WHITE PAPER

Modernizing campus network architecture with Versa SD-LAN and ZT-Prem

Why Legacy Campus Networks Architecture Don't Work for a Digital Enterprise?

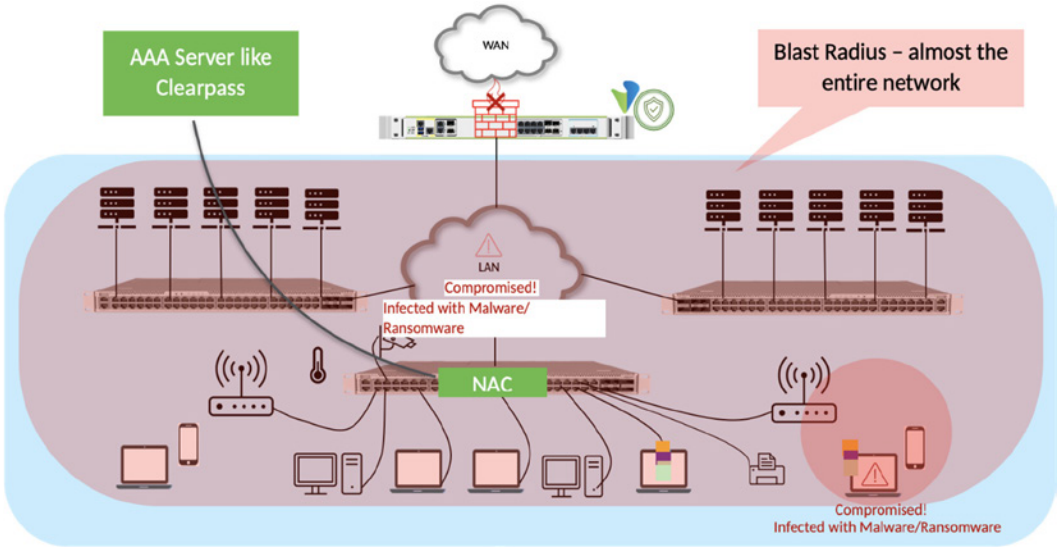

Figure-1 - Legacy Campus Network Architecture

Legacy campus network architectures were designed for an era where users were connecting to applications within local or remote data centers. The architecture was built with proprietary Layer 2/Layer 3 switch appliances and had to be refreshed every few years. Many complex and failure prone proprietary technologies like Virtual Chassis, Multi Chassis LAG, Fabric Path, ISSU are deployed which creates vendor lock in and increases the capital and operational expenses significantly. Various bolt-on approaches were used for security enforcement - in LAN access, WAN edge, and data center - using different solutions from vendors. 802.1x or Network Address Control (NAC) with external RADIUS servers were commonly deployed to authenticate and provide static, unfettered access to any resources on the network the user had access to.

These architectures are no longer sufficient to meet the needs of a digital enterprise for hybrid users and devices to connect to workloads in data center, private cloud, and public cloud. Legacy networks are not intelligent enough to adapt to the traffic pattern and apply policies, have inconsistency in configuration, are cumbersome to manage and use sub-optimal paths with serious security gaps. This results in sub-optimal network design for the new traffic types and traffic patterns with security loopholes, increased customer traffic latency, higher capex and operational expenses. In addition, legacy NAC has significant security shortcomings. As shown in figure 1, when an infected device gets connected to the LAN, it can infect the whole network that the device has access to.

Why is there a need for new thinking in Campus Architecture?

Traditional campus network architectures have been challenged by several changes in the IT landscape:

- **Hybrid work:** Hybrid and remote work styles are more pervasive, creating opportunities for zero trust network access (ZTNA) products to disrupt long-standing on-premises campus networking security technologies like NAC. Remote workers do not want different experiences when working remotely or within corporate locations (such as loading SASE clients or authenticating differently).

- **Increasing Device Diversity:** With the growing adoption of IoT devices, BYOD (Bring Your Own Device) policies, and edge computing, the number and types of devices connecting to campus networks have dramatically increased. This requires a new network design to manage, secure, and provide quality service to all these varied devices.
- **Rising User Expectations:** Today's users expect seamless, high-quality network experiences. They anticipate reliable, high-speed connectivity, whether they are using video conferencing, accessing cloud services, or streaming multimedia content.
- **Security Threats:** Cybersecurity threats have grown in number and sophistication, requiring more robust security measures. Traditional perimeter-based security models are no longer sufficient. Instead, a zero-trust security model, which assumes the network is always under threat and verifies every connection, is becoming the new norm. Today, many organizations are paying twice for their network security – once for onsite users protected by a perimeter-oriented NAC solution, and a second time for remote users using a zero trust network access approach.
- **Increasing Network Complexity:** Traditional campus network architectures can struggle to cope with the complexities of modern networks, which may include cloud services, virtualization, AI-based services, and more.
- **Fragmented Infrastructure:** Most networks incorporate a number of standalone products, each with its own separate management and policy engine. Multiple management consoles with limited or no integration between them, combined with policy managed in multiple places increases the likelihood of inconsistency, network errors, and security gaps. On top of this is the added challenge of troubleshooting across multiple consoles when issues arise.
- **Scale and Agility:** As organizations grow or their needs change, they require network architectures that can scale efficiently and quickly adapt to new requirements.
- **Data Growth:** The surge in data creation and consumption demands networks that can handle high volumes of data traffic, often in real-time. This is particularly true in a campus setting with dramatically increased usage of video collaboration tools.
- **Digital Transformation:** Many organizations are undergoing digital transformation initiatives to improve efficiency, collaboration, and customer experiences. These initiatives often require rethinking and redesigning network architectures.

Novel approaches like software-defined networking, zero trust, and the application of AI and machine learning for network management are emerging to address these challenges. These technologies aim to provide better network visibility, control, security, and automation, enabling networks to be more responsive and adaptive to business needs.

Is NAC the right model for the new campus network architecture?

Network Access Control (NAC) is an approach to network security that seeks to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication, and network security enforcement. In a modern campus architecture, however, there are several challenges and limitations associated with NAC:

- **Perimeter-based Security:** NAC relies on securing the network's perimeter and granting access based on policies. However, once inside, devices often have broad access to network resources, which can be exploited if a device is compromised.
- **Lack of Micro-segmentation:** Traditional NAC solutions might not provide enough micro-segmentation to prevent lateral movement in the network if a breach occurs. This means if one device gets compromised, the intruder might have access to vast parts of the network.
- **Device Diversity:** The growth of Bring Your Own Device (BYOD) practices and the Internet of Things (IoT) presents challenges to NAC. These devices, which might not be fully secured or even recognizable by the NAC system, increase the risk of network security breaches.
- **Cost:** NAC solutions can be expensive to implement and maintain. The cost isn't just in the form of purchasing and installing the software but also includes the ongoing cost of managing and updating the software and hardware.
- **Lack of Flexibility:** Traditional NAC solutions can lack the flexibility to accommodate the dynamic nature of modern networks, including cloud-based services and remote working scenarios.

Considering these challenges, some organizations are moving towards more flexible, identity-centric models of network access control, which use the principles of zero-trust networking and focus on authenticating and authorizing individual users and devices, rather than trying to secure entire network segments.

How do current ZTNA offerings fit into the campus network?

Zero Trust Network Access (ZTNA) is an emerging security concept primarily targeted at remote users, not campus users. While some ZTNA vendors do offer support for on-premises workers, it's evident that few of these offerings are tailored, focused, or optimized for campus or branch environments. This lack of focus might be due to the inherent network connectivity differences between remote locations and corporate locations.

For instance, campus or branch locations are usually "on-net", which means they are on the corporate LAN and inherently connected at the IP layer. In contrast, remote workers are inherently "off-net" and must initiate a client or authenticate to a browser-based portal to access internal corporate services. These fundamental differences call for unique considerations and optimizations in the design and implementation of ZTNA solutions.

Moreover, current ZTNA offerings may lack broad protocol support, particularly service-initiated data center services like Microsoft SCCM/ECM. These systems often require access "in" to campus or branch devices, while the ZTNA connectivity model is primarily designed for users to reach "out". This discrepancy presents a challenge for traditional campus and branch network setups.

In addition to these challenges, ZTNA solutions do not typically support headless devices such as IoT or OT devices often found in campus or branch locations. These headless devices do not have a human user or a client software agent that can initiate a ZTNA connection, making them unsuitable for typical ZTNA security models.

Another potential challenge is the issue of hairpin routing, where local traffic could end up taking a longer, roundabout path (like a "trombone" or a "hairpin") to the edge of the campus network or cloud security points of presence. This could lead to congestion, increased latency, and performance challenges that could impact user experience.

Lastly, implementing current ZTNA offerings in a campus or branch environment might necessitate changes to the network topology and routing. This can complicate implementation, requiring suppliers to engage with multiple teams to successfully integrate ZTNA into existing network architectures.

The Future of Campus Architecture: Zero Trust Everywhere

The future of campus architecture is set to embrace a Zero Trust model that effectively addresses the evolving challenges of network security. This forward-thinking model supports server-initiated traffic and all campus protocols, thus enabling greater flexibility and functionality. It also incorporates support for headless devices and a growing array of IoT and OT devices, which are becoming increasingly prevalent in today's network environments.

Crucially, this approach eliminates the need for tromboning or hairpinning from WAN Edge or Cloud POPs, a practice that can cause congestion, latency, and performance challenges. This model also circumvents the need for network topology routing changes, simplifying network management and reducing potential disruption.

A significant advancement offered by this approach is the use of adaptive micro-segmentation. Based on an entity's risk score and device posture, this software-based feature allows for more dynamic and responsive network security, encapsulating the principles of a true Zero Trust Architecture for campus environments.

Importantly, this model applies a single management platform and security policy that spans both remote and campus workers, ensuring consistency in security enforcement regardless of location. It results in a common experience for end users, whether they are working remotely or on-premises, fostering consistency and ease of use.

The unified approach leads to simpler troubleshooting, removing the complexity of dealing with multiple solutions. From an economic and efficiency standpoint, using one solution for two use cases (remote and on-campus worker secure network access) is a beneficial strategy.

This approach taps into the power of Artificial Intelligence and Machine Learning to create a secure predictive campus network architecture. This allows for proactive identification and mitigation of potential security threats, enhancing the overall security posture of the campus network.

Lastly, Zero Trust Everywhere will result in reduced insider threats and limited infection blast radius. According to Gartner, “Extending ZTNA products to campus environments creates several benefits for enterprises, including security gap elimination, unified policy, enhanced visibility, simplified operations and modernized pricing models.[1]“

[1] “Hype Cycle for Zero Trust Networking, 2023”, Gartner. July 2023

What is Versa's approach to Modernize this architecture?

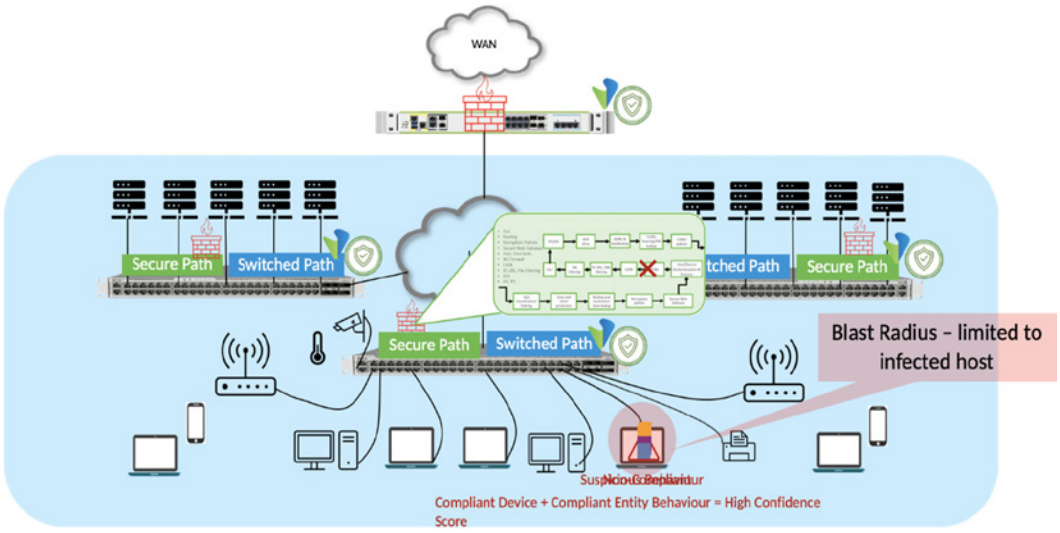

Figure-2 - Modernizing Campus Network Architecture

Versa's Zero Trust Everywhere platform provides Zero Trust Network Access (ZTNA) for both on-site and remote users and devices through a unified policy framework. Breaking new ground in the field, Versa has expanded the application of ZTNA to include on-site operations at branches and campuses, resulting in what is called ZT-Premise. Furthermore, Versa integrates policy enforcement directly within a secure software-defined LAN (Versa SD-LAN), paving the way for a true Zero-Trust LAN. This advanced LAN model incorporates next-generation security services within each switch. The activation of these services is determined by the security posture of the individual device or user, thus providing a tailor-made security environment.

The following are the key elements of the Versa solution.

1. Security policies are applied as close as possible to the user or device.
2. Security policies are applied for both inter and intra VLAN traffic.
3. Supports IoT and OT devices.
4. Software Defined Adaptive Microsegmentation.
5. Does not require any changes to network topology or protocols.
6. Seamless integration with other Versa campus technologies
7. Single pane of glass for management and visibility
8. ML/AI powered network analytics and security.

1 – Security policies applied as close to the user or device

As shown in figure 2, Versa has redefined the approach to where the security policies are enforced. The solution enables ingress network traffic to go through the full security stack as close as possible to the user in a distributed manner rather than just at a WAN edge or Cloud firewall device. It is applied in the network element where the user traffic first ingresses the network, which is either the WIFI AP or Switch in most cases.

2 – Security policies applied for both inter VLAN and intra VLAN traffic

With Versa's approach, security policies can be enforced for both E/W and N/S traffic instead of N/S traffic alone. This allows malicious lateral movement to be stopped or contained as soon as the infected user or device connects to the network. E/W traffic can be either inter or intra VLAN and policies can be enforced for both.

3 – Supports both intelligent and headless devices

Versa's solution supports traffic analysis from intelligent endpoints like laptops, desktops, servers, etc., and headless endpoints like printers, cameras, and VoIP phones. The Versa Client can be installed on intelligent endpoints to get device posture information, including device type, operating system, registry details, host AV software status etc. It can assign the user/device to a segment based on software-defined policies, and supports importing data from other vendor security managers like Palo Alto Panorama etc. Headless devices are supported using the Versa device fingerprinting solution embedded in the switches. Traffic from headless devices is continuously monitored and fingerprinted to identify the device details like device type, vendor, operating system etc., and assigned to the appropriate microsegment segment based on user-defined policies.

4 – Software Defined Adaptive Microsegmentation

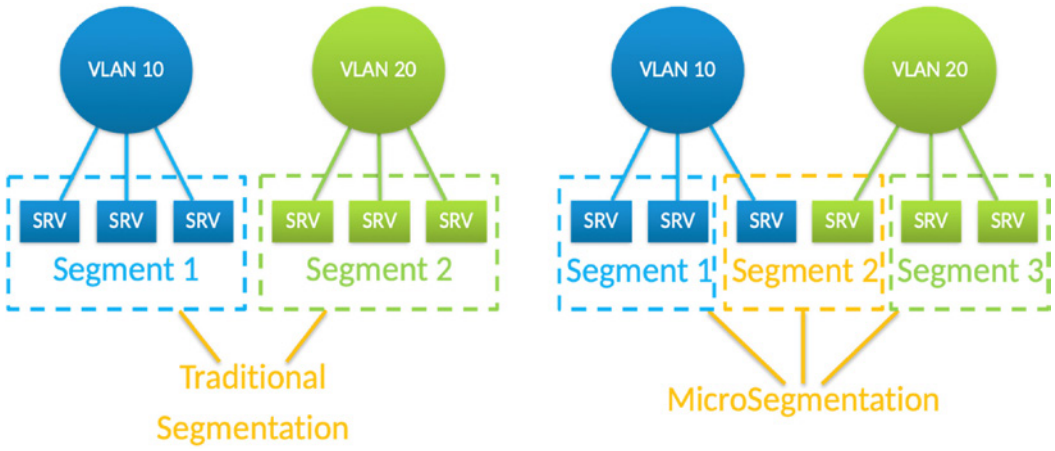

Figure 3 Segmentation Vs Microsegmentation

Traditional network elements support segmentation in various forms like VRFs, Tenants, Virtual Switches and VLANs. With Versa solution, each VLAN can be further divided into multiple more granular microsegments as shown in Figure 3. Each of these segments can be defined with its own control plane and forwarding plane policies. By default, forwarding across microsegments is blocked and the user can define policies for inter-microsegment forwarding. Microsegmentation helps in reducing blast surface, enable dynamic vulnerability confinements and simplified policy management.

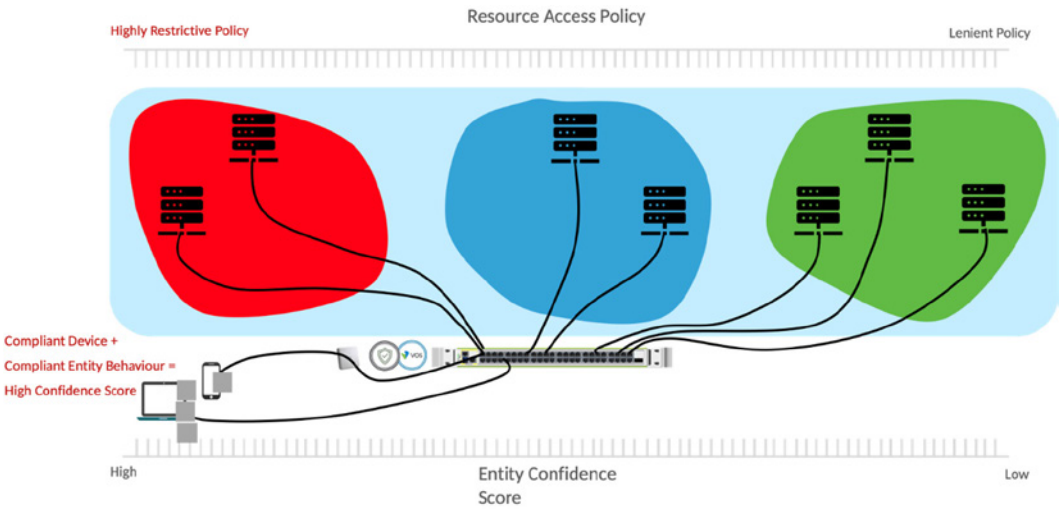

Figure 4 Adaptive Microsegmentation based on end point confidence score

Versa's solution reduces the blast radius using Software Defined Adaptive Microsegmentation based on the endpoint confidence score of clientless devices (including headless IoT devices), or endpoint posture information for devices using the Versa client application or some other vendor's client application. When an end point's confidence score or security posture changes, VOS (Versa Operating System) switches will learn that information on the fly, and the device or user will be moved to an appropriate microsegment commensurate with the risk it poses and its own set of security policies to access resources. If the security posture of the device is not meeting expected standards, it can be moved from a microsegment that allows access to sensitive applications and data (like the green microsegment as pictured), to a microsegment with more restrictive resource access policies like the red microsegment shown in figure 4. In the case of a degraded security posture, traffic is taken through a slower "secure" CPU path for applying Nextgen firewall security policies like IP/URL/File filtering, IDS, IPS, AV etc., instead of the fast ASIC path. This "secure path" can also apply more advanced features like DLP (Data Loss Prevention), malware sandboxing, etc. All security services are applied inline in a single pass architecture, and traffic does not have to trombone from the WAN edge or the cloud gateways.

Every switch or access point in the LAN is running VOS™ (Versa Operating System), which combines L2/L3 switching with an integrated next generation firewall which can handle the security requirements of the traffic entering that device. This on-premise ZTNA distributed firewall-on-a-switch architecture scales well and reduces traffic latency by eliminating the traffic hair-pinning to apply security services on a cloud security PoP.

5 – Does not require any changes to network topology or protocols.

Versa's solution forms a fungible fabric that is 100% compliant to EVPN-VXLAN standards, so it can accommodate other vendor network elements with EVPN-VXLAN support also in the fabric. VXLAN-EVPN fabric can dynamically grow or shrink and is proven to scale well in large data centers. It also supports multihoming and efficient link utilization using underlay routing. It eliminates the need for complex legacy technologies like Virtual Chassis, MC-LAG, Fabric Path, ISSU etc., which are proven to be failure prone and difficult to manage. Versa switches support Zero Touch Provisioning and extensive LAN capabilities like xSTP, EVPN-VXLAN, Virtual Switch, Bridge domains, Multi tenancy, traditional NAC using 802.1X, VLAN translation, hair pinning,

passive loop detection, mac limiting, BUM traffic suppression, DHCP snooping, IP source guard, Spoof device detection etc. To protect the existing LAN network infrastructure investment, Versa builds a secure SD-LAN overlay fabric on top of the existing LAN network and offers the similar benefits of a greenfield deployment.

6 – Integration with other Versa Campus and Cloud Solutions

Versa ZT-Prem can be a standalone solution with its own headend. It also seamlessly integrates with Versa Secure SDWAN, SASE and SSE solutions offering end-to-end secure infrastructure for a hybrid workforce. The same VOS and Versa Head End across all Versa products reduces the learning curve and thereby saves operational expenses.

7 – Single pane of glass for management and visibility

Like any other Versa solution, Versa control and management systems are used for provisioning and management of this solution. The same control and management system can manage all Versa WAN and LAN devices. Common security policies are pushed to all Versa nodes which significantly reduces the operational complexity of provisioning and managing the campus networks. Operators can reduce their operational cost significantly by having the single headend managing their WIFI APs, LAN switches, WAN edge router, on-premise firewall and cloud firewall devices. Versa's innovative approach also decreases CAPEX by reducing the network device footprint and power consumption by providing a single head end to manage the whole campus network infrastructure and by consolidating the switching, security and SD-WAN features in the same network appliance.

8 – ML/AI powered network analytics and security

Versa Machine learning and artificial intelligence capabilities provide network prediction, intelligent alerting (alarm compression), performance optimization (path selection, application user experience), security and anomaly detection, automated remediation, and capacity planning. Versa's AI/ML solutions include:

- **Versa Verbo:** The Natural Language Processing (NLP) based Versa Chatbot.
- **Versa Advanced Network Insights (VANI):** Machine learning core for network anomaly detection and network prediction.

Versa AI/ML facilitates the interaction of various components with the Versa ecosystem.

Conclusion

Versa's solution is paving the way for a future of Zero Trust Network Access in Campus networks, where Network Access Control (NAC) evolves into a Zero Trust Everywhere framework. Versa's innovative Campus architecture aims to deliver a self-managed, self-healing network, transforming the landscape of Campus network design, security and management.

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