# ZT-LAN Overview

With the rapid expansion of work-from-home requirements, the need for zero-trust network access (ZTNA) for remote workers has increased exponentially. As Enterprises now pivot to a hybrid workforce in which employees work part of the time on campus and part of the time remotely, Enterprises are seeing a need to bring the same level of zero-trust network access (ZTNA), which was developed for remote workers, back into the on-premises campus and branch environments. However, legacy LAN solutions do not meet the needs of a hybrid workforce due to a number of limitations, including:

- Security
  - The lack of comprehensive built-in security
  - No built-in protection for east-west traffic flows
  - Unable to provide a true software-defined perimeter (SDP)
- Layer 2 limitations
  - Lack of multiple active paths
  - Slow convergence times
  - Proprietary technologies, vendor-specific solutions
- Siloed solutions for switching, WLAN, WAN edge, security
  - Separate tools for management, configuration, policies, analytics
  - Complex to deploy, manage, operate
  - Prone to having interoperabiity issues

Legacy solutions are very hardware-centric, complex, and difficult to manage. Enterprises increasingly require a more standards-based, software-defined approach that provides more intelligent solutions. Enterprises increasingly see a need for the following capabilities:

- ZTNA on premises
  - Bring the equivalent ZTNA for remote users to the enterprise
- Microsegmentation
  - For corporate appliances, IoT devices, and network attached devices, a more granular level of segregation than possible using VLANs, such as segmentation based on the type of device, the status of the device, etc.
  - Use zero-trust policies to make certain decisions, such as admitting a device, user, or application to the network, and also to allow or deny access to various parts of the enterprise network based on the security posture, status of device, user, type of application, etc.
- Built-in security
  - Apply security to functions that pertain to the enterprise campus environment; apply security policies to the

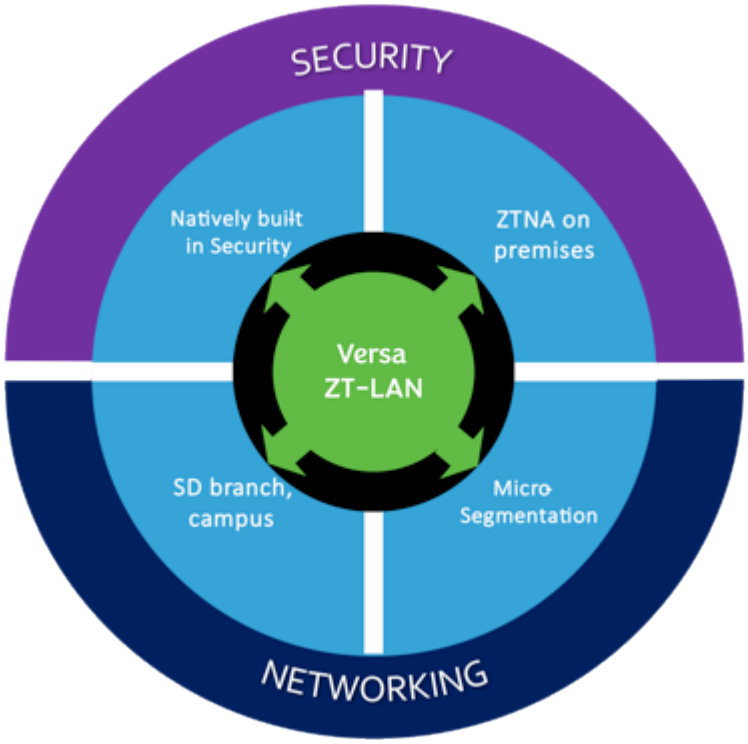
traffic of interest

- Software-defined campus and branch
  - SD-LAN solutions using standards-based technologies applied in a software-defined way

## Versa ZT-LAN

Versa Zero-Trust (ZT)-LAN solutions address the evolving security and networking needs of Enterprises. Versa ZT-LAN comprises two main component solution: ZT Edge and Secure SD-LAN. These solutions provide the following capabilities:

- ZT Edge
  - Natively built-in security
  - ZTNA on premises
    - Software-defined perimeter
    - Network access control
    - Lateral movement detection and prevention
    - Clientless and client-based options
- Secure SD-LAN
  - Software-defined campus and branch architectures
  - Microsegmentation



The Versa ZT-LAN solution operates in five sequential steps:

1. Identify—Who or what is connecting to the network, including applications, devices, users, security posture
2. Control—Applies policy-based access control; implements segmentation and placement decisions
3. Connect—Provides connections in both the north-south and east-west directions; uses overlay-based connections for flexibility and simplicity; implements network segmentation for granular control
4. Secure—Applies security policies and functions to protect the network from vulnerabilities
5. Monitor—Provides visibility into network events, traffic patterns, network activity, thresholds, etc.

Enterprises can deploy Versa ZT-LAN in the following ways:

- Full ZT-LAN solution (Secure SD-LAN and ZT-Edge)
- Secure SD-LAN only
- ZT-Edge only

Most workers use portable devices (laptops, phones, etc.) and frequently move from one location to another within a campus environment. Once a device has been admitted to the network and has security policies applied to it, these same policies follow the device throughout the campus network regardless of which wired connection or wireless AP the device is connected to at any given time.

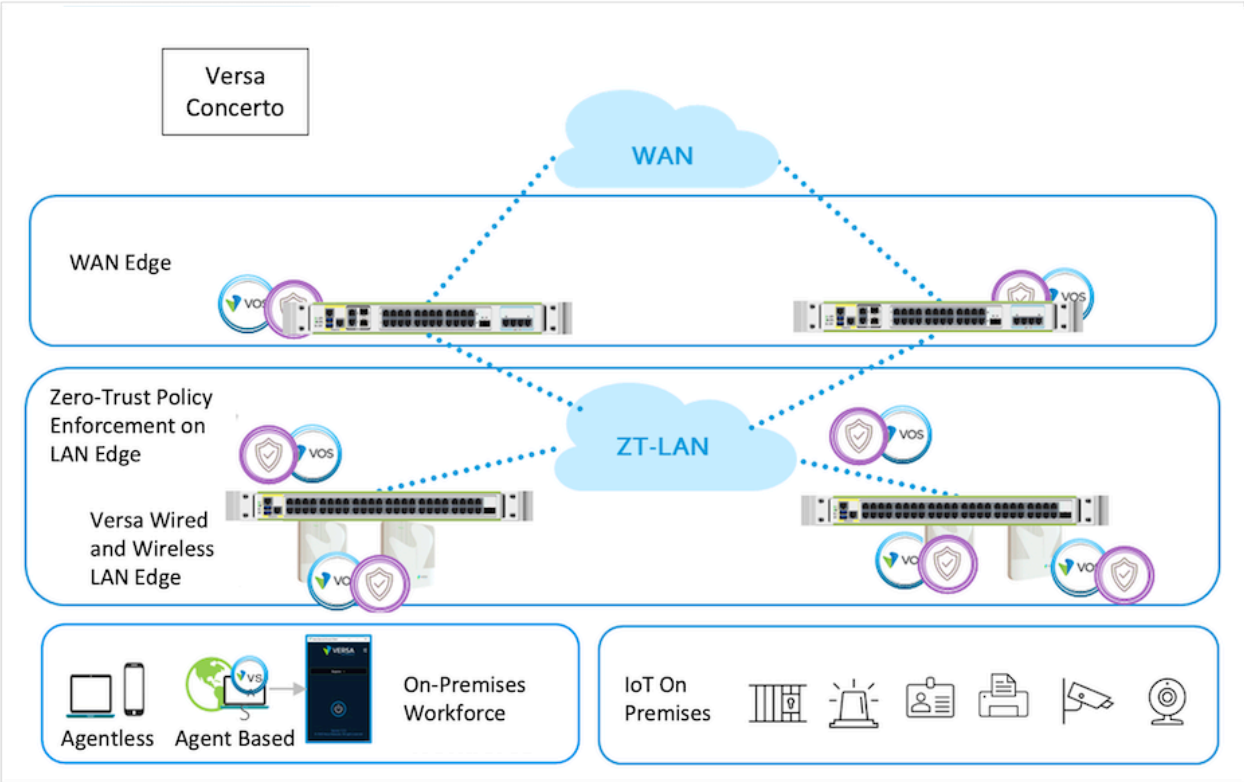
## VOS

The Versa Operating System™ (VOS™) delivers all of the ZT-Edge and Secure SD-LAN features and capabilities through the Director, Controller, Analytics (DCA) complex. VOS provides the flexibility to deploy features on all nodes or on selected nodes only while delivering consistent behavior throughout the network. VOS also provides a single portal, Versa Concerto, to manage SD-LAN, Security, and SD-WAN capabilities. Versa Analytics is a near real-time big-data solution that analyzes large amounts of log data sent from VOS devices and provides historical insights into contextual policy-to-event correlation and visibility based on application, user, device, and location

## Deploy ZT-LAN

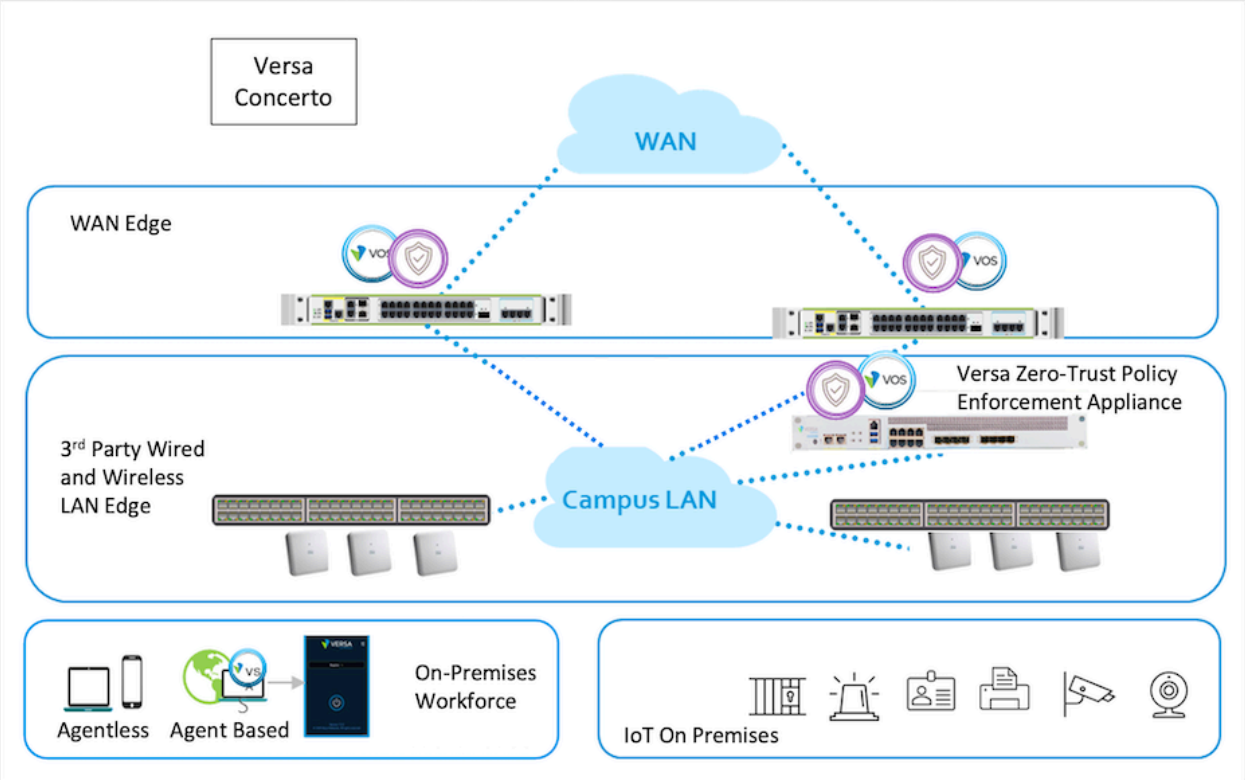
The preferred way to deploy Versa ZT-LAN is on the Layer 2 and Layer 3 switches and wireless access points (APs) at the edge of the LAN, which are the attachment points to the network. In this way, all ZT-LAN capabilities can be applied at the LAN edge: identification, placement in the network based on credentials, policy-based traffic management functions, etc. In this deployment type (shown in the figure below), the LAN edge consists of Versa wired and wireless LAN edge devices running VOS, which enforces the zero-trust policies.


Updated: Wed, 23 Oct 2024 07:32:31 GMT




In a brownfield deployment, you can insert a Versa zero-trust policy enforcement appliance into the existing campus LAN, as shown in the figure below. All traffic from third-party wired and wireless LAN edge devices is sent through a Versa appliance running VOS, which enforces the zero-trust policies. Adding a zero-trust policy enforcement appliance offers the following benefits:

- Avoids "hair-pinning" to cloud security nodes
- Delivers end-to-end visibility and enhances user experience
- Provides an integrated view (single pane of glass) for visibility and management
- Provides unified policy configuration and enforcement
- Saves cost and reduces complexity
- Sets up a dynamic SLA-based path




Another deployment method is to perform assessment and enforce policies on WAN edge devices.

Inserting a Versa zero-trust policy enforcement appliance into the existing campus LAN or performing assessment and enforcement on WAN edge devices can provide some limited benefits. However, both of these methods are less than ideal because they are *n*-layers of devices away. They are not able to protect from attacks within the LAN in the east-west direction.

## Hardware Platforms

Versa CSX 4000 series appliances are a family of next-generation software-defined (SD) enterprise LAN edge and access layer appliances combining a best-in-class merchant Ethernet switch chipset with a high-performance, x86-based processor subsystem to deliver cutting edge Secure SD-LAN capabilities from the edge of the LAN.

CSX 4000 switches run the Versa Operating System™ (VOS™), which provides the following capabilities:

- Application intelligence and application policy-based forwarding
- Big-data based analytics
- Comprehensive, integrated security (such as on-premises ZTNA)
- Fully secure Software Defined Perimeter (SDP)
- Genuine multitenancy

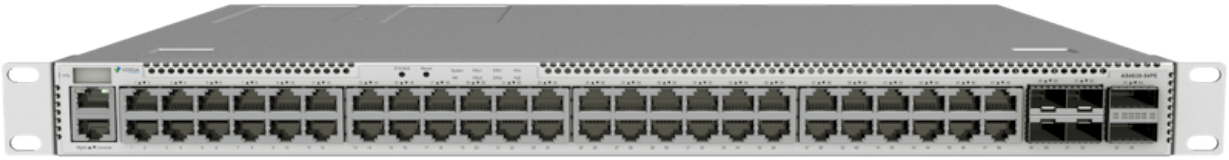
- Line-rate Layer 2 and Layer 3 switching
- Next-generation software-defined access
- Scalable, advanced routing

The CSX 4000 series comprises the CSX4300 and CSX4500 LAN switches.

## CSX4300

Versa CSX4300 is a powerful, purpose-built Ethernet switch that provides Secure SD-LAN functionality in LAN-edge and LAN-access deployments. The CSX4300 switch includes the following features:

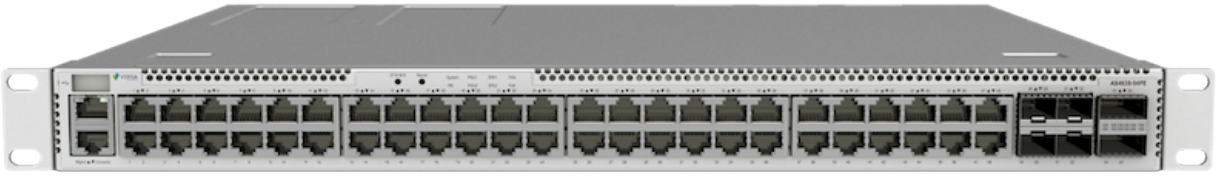
- 48 ports of 1GE with PoE++ (90W)
- 4x SFP28 (25/10GE)
- 2x QSFP28 (100GE) switched interfaces



## CSX4500

Versa CSX4500 is a higher bandwidth version of the CSX4300 that includes the following features:

- 48 multirate ports installed as 12 ports of 10/5/2.5/1GE with PoE++ (90W), 36 ports of 2.5/1GE with PoE++ (90W)
- 4x SFP28 (25/10GE)
- 2x QSFP28 (100GE) switched interfaces



For more information, see the Cloud Services Switch 4000 Series guide.

## Additional Information

ZT-LAN Architecture
ZT-LAN Features and Capabilities