Nile Trust Service For Wired And Wireless Threat Prevention

The Nile differentiation and simple steps that help you use Campus Zero Trust to protect your campus, branch, and remote users.

Introduction

Enterprise campus network security has historically been defined by a series of tradeoffs. Simply put, easy to manage flat networks gave attackers free reign to move laterally and cause damage without really being detected. On the other hand, more secure and tightly controlled Zero Trust network environments increased the cost, complexity, and effort required to meet evolving threats, services, and user behavior.

Ultimately, organizations that ventured into expensive security projects left IT teams overworked and a network that fell well short of the ideals of what Zero Trust promised. One problem is the continued use of older technology within the LAN architecture by legacy network vendors that does not hold up to today's sophisticated ransomware and cybersecurity threats, and user demands.

Nile has redesigned the enterprise network so that Zero Trust principles and advanced segmentation techniques are built-in by default, eliminating expensive add-on projects. Unlike traditional approaches based on outdated technology with layered security on top to make up for inadequacies, Nile gives organizations a new, secure foundation to build off of that improves their overall security posture and compliance. Campus network security is no longer your weakest link.

In this paper, we introduce the key principles of Nile's comprehensive Campus Trust Service offering and how this translates to more efficient and effective enterprise-class security.

A New Network Architecture Designed for Security

Nile was founded on the concept of making enterprise connectivity as simple and safe as turning on the lights. This required a foundational redesign that makes security an integral part of the network, not an afterthought. While a great deal goes on under the hood, we started with some fundamental changes to protect against external and internal threats. The following will help you understand where we've addressed some legacy issues:

- Secure network infrastructure
- Segmentation and the isolation of devices
- Encryption of all traffic within the network
- Enhanced authentication and policy enforcement (on-premises and cloud)

> Ransomware and insider threats have quickly become the most prominent and visible types of security risks today. A recent example is a March 2024 ransomware attack on Belgium's Duvel Moortgat Brewery by the Stornomous ransomware group, wherein 88 gigabytes of data were stolen, causing production to come to a standstill.
>
> From an insider threat perspective, 70% of organizations attribute either technical challenges or cost as the primary obstacles preventing them from implementing effective insider threat management[1].

1. Cybersecurity Insiders, 2024 Insider Threat Report

A New Approach to Securing Network Infrastructure

The Hardware

It's still not uncommon to find people online asking if console ports on a switch or other network infrastructure create a security vulnerability. Some argue that physical access and authentication controls are a must, while others discuss how console ports have been circumvented in the past. You can also find others asking if Trusted Platform Module (TPM) chips are built into a vendor's access points or switches.

A network today should ensure that the underlying elements are secure – no excuses. Nile-designed network infrastructure completely removes the need to physically connect to it, allowing the removal of SSH, Telnet, or other remote services, which can be accidentally left open or exploited by attackers. In fact, there are no management or console ports that can potentially be abused by someone with malicious intent.

Every Nile network element contains a Trusted Platform Module (TPM) and a unique device certificate that is created during its manufacturing. As a result, each element can verify the integrity of its hardware, firmware, and software on every bootup. Nile infrastructure will not boot if it has been compromised or tampered with. Likewise, each wireless and wired element is uniquely tied to an individual Nile customer and will only work in that customer's environment.

The Software

With the idea of creating a new network architecture, Nile was free to focus on each device (access point, switch, etc.) and its most necessary services. Fewer services mean fewer opportunities for vulnerabilities. Likewise, each network device leverages Nile's custom-hardened OS where all network configuration is fully automated, removing the potential for human errors.

Common firmware versions across our wired and wireless devices ensure uniform security services and the ability to quickly patch any vulnerability. While not uncommon to see IT organizations wait for 10 months or longer to perform standard software upgrades, Nile is able to work with customers to automatically add features and fixes as needed, offering an enhanced security posture.

Segmentation and Per-device Isolation

The idea of segmenting a network has been around for a long time. In fact, we went from large flat networks to logically separated broadcast domains when VLANs were introduced over thirty years ago. The popularity of routers and ACLs (access control lists) then led to the idea of using VLANs to control access across domains as a security measure, which can be seen as the beginning of network segmentation.

This allowed IT teams to apply policies to different groups and devices across the network. Often, this led to big projects that included implementing network access control (NAC), dynamic segmentation, and VPN-based remote access solutions. Unfortunately, the issues associated with VLANs such as broadcast domain and DHCP attacks, lateral movement, and misconfiguration vulnerabilities remained.

A modern segmentation and isolation model

Nile's innovative secure-by-design campus Zero Trust architecture ensures that there are no blind spots in the network where attackers can sit and hide. We've eliminated the use of VLANs and provide customers with Layer 3 segmentation and per-host isolation on day one. The elimination of VLANs and lateral movement between devices offers a new level of ransomware and insider threat protection.

Connectivity is based on policies that can be equally applied to any device, whether wired or wireless. Each device is profiled, authenticated, authorized, and segmented based on its needs. Traffic is encrypted, and an enforcement point of the customers choosing evaluates each packet for threats and its intended destination.

In essence, Nile works with and enhances an organization's existing policies and security tools. These security solutions behave normally, enhanced with the ability to see a far more complete view of internal and external bound traffic, with the option to enforce far granular controls.

Just as importantly, Nile automatically handles the configuration needed to make this happen so that network and security teams can focus on higher-priority projects versus being bogged down with microsegmentation, VLANs, ACLs, and complex NAC-driven dynamic segmentation projects.

> Because VLAN-based networks lead to a situation that makes it difficult to identify a threat. IoT devices are particularly vulnerable as they typically lack any host-based protections and are considered east-west blind spots. The ability to eliminate lateral movement using per-host isolation and the tunneling of traffic not only limits the blast radius of an attack but also helps identify abnormal behavior more quickly as a firewall has greater visibility.

Encryption Of All LAN Traffic

In addition to securing each individual network element, all traffic between Nile elements is also encrypted and secure. High-end hardware ensures that once endpoint devices are connected, their traffic is also encrypted using MACsec (802.1AE) to ensure that it cannot be sniffed or modified regardless of user, device, application, whether on the wired or wireless networks. The elimination of VLANs and the addition of encryption throughout a deployment better protects against denial of service, man-in-the-middle, and other threats.

The ability for organizations to leverage bring your own key (BYOK) for Nile's cloud service ensures that our customers retain control and management of their encryption keys. From a data perspective, Nile cannot see a customer's actual data, which adds to an organization's security posture. All of this is something that is not easily achievable when working with traditional vendors due to cost and architecture considerations.

> Most wireless networks will likely implement a form of encryption for traffic over the air, but the same is not true once that traffic hits the Ethernet side of the network. Unencrypted traffic allows attackers to use man-in-the-middle (MiTM) techniques to sniff packets, steal data, and even capture login credentials in transit.
>
> 31% of all breaches over the past 10 years have involved the use of stolen credentials[2].

2. Verizon 2024 Data Breach Investigations Report

Zero Trust Authentication for Users and IoT

At the core of a campus Zero Trust implementation is the principle that no users or devices should be trusted by default and that everything must be verified before accessing a network.

From a user and IoT standpoint, different authentication methods are often used depending on the device type and security capabilities. While laptops and smartphones easily leverage more secure authentication protocols, IoT devices often lack strong security capabilities. Guest networks pose an additional challenge as users are joining open networks. These networks rarely utilize more than VLAN segmentation, ACLs, and acceptable use verbiage as controls.

In addition to very granular segmentation, the Nile Access Service supports an authentication structure that allows organizations to leverage existing RADIUS services, or a Nile provided RADIUS service, as well as MAC authentication for IoT, or utilize single sign-on (SSO) for both wired and wireless networks. Device fingerprinting also allows organizations to include the identity of IoT devices and other headless assets within the authentication and authorization process.

With the expanded use of cloud-based applications and access from anywhere, the use of SSO and multi-factor authentication (MFA) have become mainstream in an effort to streamline access management, enhance security, and improve user experience. Ultimately, this drives operational efficiency and productivity across the enterprise.

From an SSO perspective, built-in support for SAML (Security Assertion Markup Language), as well as SCIM (System for Cross-domain Identity Management) provides the ability for organizations to treat the network as a resource or service provider (SP). As customers shift from using RADIUS and complex NAC solutions, Nile offers the ability to leverage SSO for wireless access as well as wired connections, which is unique. The same can be said for the support of SCIM, specifically for organizations that require a centralized solution for managing and removing access to applications at scale.

Just as importantly, a periodic re-authentication is performed on each device to ensure that a user cannot walk into an environment and connect or plug into a wired port and gain access. Indicators such as changes to the MAC address, DHCP, HTTP, or a variety of other traits would trigger a re-authentication.

Enhanced Policy Enforcement

Nile's campus Zero Trust architecture ensures that all security features are applied across an entire deployment for every connection and exchange of traffic. As a result, enhanced authentication features with granular segmentation and device isolation enable organizations to better leverage policy enforcement tools, whether on-premises solutions or cloud based Security Service Edge (SSE) alternatives.

As all traffic is routed to a customer's firewall or SSE solution, this allows access policies to be enforced based on strict internal and external security and compliance requirements. With built-in device isolation, Layer 3 segmentation, and complete control of traffic inspection, organizations minimize the spread of malware, ransomware, and other threats more quickly, as unsuspecting lateral movement is no longer an issue.

The simple integration from the Nile Access Service with Nile Trust Service support for SSE also ensures that users receive a consistent or Universal Zero Trust connectivity experience regardless of where they connect, in the office, at home or on the road.

Putting It All Together

Managing a network and the associated security responsibilities is a big responsibility. For many organizations, the added burden of handling new AI related security threats, upgrading firewalls, NAC, SIEM, and a host of other other solutions has become a daunting task with no end in sight.

For one Nile customer, a network upgrade also provided an opportunity to deploy a new campus Zero Trust implementation that removed the need to manage VLANs in their corporate and branch offices and enhanced their security posture. This also delivered the confidence to offer guest access for the first time, as well as the ability to plan for new IoT/OT smart office projects.

Conclusion

For many, the built-in Nile Trust Service capabilities introduce a completely new way to deploy campus Zero Trust security and access control through the elimination of legacy network security complexity. Gone are VLANs, complex ACLs, and the need to add on intricate dynamic segmentation solutions with expensive hardware and software requirements.

We understand a new approach to network security after working with and believing in something for over 30 years is a challenge. But, just like the all-electric vehicle, a shift to cloud-based security solutions is happening all around us. There truly is a more secure way to ensure that your assets and data are protected.

For the first time in over three decades, a new and comprehensive campus Zero Trust solution, puts an end to challenges that have burdened IT networking, and security teams for too long. Your campus network is no longer your weakest link.