VERSA
NETWORKS

WHITE PAPER

Modernizing the Corporate Campus Network Architecture

March 2024

Table of Contents

Challenges to the traditional campus network architecture

Legacy campus network architectures were designed for an era when users connected to applications hosted in 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 were deployed, creating vendor lock-in and increasing the capital and operational expenses significantly. Various bolt-on approaches were used for security enforcement – in LAN access, WAN edge, and the data center – using different solutions from vendors. 802.1x or Network Address Control (NAC) with external RADIUS servers was 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 with hybrid users and devices connecting to workloads alternately in the data center, private clouds, and public clouds. Legacy networks are not intelligent enough to adapt to the traffic patterns and apply desired 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, and higher capex and operational expenses. In addition, legacy NAC has significant security shortcomings, including when an infected device gets connected to the LAN, there is no compartmentalization – it can infect the whole network that the device has access to.

A changing IT landscape

The challenges to legacy campus network architectures from a changing IT landscape include:

- **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 (such as loading SASE clients or authenticating differently) when working remotely or within corporate locations, and especially when constantly switching between the two.
- **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.

Limitations of the NAC approach

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 microsegmentation:** Traditional NAC solutions might not provide enough microsegmentation 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 lack the ability 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.

Considerations with ZTNA offerings

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 the 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 advance offered by this approach is the use of adaptive microsegmentation. Based on an entity's risk score and device posture, this software-based feature allows for more dynamic and responsive network securit, with the added benefit of reducing insider threats and limiting any possible infection blast radius.

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. The unified approach also 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.

Finally, this approach taps into the power of artificial intelligence and machine learning to create a secure predictive campus network architecture, allowing for proactive identification and mitigation of potential security threats, enhancing the overall security posture of the campus network.

About Versa Networks

Versa Networks, the leader in single-vendor Unified SASE platforms, delivers AI/ML-powered SASE, SSE and SD-WAN solutions. The platform provides networking and security with true multitenancy, and sophisticated analytics via the cloud, on-premises, or as a blended combination of both to meet SASE requirements for small to extremely large enterprises and service providers.

Thousands of customers globally with hundreds of thousands of sites and millions of users trust Versa with their mission critical networks and security. Versa Networks is privately held and funded by Sequoia Capital, Mayfield, Artis Ventures, Verizon Ventures, Comcast Ventures, BlackRock Inc., Liberty Global Ventures, Princeville Capital, RPS Ventures and Triangle Peak Partners.

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