and diagnosed.

A modern architecture shifts away from the older network-centric model where traffic is forced to a specific policy enforcement point to get the appropriate controls. Instead, it is structured around an identity-centric model where capabilities are "ubiquitous" and controls are applied based on authentication and context. Google's BeyondCorp holds that traditional security controls for the corporate perimeter are insufficient and that the perimeter must be extended to every user and device.

What is Zero Trust Security?

Gartner defines ZTNA as "a product or service that creates an identity- and context-based, logical access boundary around an application or set of applications. The applications are hidden from discovery, and access is restricted via a trust broker to a set of named entities. The broker verifies the identity, context and policy adherence of the specified participants before allowing access and prohibits lateral movement elsewhere in the network. This removes application assets from public visibility and significantly reduces the surface area for attack."

The term "zero trust" was officially coined in 2010, and maintains that all network traffic is by default untrusted, and all resource access requests must be individually controlled by identity, context and policy.

Trust Nothing

In short, the essence of ZTNA is to trust nothing: not an IP address, not a device, not a connection, not an application—the network is assumed to be hostile, and the default security posture is "deny all". With a ZTNA approach, user access to resources is adaptive, granted dynamically per access attempt, restricted to need-to-know, and based on verified identity and context. This approach significantly reduces your network's attack surface. ZTNA removes network location as an implicit trust parameter, focusing instead on establishing explicit identity-based trust:

- Verify the user
- Verify the device
- Verify the application

A ZTNA architecture employs preventive security measures such as:

- Multifactor authentication (MFA)
- Micro-segmentation
- Least-privilege access

The Principles of ZTNA

The key tenets of zero trust—first established by the Jericho Forum—include:

- Trust no one: Access is granted only to users, devices and applications that provide verifiable credentials.
- Verify identity: The identity and authentication of an end-user is paramount.
- Allow least-privilege access: User privileges start at zero, and are only granted when necessary.
- Device-awareness: Disallow access to all anonymous, unverifiable or compromised devices.
- Application-awareness: Logically isolate each application and authenticate the user before granting access.

Why do you Need Zero Trust Security?

Traditional fixed perimeter security defense technologies such as centralized firewalls, IDS/IPS and VPN aggregators are no longer able to adequately protect your network: they cannot protect internet access links, WFA users or cloud access without forcing all traffic through a choke point (such as your data center or a hub location) which impairs application performance, doesn't scale to the suddenly very high percentage of the WFA workforce due to the covid-19 pandemic, doesn't solve IoT device exposures on your internal network, and doesn't guard against bad actor lateral movement once some aspect of your network was breached.

In summary, a ZTNA architecture provides the following solutions and benefits:

- Embedded security: Security must be available on-demand for all traffic and all endpoints: it must be distributed, augmented with cloud-based presence, flexible, simple, and available everywhere, including, at a minimum, NGFW, URL filtering, SSL decryption, IPS, antivirus, anti-malware, SWG, ZTNA and CASB.
- Unmanaged and BYOD devices: Partner organizations, WFA users and IoT rely on ZTNA to securely and appropriately access applications without IT having to trust the location or a VPN connection.

- Reducing the attack surface: ZTNA provides controlled identity- and context-aware access for a software-defined perimeter (SDP). It also restricts lateral movement and therefore limits the damage a bad actor can do if your network should be breached somewhere.
- Alternative to VPN: VPNs are slow for users, offer poor security, are difficult to manage, don't scale, and don't protect against bad actor lateral movement. ZTNA is a flexible, scalable, easily manageable alternative for modern networks.
- Secure multi-cloud access: Securing hybrid and multi-cloud access requires a ZTNA approach. Traditional mechanisms simply don't scale or perform adequately in a multi-cloud environment.
- Network visibility: A ZTNA architecture allows you to see, track, monitor and measure traffic and events beyond your traditional private network, such as cloud and internet traffic.
- Risk management for remote access: ZTNA provides protection for the SDP that extends to all home, mobile, partner, cloud and other "off-prem" locations.
- Protection from "insider" attacks and exploits: ZTNA provides detection and protection for attacks from compromised internal devices and IoT.
- Controlled application access: One-on-one, per attempt, control of application access, or to grant conditional application access.

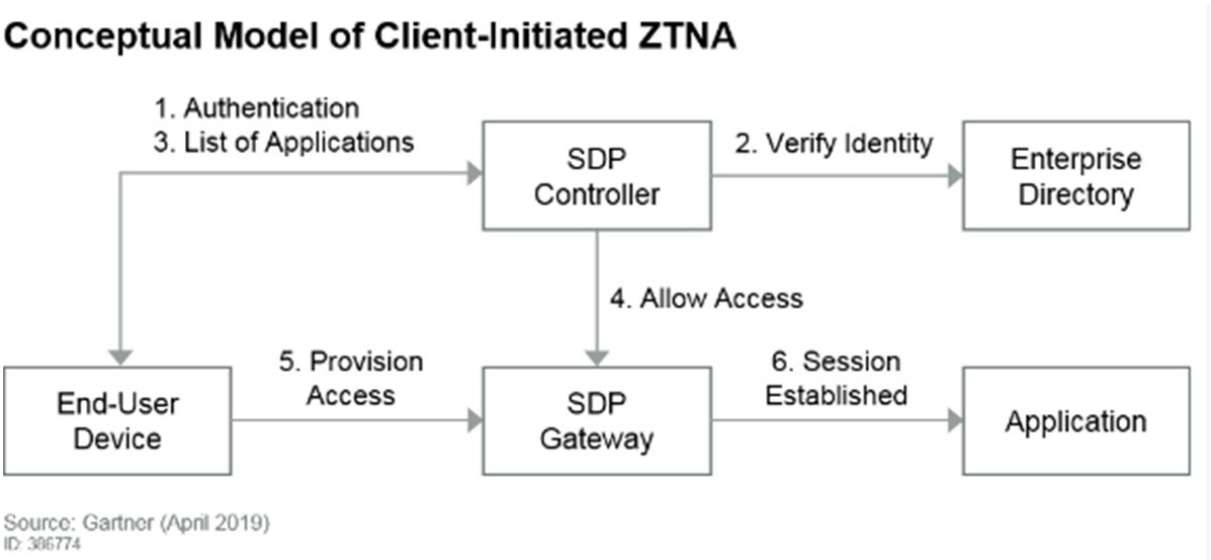
Implementing Zero Trust Security

ZTNA as an integral part of your SASE solution. ZTNA architecture works fundamentally different from traditional network-centric solutions: it is most often entirely software-defined with all security functions (FW, IPS/IDS, anti-virus, authentication, DDoS etc.) embedded in a single software stack.

Gartner's ZTNA Market Guide highlights two models of ZTNA architecture: client-initiated and service-initiated. These two models may be combined in any particular implementation.

Client-initiated ZTNA

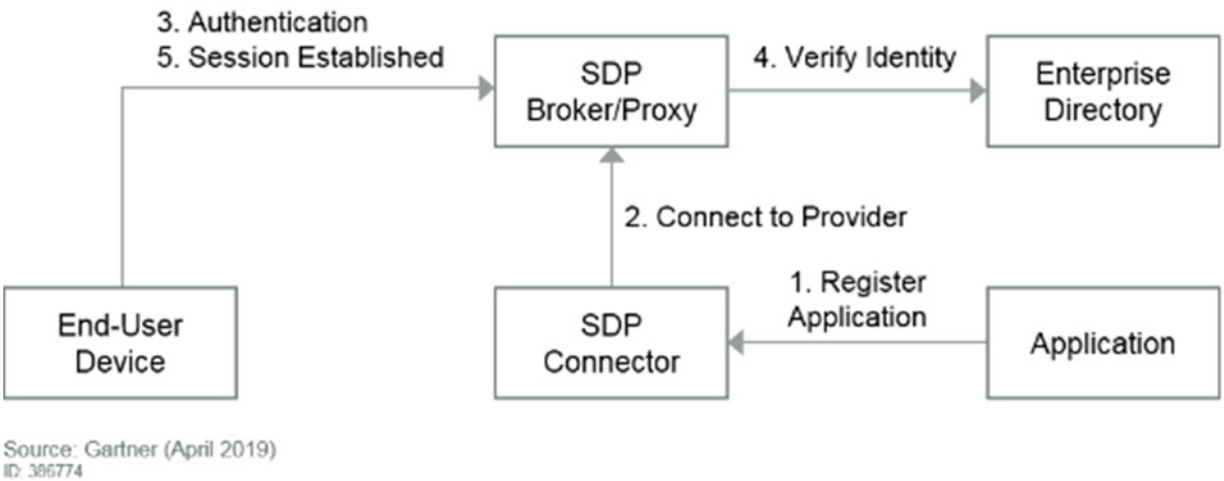
This model follows the original Cloud Security Alliance (CSA) SDP specification. A software agent installed on the device sends its security context and credentials to the SDP controller. The SDP (or ZTNA) controller authenticates the user on the device resulting in a list of allowed applications. Once authenticated, the SDP controller provisions connectivity from the device through a gateway that protects services from direct internet access and applications from DDoS attacks. This approach is most useful to implement on managed devices as it requires the installation of a software agent on the device.



Service-initiated ZTNA

This model follows Google BeyondCorp's architecture. An SDP (or ZTNA) connector installed along the application establishes and maintains an outbound connection to the cloud provider. Users are challenged to authenticate to the provider to access protected applications. The provider subsequently authenticates to the enterprise's identity management system. Application traffic passes through the provider's cloud, isolating the application from direct access via a proxy. In this model, firewalls no longer require openings for inbound traffic.

This model works well for unmanaged devices as no special software is required on the end device. However, this approach requires application protocols to be based on HTTP/HTTPS, limiting the architecture to web applications and protocols such as Secure Shell (SSH) or Remote Desktop Protocol (RDP) over HTTP.



Authentication

When a user requests access to an application in a zero-trust environment, the security software enforces authentication and evaluates the application access policy based on user, device, and identity. Authentication is performed using an enterprise-specific authentication system, such as Active Directory, or Single Sign-On (SSO) using Security Assertion Markup Language (SAML). Depending on the context and security requirements, Multi-factor Authentication (MFA) may be enforced in addition to the enterprise-specific authentication system.

As a result of WFA and digital transformation, most enterprises have more applications, services, data and users residing outside their traditional borders than inside. Cloud-based ZTNA services place the security controls where the users and applications are—in the cloud. Adopting a zero-trust security model normalizes the user authentication experience for application access by eliminating the distinction between being on and off the corporate network.

A wide range of potential policy-based responses aligns with an observed level of risk for a particular access attempt, including blocking, MFA, reducing user privileges, forcing a password change, requiring an authorizer, or isolating the user from the internet. All responses can be triggered based on identity, behavior, risk level, and other event contexts.

Components of a ZTNA Solution

A leading-edge ZTNA solution includes several functions and attributes to determine a risk-based allow-or-deny decision for any particular transaction or access attempt.

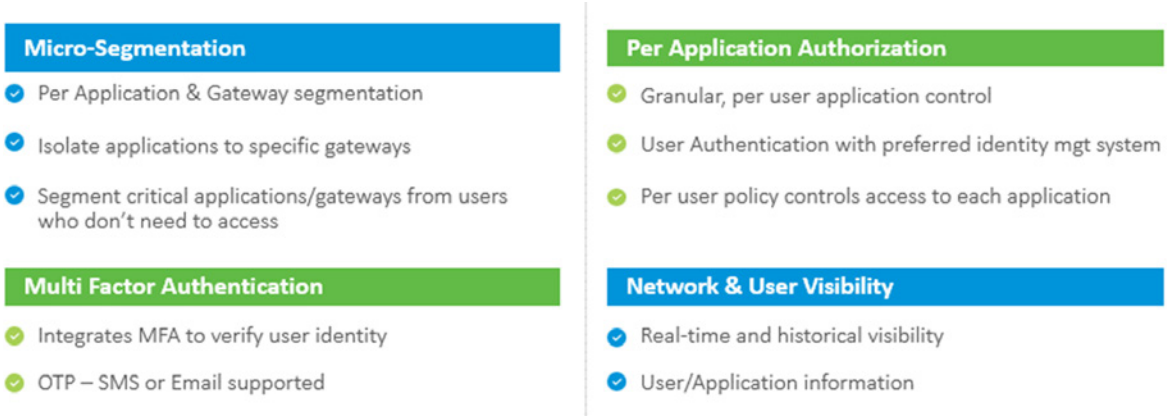
There are several components that comprise a ZTNA solution—all of which can be implemented as software only.

- SDP controller: SDP architecture uses a controller to establish trust between the end-user device, application and corporate security policy controls by authenticating users and devices. It manages a variety of real-time data—for example, the application being used, the location of the device, the device's operating system, and the network it is connected to—used in the risk assessment of each request to determine whether or not user access should be granted.
- SDP broker/proxy: This component is used in the server-initiated ZTNA approach where the client does not connect to the application directly, making the location of the application irrelevant to the access interaction. The SDP broker may be an appliance or a cloud service.

- Gateways: Gateways authenticate users, authorize application access protected with ZTNA, and secure the enterprise network from external threats, while optimizing the user experience by providing direct and optimized access to cloud applications.
- Authentication services: User credentials are verified using the organization's authentication and authorization services. This may include a wide variety of mechanisms such as Active Directory, MFA, device fingerprinting, geolocation, SAML (Security Assertion Markup Language), OpenID, OAuth, OTP (one-time passwords), LDAP, Kerberos, PKI and more.
- Unified policy: SD-WAN architectures provides a means of implementing unified user role and privileges that are maintained, updated and monitored independent of any device, unlike older methodologies such as FW rules that were specific to each device.
- Device choices: Enterprises can use managed corporate devices or BYOD. Security for IoT devices is also covered by ZTNA.
- User and Entity Behavior Analytics (UEBA): This function tracks users' behavior to identify anomalous events in the environment. Gartner defines UEBA as a cybersecurity process to detect insider threats, targeted attacks, and financial fraud. UEBA examines human behavior patterns and applies ML/AI or statistical analysis techniques to detect anomalies in the patterns.

Attributes of a ZTNA Solution

There are particular characteristics that a ZTNA solution must include to provide acceptable levels of security to your SDP.



Isolation is paramount: ZTNA completely isolates the decision to provide application access from network access, and grants application access only to authorized users. This reduces application attack risks from infected devices or compromised network segments.

Micro-segmentation ensures that once a user is authorized, application access is granted on a one-to-one basis for that specific user and that specific access attempt only. ZTNA enforces user access only to specific applications rather than granting full access to anything connected to the network as the older network-centric and border security mechanisms did.

ZTNA mechanisms also safeguard IP addresses so they are never exposed to the internet, in effect creating a "virtual network" that makes the rest of the network impossible to find.

One of the critical attributes of ZTNA is its network and user monitoring and visibility tools: user and device behavior are continuously monitored for abnormal activity, as described in Gartner's Continuous Adaptive Risk and Trust Assessment (CARTA) framework. ZTNA creates individualized "virtual perimeters" encompassing only the user, the device and the application.

Using ZTNA tools, the IT or security team can customize and automate user access based on an individual's role, responsibilities and needs within an organization. Sensitive data remain secure, while user access to data or applications is seamless and invisible, whether or not the user is on-prem or WFA, as well as whether or not the application is on-prem or in the cloud.

ZTNA is Integral to a SASE Solution

Securing DIA traffic is a primary SASE responsibility that protects the soft perimeter around every session and every location. In summary, SASE security functions include at least:

- A fully functional NGFW
- URL filtering
- SSL decryption
- IDS/IPS
- Antivirus
- Anti-malware
- SWG
- ZTNA
- CASB

SD-WAN gateways are globally available and provide distributed secure, reliable, and high-performance access to cloud applications, services, and resources in addition to providing cloud-delivered SASE and being part of a ZTNA framework. Enterprises may implement their own gateways (their own SASE/ZTNA services) or use provider gateways (a provider's SASE/ZTNA services).

How Versa can Help with Zero Trust Security

The Versa Secure Access (VSA)—part of Versa SASE—solution delivers leading-edge SASE services and secure connectivity to efficiently connect distributed users with distributed applications without compromising either security or the user experience of employees working from home or remotely from any other location.

VSA provides zero-trust security to your organization and assets, offering unique secure access benefits designed for an elastic workforce, and includes the following benefits:

- Services Edge (SASE)
- Zero Trust Network Framework
- Soft-perimeter protection for your business
- Extends perimeter protection to the end-user device
- Always-on application experience
- Elastic architecture that delivers scale and extends to WFA
- Hassle-free, software-based, single-software-stack integration, cloud-delivered services that fit into any existing environment
- Application segmentation to restrict access to applications
- Enterprise-grade authentication with MFA
- Granular application control
- Application and network visibility

VSA builds on the Versa Secure SD-WAN solution to securely connect remote employees to corporate resources. The VSA client provides horizontally highly-scalable access to deep security features—stateful firewall, anti-virus filtering, denial of service protection, malware filtering and more—embedded in the Gateways. VSA's Cloud Gateway architecture eliminates the need for VPN concentrators and VPN clients for the increasing numbers of remote workers. Instead, organizations subscribe to VSA's fully managed cloud service that scales horizontally and easily adapts to organizations' changing needs.

Key VSA features include:

- Quick and easy deployment, with zero infrastructure cost to implement a WFA solution.
- Seamless extension of application access, taking location out of the user experience—complete with security, performance, and visibility of remote working.
- Secure, seamless and instant connection to on-prem, cloud and personal resources without intrusion and with a minimized attack surface.
- Cloud-based control and visibility for monitoring, configuration, management that considerably simplify IT tasks.

What This Means for Your Organization

In a de-perimeterized environment, enterprises must implement elastic, secure, and scalable solutions that can be deployed and managed flexibly with modern software-defined techniques—including SD-WAN, SASE and ZTNA.

These modern solutions free organizations from the scalability choke points and traffic backhaul penalties of legacy VPN aggregator and FW appliance deployments which allow access based only on IP attributes. These legacy VPN-FW solutions leave large opportunities for bad actors to breach once and then move laterally in your network to inflict maximum damage on all assets connected to the network. With ZTNA the network becomes simple transport—with

the internet part of the corporate network—with end-to-end (client to application) encrypted micro-tunnels able to securely use any transport.

ZTNA provides a fresh client-to-application, identity-based concept of security where, by default, no user, device, system, or application is trusted, either inside or outside the traditional network boundaries. Instead, trust is established and adjusted dynamically based on fine-grained authentication, authorization, and encryption technology on a per-access basis: it is a "built-in security" mechanism.

In summary, the key capabilities of ZTNA are:

- Identity-based authentication for every access attempt
- Secure, micro-segmented access to all resources and assets
- Continuous assessment and monitoring of risk and trust

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