QUICK START GUIDE

January 2026

VPN to ZTNA Migration

Contents

About this Quick Start Guide

This document serves as a starting reference for performing VPN Migration to Zero Trust Network Access (ZTNA) using Versa Unified SASE platform's Versa Secure Access (VSA) and Versa Security Service Edge (SSE). This guide is designed to offer a framework and basic setup guidance to accomplish this migration.

Before You Begin

Before you proceed with this guide, please ensure you've met the following prerequisites:

The provider administrator must complete your tenant configuration. If you haven't received this information, please get in touch with your Managed Service Provider or Account Manager for assistance.

You have the Enterprise Administrator (Tenant Admin) credentials for the Versa SASE portal, also called the Concerto User Interface.

Overview of VPN to ZTNA Migration

Versa ZTNA delivers fast, reliable, and secure direct-to-application access using identity and context-driven policies. Integrated into the Versa Unified SASE architecture, it unifies access, security, and networking under a single cloud-delivered framework for lower cost and higher agility.

To successfully migrate your workforce from VPN to Versa ZTNA, you will need to perform the following planning and migration activities:

1. Inventory Your Existing VPN and Use Case Needs
2. Perform ZTNA Migration for a Use Case
3. Validate and Scale Up ZTNA Implementation Into Production

Versa recommends you perform these activities for an individual use case, such as for a specific group of users. After you have completed the production migration of a use case, you can repeat the steps for additional use cases.

Inventory Your Existing VPN and Use Case Needs

Who are your users? What are they connecting from, and where are they located? What applications are they connecting to? Understanding the requirements of your users and what access they require to perform their jobs is critical when transitioning from a VPN environment to Versa ZTNA. Versa ZTNA focuses on granting explicit, conditional access to the application or service based on user identity, device posture, and other contextual factors. Users should be granted access to only the applications and services they need. This protects the company from threats of undesired lateral data movements which can compromise the integrity of their business or result in exfiltration of critical data assets.

One of the key activities you must perform to properly transition from VPN to ZTNA is to inventory your workforce and related use case requirements. Examples include user groups, user devices, locations, authentication methods, and application or service resources. Try to identify as much commonality as possible between use cases and their downstream requirements, so that there is maximum overlap when creating your ZTNA policies and rules. For example, all users require access to a common set of applications, regardless of their assigned user group. Doing this increases the speed of the deployment and improves the resiliency of the company's security by standardizing as many rules as possible and minimizing the number of exception rules that must be created.

Inventory Item	Description & Examples
User Groups	Which user groups does your company have? Examples include contractors, engineers, C-suite, human resources, finance, general employees, interns, IT staff, etc.
User Devices	On what devices are these users connecting to your applications and services? Examples include laptops, desktops, and mobile devices. Additional information to collect is operating system types, and if managed endpoint software such as anti-virus or EDR software is deployed.
Authentication Method	How are the users being authenticated to the corporate network and resources? Examples include an identity provider such as Microsoft AD/Entra or Okta, and authentication protocols like LDAP or SAML.
Location	What locations can the user be permitted to connect to the corporate network and resources from? Examples include home office, work office, and geographical locations such as the USA and Europe.
Resource	What resources is the user connecting to? Examples include web-based SaaS applications, internal applications, file shares, code repositories, etc. Resources can be external or internal.

To aid with performing this key activity, use Appendix A: ZTNA Transition Plan Checklist to help you identify, organize, and prepare the critical requirements for each use case.

Perform the ZTNA Migration for a Use Case

Implement your first use case according to the table of activities below. Note that the activities you will need to perform depend on the Appendix A: ZTNA Transition Plan Checklist for the use case. Some steps may not be required, and some steps might only need to be performed once across several use cases, such as configuring the authentication method for your users. Leverage previously configured policies and/or rules if they overlap between use cases to minimize the amount of new configuration required.

Configure Site-to-Site Tunnels
Location: Configure > SSE > Settings > Site-to-Site Tunnels

Documentation | Quick Start Guide

Key Components to Configure
IPSEC | SA Information | Routing Information | Static Routing

Configure Authentication, Add Users & Groups
Location: Configure > SSE > User & Device Authentication > Profiles

Documentation | Quick Start Guide

Key Components to Configure
LDAP protocol | SAML protocol | RADIUS | Versa Directory | Certificate-based (User or Device)

Configure User-Defined Objects
Location: Configure > SSE > User-Defined Objects

Documentation | Quick Start Guide

Key Components to Configure
Private Apps | Private Services | URL Categories

Configure Secure Access Profiles
Location: Configure > SSE > Secure Access > Client-based Access > Profiles

Documentation | Quick Start Guide

Key Components to Configure
Public DNS Servers | Private DNS Servers | Private Routes | Digital Experience Monitoring (DEM)

Configure Secure Access Policy Rules
Location: Configure > SSE > Secure Access > Client-based Access > Policy Rules

Documentation | Quick Start Guide

Key Components to Configure
Operating System | User/Groups | Source IP Location | Traffic Action Split Tunneling | Preferred Gateways | Client Features

Configure TLS Decryption
Location: Configure > SSE > TLS Decryption >
Profile Location: Configure > SSE > TLS Decryption > Policy Rules

Documentation | Quick Start Guide

Key Components to Configure
Decrypt/Inspect Certificate/Decryption Options | Applications/Users/Groups/Endpoint Posture

Configure Real-time Protection Profile(s)
Location: Configure > SSE > Real-Time Protection > Profiles

Documentation | Quick Start Guide see right

Key Components to Configure
Quick Start Guide: Filtering: URL DNS IP File | Malware | CASB | DLP | RBI | ATP

Configure Real-time Internet Protection Policy Rules
Location: Configure > SSE > Real-Time Protection > Internet Protection > Policy Rules

Documentation | Quick Start Guide

Configure Real-time Private App Protection Policy Rules
Location: Configure > SSE > Real-Time Protection > Private App Protection > Policy Rules

Documentation | Quick Start Guide

Install And Configure Versa SASE Client on User Device

Documentation

Validate and Scale Up ZTNA Implementation

After performing the configuration activities in section Perform the ZTNA Migration for a Use Case, above, you need to validate the solution requirements for a specific test user and/or pilot test user group in the use case. Common validation activities include:

- Can the user successfully connect to the Versa gateway, and are they connecting to the preferred (typically local) gateways available in the secure access policy?
- If Versa TLS decryption is enabled, is the web browser on the user's device properly showing a Versa certificate for an encrypted site (ie. https:// website)?
- Is the user able to reach all the required applications and services, both internally and on the Internet?
- If rule enforcement is being implemented by a policy, is the corresponding action being taken according to the policy?
- Are the access and application security activities reporting in the dashboards, and being properly logged, within the View dashboard of Concerto according to the configuration?

Gather feedback from both users and administration and address all issues or concerns so that the full scale up for the use case can occur successfully.

After verifying the use case requirements are being met with the test user or pilot group, expand and scale up the ZTNA migration for the user group into production, according to the defined migration plan. This can and will likely involve making additional corrections to the configuration of the solution, such as verifying the integration with your existing identity and access management systems. You should also verify and if necessary modify the access and security policies through the implementation process as defined by your organization, and monitoring the solution performance and behavior through View dashboard of Concerto.

Appendix A: ZTNA Transition Plan Checklist

Use this checklist to plan your ZTNA transition for your organization. Identify requirements for each use case (typically, a user group) that requires access to specific applications or services, and the conditions under which access should be granted. Repeat this checklist for each use case as you proceed with the inventory planning.

Use Case/Group Name: _____

Requirement	Circle/fill in	Requirement Details (fill in)
Need a Site-to-Site Tunnel? I.e. Versa Gateway to Versa appliance or company DC/ enterprise router via IPSec or GRE?	Y / N	
Allowed User Authentication Method?	LDAP, SAML, RADIUS, Versa Directory, User Certificate Based, Device Certificate Based	
Accessing Internet Apps? Which Apps? I.e. Office 365, Salesforce, Google Apps, etc.	Y / N	
Accessing Private Enterprise Apps? Which Apps? I.e. CRM, ERP, or HR systems, DB systems, file shares, dev tools, etc.	Y / N	
Approved End-user devices, configurations, locations? I.e. Laptop, desktop, mobile devices, Americas	Windows, Linux, Apple, Android Geographies	

Inspection of encrypted application traffic? Which Apps?	Y / N	
Endpoint Posture (I.e. managed EDR/XDR, AntiVirus, Antiphishing, DLP, disk backup, etc on an end user device)?	Y / N	
Security Policies (CASB, DLP, SWF, Malware) currently deployed? I.e. SaaS controls, PII regulations, website filtering	Y / N	

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