ZT-LAN Features and Capabilities

The Versa Networks ZT-LAN solution includes a rich set of LAN features, security features, and other features and functionality.

The Versa ZT-LAN solution eliminates the need to deploy dedicated firewall appliances. A full security stack is available in each secure Ethernet switch, secure WLAN AP, and ZT-LAN appliance.

Layer 3 and Layer 4 through Layer 7 functions are applied inline with the platform. Layer 3 and Layer 4 security functions include trusted and untrusted zones, and Layer 7 security functions are applied to manage application and URL traffic. In addition, Layer 4 through Layer 7 and ZT-Edge functions are deployed close to the user for reduced latency and better performance.

UTM security functions scan payloads and secure the against malware and vulnerability exploit attacks in the north-south and east-west directions.

LAN Capabilites on ZT-LAN Platforms

The Versa ZT-LAN solution provides standards-based, multivendor interoperability that is tested and verified to eliminate vendor-specific lock-in. It comprises a comprehensive stack of Layer 2 and Layer 3 features, ACLs, and QoS implemented on LAN platforms and leverages hardware offload engines for wire-rate ZTNA enforcement and microsegmentation. Stateful functions running in the Versa Operating System™ (VOS™) are embedded in the platform, and stateless functions operate at wire-rate on LAN switches and access points. In addition, specialized hardware complexes seamlessly integrate with VOS via SDKs.

The Versa ZT-LAN solution provides the following comprehensive LAN capabilities:

- Access, trunk interfaces
- Access control lists (ACLs)
- Bridge domain
- EVPN control plane
- Integrated routing and bridging interfaces (IRB)
- Layer 3 protocols
- Link aggregation (LAG), split LAG
- Link Layer Discovery Protocol (LLDP)
- Multi-active
- Passive loop detection

- QoS
- Virtual switch
- VLAN manipulations
- VXLAN overlays on/off-ramp
- xSTP

Security Capabilities on ZT-LAN Platforms

The Versa ZT-LAN solution provides the following security capabilities:

- 802.1X
- Device ID and fingerprinting
- DNS security
- DOS protection
- IP feeds and filtering
- Lateral movement protection
- Malware protection
- NG-firewall (NGFW)
- NG IPS
- Predictive analysis
- Secure proxy, proxy chain
- Security policies
- SSL/TLS proxy
- Stateful Firewall
- URL feeds and filtering

Advanced Access Control

Advanced access control policies determine how devices are admitted to the network and include both clientless and client-based options. The Versa Secure Private Access (VSPA) client supports on-premises ZTNA functions. The VSPA client finds the nearest VOS instance through control-plane exchanges, identifies the right set of policies for the user, and applies them.

Clientless Access Control

802.1x alone is no longer sufficient to provide network access control. New LAN environments need to use additional techniques, such as device fingerprinting and user and group access control, which are all provided in the Versa ZT-LAN solution, as follows:

- 802.1x provides the following capabilities:

    - Ability to place clients in respective microsegments
    - Certificate-based client device authentication
    - RADIUS-backed rich interoperability options
    - Single-supplicant, multiple-supplicant profiles per port
- Device fingerprinting (Dev-ID) adds the following capabilities:
    - Inline analysis of traffic flows for IoT, corporate, and BYOD devices
    - Device fingerprint data base, Layer 2 through Layer 7
    - Low-latency, rule-based engine
    - Matches based on a device's class for the consumption of policies, analytics, etc.
- User and group access control adds the following capabilities:
    - Captive portal or passive/inline user authentication
    - Network access criteria, user policies based on user and group credentials
    - User authentication via common IDP services or via the Enterprise’s own Active Directory
    - User group policies

Client-Based Access Control

In client-based access control, a client—such as the VSPA client—creates a detailed on-premises-based ZTNA profile for any device requesting access to the network. The client reports this information to the nearest VOS device, which applies the appropriate access and security policies based on the device's security posture. The client can be running on the Windows, MacOS, ioS, Android, or Linux operating systems.

Client-based access control includes the following capabilities:

- Facilitating connectivity and end-device profile checks
    - Connects to the nearest on-premises VOS instances
    - Performs user and device authentication
- Endpoint (device) Information Profile (EIP) selection based on:
    - Antivirus engine version, signature data base version running on the endpoint
    - Compliance check
    - Disk encryption and other parameters
    - Operating system type and version, security patch versions
    - Policy application starting from client devices
    - Traffic steering via SASE client
    - Whether a device is a corporate asset or a personal device
    - Whether or not specific software is installed
- EIP-based policy enforcement:
    - Implemented on the nearest VOS platform
    - Inline, high-performance traffic processing
    - Managed via network and security policies

- Reported to Versa Analytics

The same VSPA works remotely using a tunnel to the Versa Cloud Gateway. VOS in the cloud applies the policies and allows the device to connect. When used on-premises, the same client works in a tunnel-less mode due to it being on a trusted network. The VOS device applies the policies without using a tunnel, although you can use a tunnel if desired.

Multitenancy and Microsegmentation

Multitenancy and microsegmentation policies provide the complete separation of each tenant's traffic, applications, and devices across management, control, and data planes.

Microsegmentation across nodes reduces security risks and increases resilience by providing the following capabilities:

- Mapping of LAN overlays across the WAN
- Organization-level separation, including VRF, VPN, virtual switch, IRB, and Layer 4 through Layer 7 services
- Use-case-level management separation: security for LAN, WAN, and WLAN administrators, and for operational roles
- VXLAN overlays across ZT-LAN nodes to extend multitenancy in the campus

Policy Engine

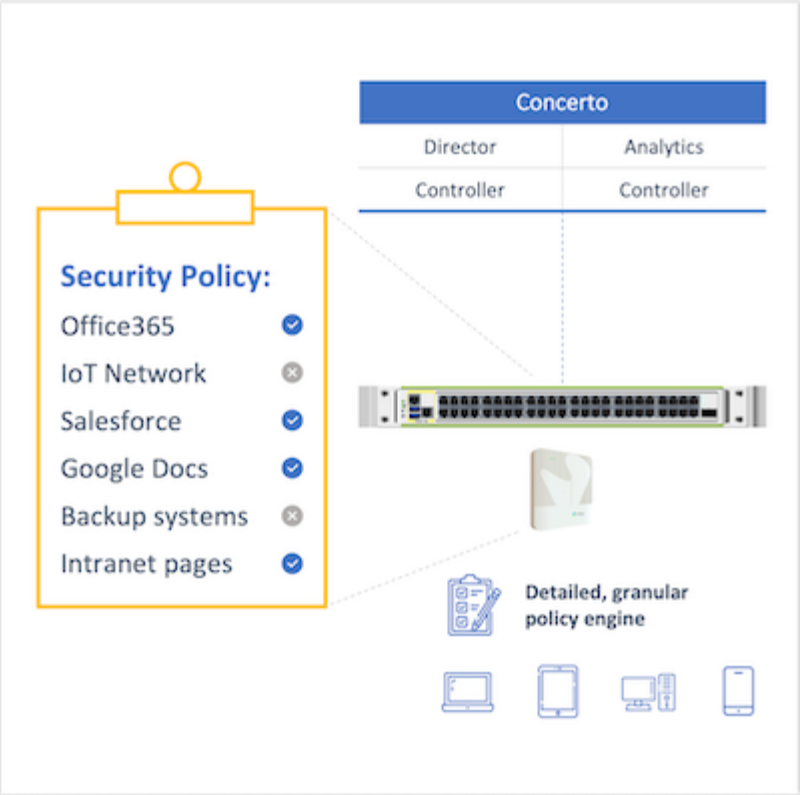
The Versa ZT-LAN policy engine operating in Layer 3 through Layer 7 allows you to create flexible policies to trigger match conditions based on the following:

- Applications (protocols)
- Filtered applications and grouped traffic classes with predefined default actions
- URLs and URL categories (Enterprise applications)
- Events, context, logs, etc., based on location (allow, disallow)

Policy options allow, block, rate-limit, and classify network traffic based on application identification and user-defined policies. Risk-based traffic management allows you to create user policies to control user access to all segments of network.

The following figure shows an example of the policy engine applying a security policy to user traffic, allowing or denying access to certain applications and network segments.

Updated: Wed, 23 Oct 2024 07:32:27 GMT

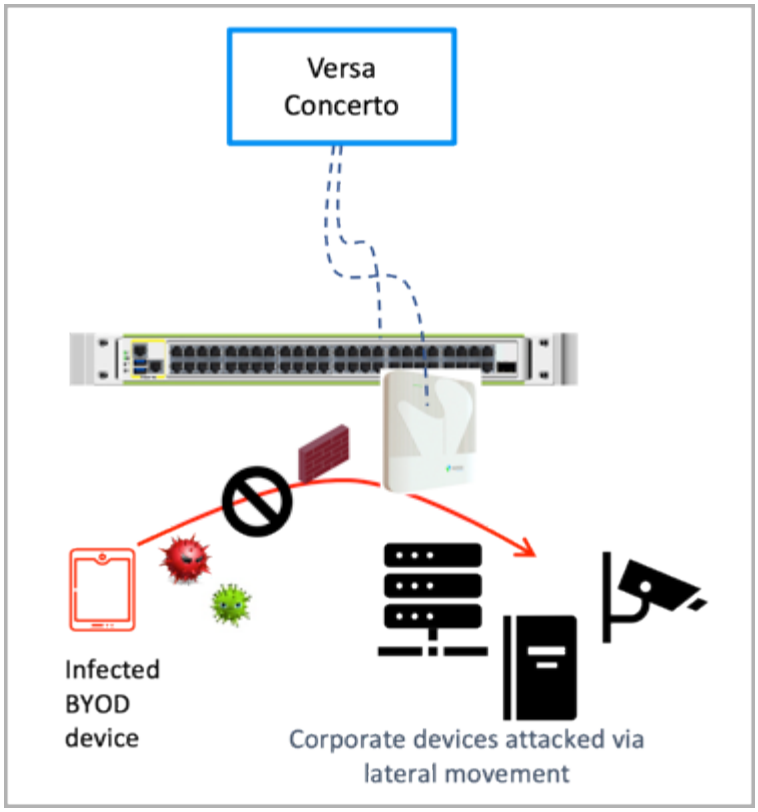


Lateral Movement Protection

Lateral movement is a technique that allows attackers to move progressively through a network, searching for key data and assets. A lateral movement attack typically consist of the following actions:

1. Initial infiltration of the network
2. Discover, identify, and inventory attack targets
3. Modify data, restrict or deny availability of data, exfiltrate data

The following figure shows an example of a lateral movement attack inside a LAN network that was initiated from an infected employee device.



The Versa ZT-LAN solution's lateral protection to detect and prevent lateral movement includes:

- Extended IPS threat library
- Extended malware signature base to detect binaries used for lateral movement
- Inline traffic inspection to identify the activities typical to ransomware and malware, as well as activities seen by commonly misused tools

Single Pane of Glass

The Versa ZT-LAN solution features the Versa Concerto Orchestrator to provide an on-premises or cloud-based management portal to design, deploy, and operate ZT-LAN implementations. This single-pane-of-glass management portal provides the following capabilities:

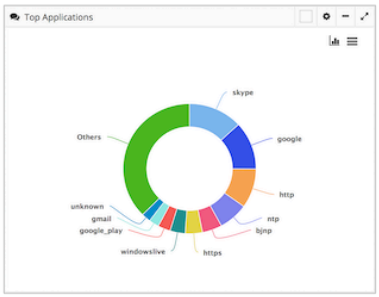
- Centralized policy management and enforcement
- Can be integrated with cloud management systems, such as:
  - Automated AWS and Azure
  - VMware, OpenStack, Docker
- Device, security, and service monitoring
- Hierarchical multitenancy with role-based access control (RBAC)
- Service orchestration and management (Versa and validated third-party VNFs)

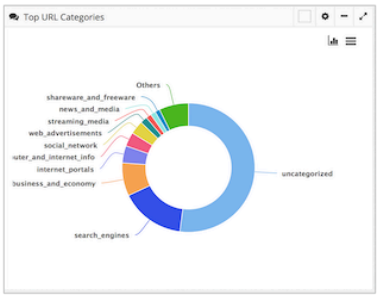
- Third-party API integration

ML/AI-Based Insights with Versa Analytics

Versa Analytics provides behavior analysis and predictive networking, including the following:

- Application and application-performance traffic analysis
- Big-data AI/ML-based analytics
- IPFix- and Netflow-based traffic flow reportingReporting of SD-LAN topologies
- Near real-time traffic information
- Per-user and per-group traffic analysis
- Strong multitenancy and RBAC





Additional Information

ZT-LAN Architecture
ZT-LAN Overview