Enterprise Wired & Wireless Network Security by Nile

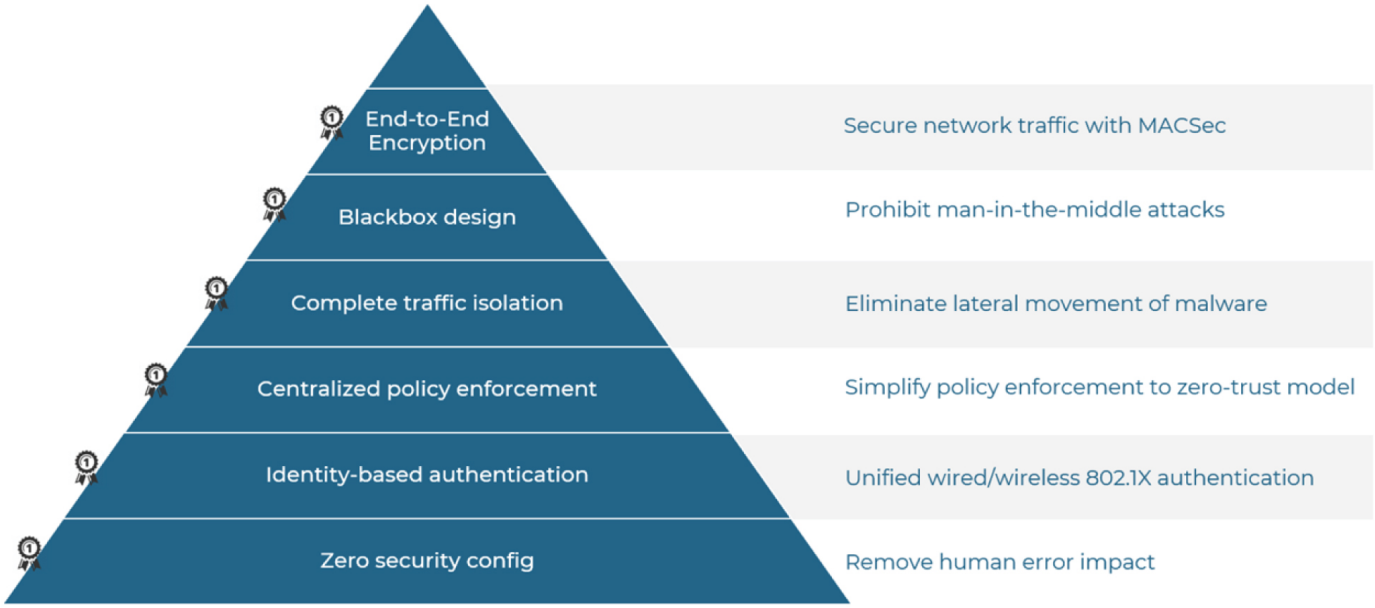
Engineering a complete enterprise network system around the principles of zero-trust to protect the network against advanced threats

Introduction

Historically, enterprise network security has been defined by a series of painful tradeoffs. Simply put, flat networks were easy to manage but gave attackers free reign to spread and cause damage once inside the network. On the other hand, the more secure and tightly controlled architectures defined by Zero Trust exponentially increased the cost, complexity, and effort required from staff. Ultimately, this forced organizations into uneasy compromises that were expensive, left technical teams overworked, and fell well short of the ideals of Zero Trust. Nile introduces a new enterprise network in which security and Zero Trust principles are built-in by default with no additional costs or network management required. Unlike traditional approaches which layered security on top of the enterprise infrastructure and assets, Nile allows security to be truly integrated into the infrastructure itself.

Nile ensures that each device can be segmented based on its needs; all traffic is encrypted; and every network connection is authenticated, authorized, and evaluated for threats based on enterprise policy. Nile's innovative secure-by-design architecture ensures that there are no blind spots in the network where attackers may hide, and the policies can be equally applied to any traffic, whether wired or wireless, from client to cloud, or even between hosts on the same access network.

While Nile transforms the status quo in network design, it integrates smoothly into the enterprise. Nile does not try to take over an organization's approach to security. It works with and enhances an organization's existing policies and security tools. All of these tools behave normally, enhanced with the ability to see a far more complete view of enterprise traffic, and the option to enforce far more fine-grained controls.



Just as importantly, Nile handles all of the configuration needed to make this happen automatically so that network and security teams can focus on real security work instead of being bogged down managing the complexities of microsegmentation, VLANs, and ACLs. The Nile solution has been designed from scratch to deliver an enterprise network that massively reduces both enterprise risk and operational complexity.

In this paper, we introduce some of the key principles of the Nile solution and how they translate to more efficient and effective enterprise security outcomes

A New Network Designed for Security

A secure network begins by ensuring that the underlying elements of the network are secure. Security begins in the supply chain long before a Nile component is deployed into the user environment. Every Nile device has a unique device certificate that is created during manufacturing and is burned into the Trusted Platform Module (TPM) of the device. All software is signed using this certificate. As a result, each device can verify the integrity of its hardware, firmware, and software on every startup and a device will not start if it has been compromised or tampered with. Likewise, each device is uniquely tied to an individual Nile customer and will only work in that customer's environment.

Additionally, by delivering a network as a service, Nile was free to rigorously reduce each element (access, point, switch, etc.) to its most necessary services. Fewer services mean fewer opportunities for vulnerabilities. Nile designed deep instrumentation and sensors into every hardware and software component, and Nile's cloud-based AI uses this insight to ensure that the network is continuously and automatically optimized.

The Nile design completely removes the need for a human to connect to a device, allowing the removal of SSH, Telnet, or other remote services, which can be accidentally left open or exploited by attackers. In fact, there is no management or console port that could potentially be abused by attackers. Likewise, all network configurations are fully automated by Nile, removing the potential for human errors. Each device leverages Nile's custom-hardened OS and all code is updated automatically.

Why it matters:

Ransomware and advanced threat actors have heavily targeted networking infrastructure both as a way of gaining initial access into an organization and to further distribute additional malicious payloads to other hosts within the network. Vulnerabilities within network devices will often be overlooked by standard vulnerability scans, or teams may delay updating them due to concerns about impacting the network… Furthermore, as the complexity of a network grows, so do the opportunities for configuration errors and mistakes. Human error can easily leave devices, segments, and services unprotected or at risk without the security team's knowledge. Nile removes all of these risks without staff having to do anything or ever even having to think about them at all.

Encryption of All Traffic

In addition to securing each individual element, Nile ensures that every connection and all traffic between Nile elements is secure. Nile implements TLS between all network elements to ensure that only devices tied to that specific customer are allowed on the network, and all traffic is encrypted via MACSec (802.1AE). All traffic on a customer's Nile network is encrypted and can't be sniffed or modified regardless of user, device, application, or whether the asset is on the wired or wireless network. Nile also lets organizations bring their own key (BYOK), ensuring that not even Nile can see the customer's actual data.

Why it matters:

Encryption can be handled in many ways by many components depending on the network, application, and user device. Any enterprise wireless network will likely implement strong encryption as a standard practice for traffic over the air, but the same is not true once that traffic hits the wire or for the wired Ethernet side of the network. Any unencrypted traffic can allow attackers to sniff traffic and to steal data or even capture login credentials in transit. The well-known Emotet trojan is just one example of malware that will attempt to sniff traffic, and in some cases, even when the application implements its own encryption.

Unencrypted traffic can also allow an attacker to intercept and manipulate traffic in transit using man-in-the-middle (MITM) techniques. Even when encryption is implemented between a user and application, attackers can use MITM connections by taking advantage of vulnerabilities or weak implementations of encryption by performing SSL stripping, hijacking, and other techniques.

With Nile, all traffic on the network is encrypted by default including access to internal resources that may not encrypt traffic as well as applications that may have vulnerable implementations of encryption.

Consistent Identity-Based Authentication

The Nile solution provides a universal southbound interface to all clients regardless of their location in the network. All client traffic is automatically routed to the northbound interface even if the device attempts to make a direct device-to-device connection in the same segment or access layer.

This design makes it possible to deliver a highly consistent, granular approach to security. The first benefit is that it ensures that all traffic and devices can be authenticated and authorized based on enterprise identity and policy. This not only enables consistent policies, but also it ensures a consistent experience for end-users across the wired and wireless networks. Organizations can support a single, unified authentication infrastructure (e.g. RADIUS) or can support multiple authentication methods as needed by policy. Nile also performs device fingerprinting, allowing policies to identify IoT devices and other headless assets that may not support an organization's preferred authentication methods.

Just as importantly, each connection is re-authenticated to ensure the most granular level of control. Nile continues to look for any changes in the connection for signs that the device or user should be re-authenticated such as changes to the MAC address, DHCP, HTTP or a variety of other traits. As a result, Nile verifies that both users and machines are who they say they are and that they should still be allowed to access the target resource. This means that new policies will be enforced immediately, and privileges can be immediately revoked if there are signs that a device or account is compromised.

Why it matters:

Identity is one of the most important aspects of modern security, and Nile makes it easy to ensure that identity is a part of every connection on the network. At its foundation, this capability ensures that an untrusted user can't simply walk into an environment or gain access by social engineering and then plug into the network.

Additionally, as attackers increasingly attempt to compromise credentials or spoof the identity of approved devices, it is critical for security teams to have insight into every authentication, both for continuous identity verification as well as revealing anomalies that could indicate signs of a compromise.

Per-Device Segmentation

Nile works with an organization's firewall and other security tools to ensure that every device is segmented and security policy is applied to connection. Once again, all connections on the network pass through the Nile interface. This interface then passes each request northbound to the enterprise firewall to determine if the connection should be authorized based on policy.

Nile introduces two major improvements in the way that organizations protect their users and assets. First, it ensures that all traffic is seen by the firewall and the rest of the security infrastructure. In the past, traffic that didn't go to the Internet or cross a core switch would never be seen. This means that an organization can apply the full power of its security stack to every connection, whether firewall rules, the latest threat intelligence, the security posture of the connecting device, behavioral anomalies, and so on. This level of segmentation also enables policies to be applied to peer-to-peer traffic or traffic on the same network segment. For example, should Device A be allowed to send SMB traffic to device B on the same subnet? This type of visibility and control is critical for preventing the lateral movement techniques used by malware and advanced adversaries.

Why it matters:

The Nile architecture ensures that every connection can be analyzed and all appropriate policies enforced. Since all traffic is automatically segmented by design, there is no need for staff to build complex VLANs or ACLs to apply segmentation. The plumbing is taken care of automatically, and organizations are free to enforce any policy that they choose.

The Nile architecture also extends security enforcement deep into the network to detect and prevent attacker reconnaissance, lateral movement, and persistence techniques. For example, after compromising a host on the network, attackers will regularly attempt to map the local environment or attempt to directly connect to hosts in the infected machine's ARP cache. Many of these techniques can be focused on devices in the same access or distribution layer and would typically never be seen by an organization's security infrastructure. This leads to a situation where most networks lack visibility precisely in the areas where attackers are most active.

IoT devices are particularly vulnerable to threats on the inside the network as they typically lack any host-based protections. Likewise, they are rarely updated and typically contain well-known exploitable vulnerabilities. And while IoT may have limited resources compared to an enterprise server, they can still provide attackers with persistence and an ongoing command-and-control channel.

Nile removes this east-west blind spot and ensures that all intelligence and enforcement is applied to all connections.

Per-Request Policy Enforcement

Nile's ground-breaking architecture ensures that all security functions (authentication, authorization, threat detection, behavioral analysis, etc) can be applied to every connection and session. As a result, security is not treated as all-or-nothing decisions limited to a single point in time, but instead is continually reassessed based on the most up-to-date information and context. All security policies remain completely under the customer's control. Nile simply ensures that organizations can implement controls to any level of granularity without ever having to think about the complexity of the network.

Why it matters:

Security is always in flux, and attackers routinely take advantage of the privileges and trust given to internal devices, accounts, and resources. By validating and analyzing every connection, Nile ensures that trust is never blindly granted to any asset, and instead is actively verified based on the most current information available.

Summary and Next Steps

Nile introduces a completely fresh view not only to enterprise connectivity, but also to how organizations can approach their security. By redesigning the network from the ground up, Nile truly built security into the architecture of the service. But most importantly, Nile does not try to wrest control of security away from the organization. Instead, Nile multiplies the power of any existing security tools and policies, while removing the complexity and friction that long have plagued IT, networking, and security teams.

With Nile:

- Every device is segmented, every connection is controlled, and all traffic is encrypted automatically
- Threats are no longer free to perform reconnaissance or move laterally from device to device
- Existing security tools become far more powerful by automatically having visibility into previously hidden traffic and connections
- The security team retains full control over all their policies, all of this is happening automatically without the need for ongoing effort and configuration work, freeing staff to focus on higher-value projects