nile | SOLUTION BRIEF

VLAN-Free Campus Zero Trust

The Prevention of Lateral Movement Initiated Attacks

Organizations today face mounting security challenges from controlling network access and protecting sensitive data to defending against zero-day exploits and advanced malware. At the same time, they must strike a balance between robust security, operational efficiency, and seamless end user experience.

The growing use of Internet of Things (IoT) presents an additional challenge due to their provable security inefficiencies, such as hardcoded or weak passwords and outdated software protocols that are easily exploitable. As a result, IoT devices represent a particularly alluring target for threat actors aiming to move laterally and create persistence within any network.

Owing to insufficient network segmentation, inadequate access controls, poor traffic visibility, and emerging threats, lateral movement within a **VLAN-based network** poses significant security risks. Attackers exploit the weaknesses of flat network architectures, **moving undetected across networks** and expanding their reach undetected.

The VLAN "trust and verify" model has several critical weaknesses that can be exploited by attackers for lateral movement within a network. Here are five key vulnerabilities:

1. Lack of Segmentation & default Isolation

- Traditional VLANs depend on **static segmentation**, often grouping multiple devices within the same broadcast domain using manual or complex NAC placement rules. Once attackers gain access, they can **move laterally** across the VLAN without further inspection.

2. Weak Access Control & Excessive Trust

- VLANs typically require add-on NAC solutions to grant devices necessary privileges. An **implicit trust model** allows infected or compromised devices to interact freely with critical assets.

3. VLAN Hopping & Spoofing Attacks

- Exploiting misconfigured VLANs or weak trunking protocols (e.g., VLAN hopping attacks) to bypass network boundaries, along with **MAC spoofing** or **ARP poisoning**, allows unauthorized devices to impersonate trusted assets.

4. Challenges in Identifying Threats

- Traditional VLANs focus on very broad network segmentation rather than behavioral monitoring, and a **lack of deep packet inspection** allows attackers to blend into legitimate traffic patterns.

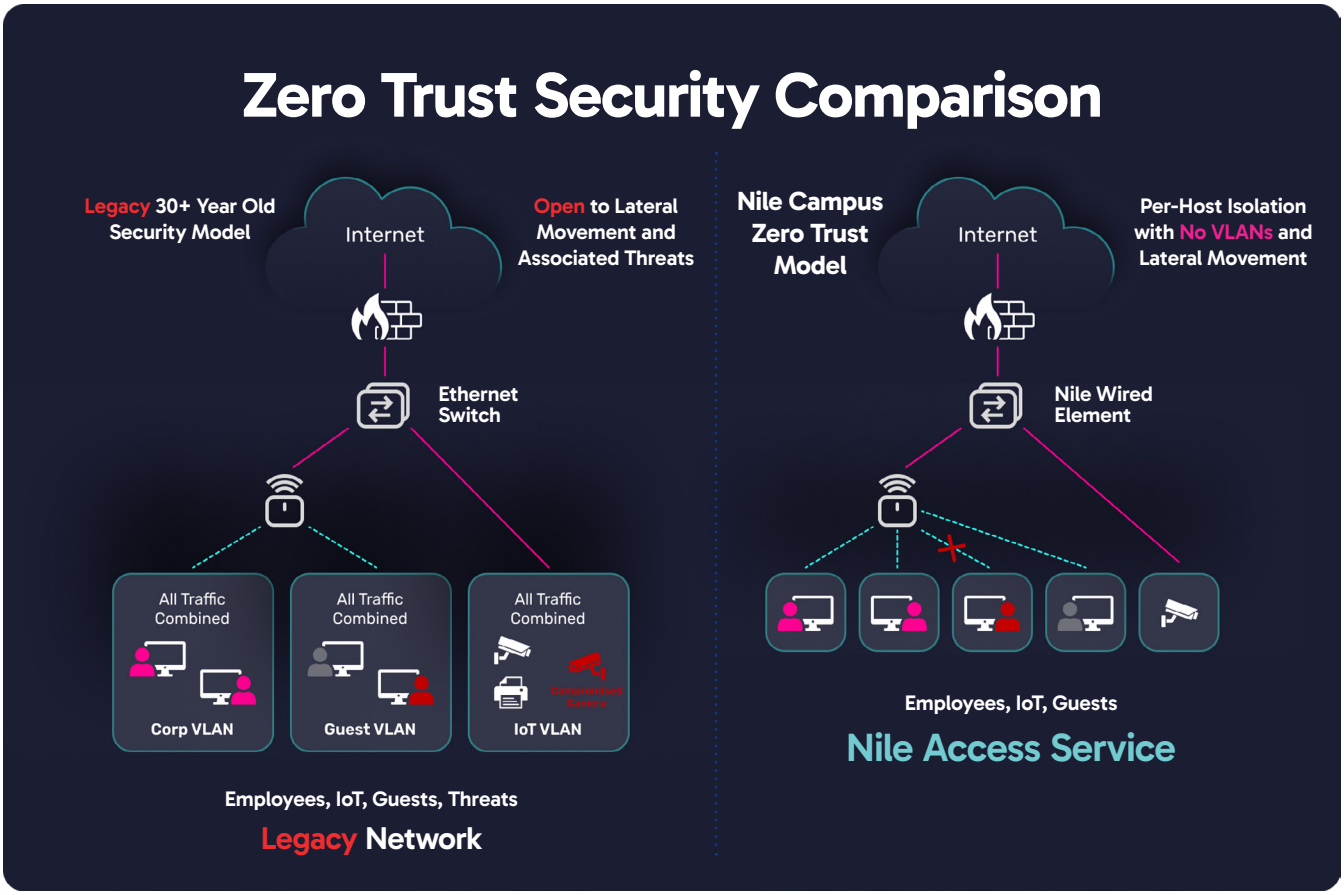
5. Ineffective Threat Containment

- Once **malware or ransomware** infiltrates a VLAN, it can spread rapidly to all devices, making threats difficult to identify a compromise. Per recent IBM data, the average time to identify a breach (which often includes malware detection) is around **277 days**.

Unfortunately, the majority of wired and wireless network solutions sold today rely on decades-old VLAN principles. To circumvent the issues described above, a combination of network access control (NAC) appliances, comprehensive software and hardware upgrades, and distributed gateway components are required to appropriately segment devices onto the network. The complexity alone often makes microsegmentation or dynamic segmentation unachievable.

What is Lateral Movement?

Within the cyber kill chain and MITRE ATT&CK frameworks, Lateral Movement is defined as any activity that allows adversaries to progressively move deeper into a campus network in search of high-value assets. Oftentimes, an attacker's goal is to remain in the network as a Advanced Persistent Threat (APT), to reach as much data as possible.



Nile Trust Service – Stronger Security, Less Complexity

Organizations now have access to a modern Zero Trust approach to campus and branch network and device security where endpoints are completely isolated by default using next-generation security practices. Traffic from each endpoint is isolated and encrypted all the way to your selected enforcement point, such as a firewall, SSE solution, or gateway. This completely eliminates the risk of a breach expanding beyond a single device.

The Nile Access Service then includes an innovative framework for Zero Trust security that leverages new principles, providing Layer 3 (L3) segmentation of all devices without VLANs, complicated ACLs, Spanning Tree attacks, and repetitive manual configuration tasks. Not only does this eliminate the need for AI to identify that a VLAN is missing when a switch is installed or replaced, adversaries can no longer sniff traffic or easily infect other devices connected to the same VLAN.

Nile's standardized cloud-based framework also allows for the unified distribution of policies without the introduction of complicated EVPN/VXLAN (Ethernet VPN-Virtual Extensible LAN) deployments, which are gaining popularity with legacy network vendors today.

The following principles are applied to mitigate lateral movement threats:

1. **Device Isolation:** The implementation of per-device isolation instead of VLAN-based trust models and static VLAN segmentation.

- Network access is determined by **user and device identity as well as role definition, rather than by grouping devices by VLAN.**
- Employee, guest, and IoT devices exist in the same network **but remain isolated** via a segment of one implementation.

The benefits include the elimination of VLAN sprawl, least-privilege access enforcement, and prevention of lateral movement.

2. **Campus Zero Trust Network Access:** Continuous verification of user and IoT devices before granting access that replaces any open VLAN or passphrase authentication.

- Per Zero Trust principles, every user and device **must be continuously authenticated and authorized** before accessing resources.
- Allows for multi-factor authentication (MFA), device health checks, and behavioral analytics to **grant or revoke** access.

Nile eliminates persistent access risks by ensuring every request is verified before granting network access.

3. **Layer 3 Segmentation with Deny by default:** Allows for the inspection of traffic and enforcement of policies per device without the need of complex VLAN-based ACLs (Access Control Lists).

- Policies are applied at the **user and device level**, not tied to static network configurations.
- **East-West Traffic Monitoring** to identify lateral movement attempts.

For enhanced protection, Nile allows organizations to better utilize firewalls, SSE solutions, and gateway enforcement points to identify malicious and persistent threats, like malware and ransomware.

Nile Campus Zero-Trust versus VLAN-Based Security Differentiation

Feature	VLAN-Based Security	Nile Campus Zero Trust
Security Model	Implicit trust and Default Allow model within VLANs	Continuous authentication & least-privilege access
Threat Containment	Porous segmentation with complex add-ons and network configurations	Real-time, automated micro-segmentation with “Segment of One” isolation and single device blast radius
Lateral Movement Prevention	Weak. VLAN hopping, Spanning Tree attacks, and other possible threat vectors	Eliminated. All traffic from each device inspected prior to forwarding per Isolation
Complexity	High, requires constant VLAN management and bolted-on complex NAC solutions	Built-in campus Zero Trust with dynamic policy enforcement via firewalls, SSE or gateway service

The Bottom Line

Moving beyond VLANs with campus Zero Trust principles enhances security, flexibility, and scalability by ensuring that every access request is verified, threats are contained in real time, and networks remain agile without manual VLAN management and third-party NAC complexity.

In summary, the very core of the Nile Access Service adheres to strict campus Zero Trust principles that are intended to simplify a network architecture while reinforcing campus and branch security.