Nile and Palo Alto Networks: Delivering a Zero Trust Enterprise Network Together

Executive Summary

THE CHALLENGE

Segmenting and securing the enterprise network against intrusions, while also protecting IT assets and sensitive data have created immense complexities for today's enterprise networking architectures. Data breaches and cyber-attacks are rising alarmingly, with 96 percent of CEOs and executives experiencing security breaches in 2022[1]. The more recent cyber-attacks have been using lateral movement to gain deep access to the network through east-west propagation.

JOINT SOLUTION

The Nile service architecture seamlessly integrates with Palo Alto Networks Next-Generation Firewalls (NGFWs) to deliver a simple and secure zero trust campus network. This joint solution offers enterprise-grade availability and performance, while effectively safeguarding against unauthorized access and malware proliferation. Together, the solution ensures a secure network environment without unnecessary complexities.

JOINT SOLUTION COMPONENTS

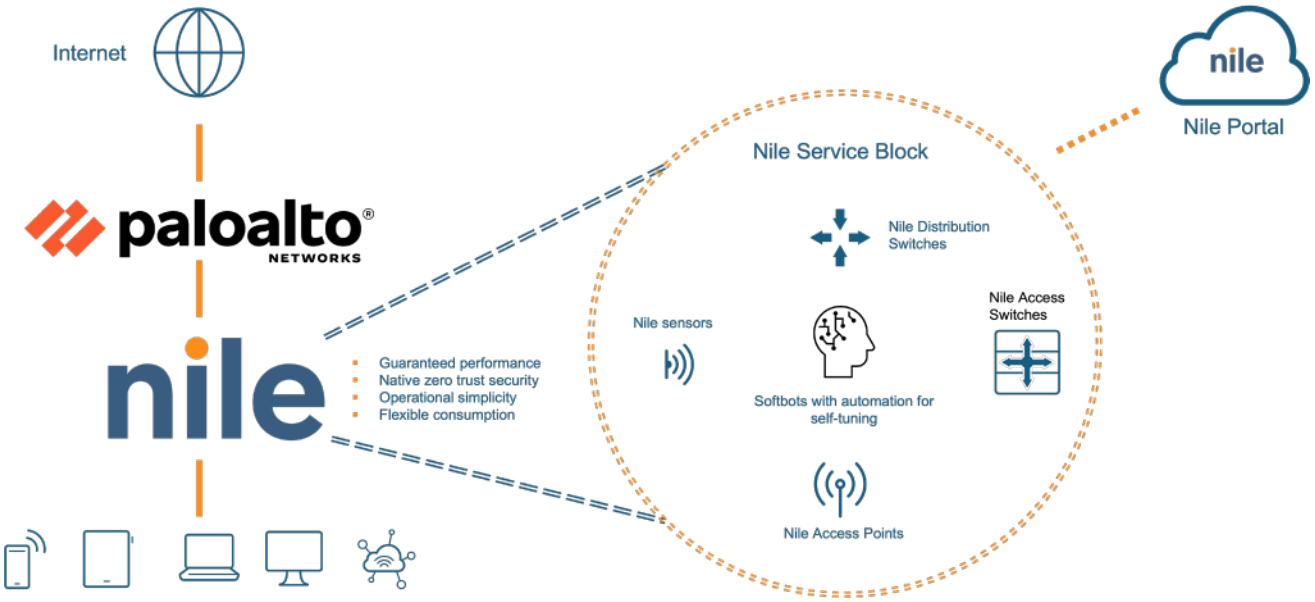
- Nile Access Service
  - Guaranteed network performance
  - Native zero trust security
  - Complete network lifecycle (Day 0 → Day N)
  - Flexible consumption model
- Palo Alto Networks NGFW
  - Advanced security features
  - Identity-based protection
  - Zero-delay signatures
  - ML-powered visibility

JOINT SOLUTION BENEFITS

- **Simplify security workflow**: The Nile architecture enables all traffic to be automatically directed to Palo Alto Networks NGFWs for a centralized architecture, providing complete visibility and control.
- **Protect against malware proliferation**: The joint solution provides a powerful framework that safeguards against malware proliferation by blocking direct peer-to-peer communications by default with Nile Access Service architecture and utilizing PAN NGFWs as a centralized enforcement point.
- **Create granular intent-based segmentation**: Automatic mapping of users and devices based on identity and role in the Nile-powered network enables precise control and dynamic policy creation, reducing misconfigurations and inefficiencies for enhanced security.
- **Simplify device authentication**: Authenticate every user or device seamless within the Nile Access Service regardless of wired and wireless architecture. Enhance with PAN NGFW's secure edge access mechanisms to authenticate every external user or device attemping to gain access to internal resources.
- **Get enterprise-grade availability and performance**: Fully redundant and resilient network with the Nile Access Service and PAN NGFWs. The Nile service additionally provides guaranteed performance backed by Service Level Agreements, reducing the areas of risk for network failures.

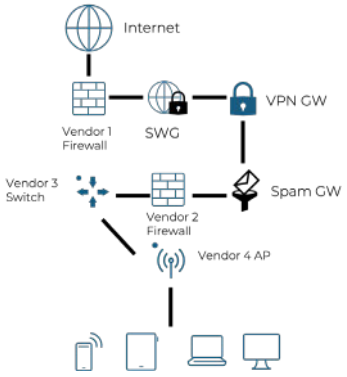
Securing the enterprise network together

The Nile Access Service seamlessly integrates with Palo Alto Networks (PAN) NGFWs to provide zero trust in the enterprise campus network.



Simplified security workflow: The Nile service architecture by the Nile Access Service enables all network traffic to be directed upstream to PAN NGFWs for granular inspection and enforcement. The approach streamlines security workflows for IT teams, granting them granular control over the network by ensuring that no traffic is permitted unless explicitly allowed on PAN NGFWs. As the Nile service is designed to simply use, IT team can focus on creating effective segmentation strategies to implement on PAN NGFWs to improve the overall security posture of the network.

DISPARATE ARCHITECTURE



- Complex
- Multiple touchpoints
- Expertise required
- High OpEx burden

JOINT SOLUTION

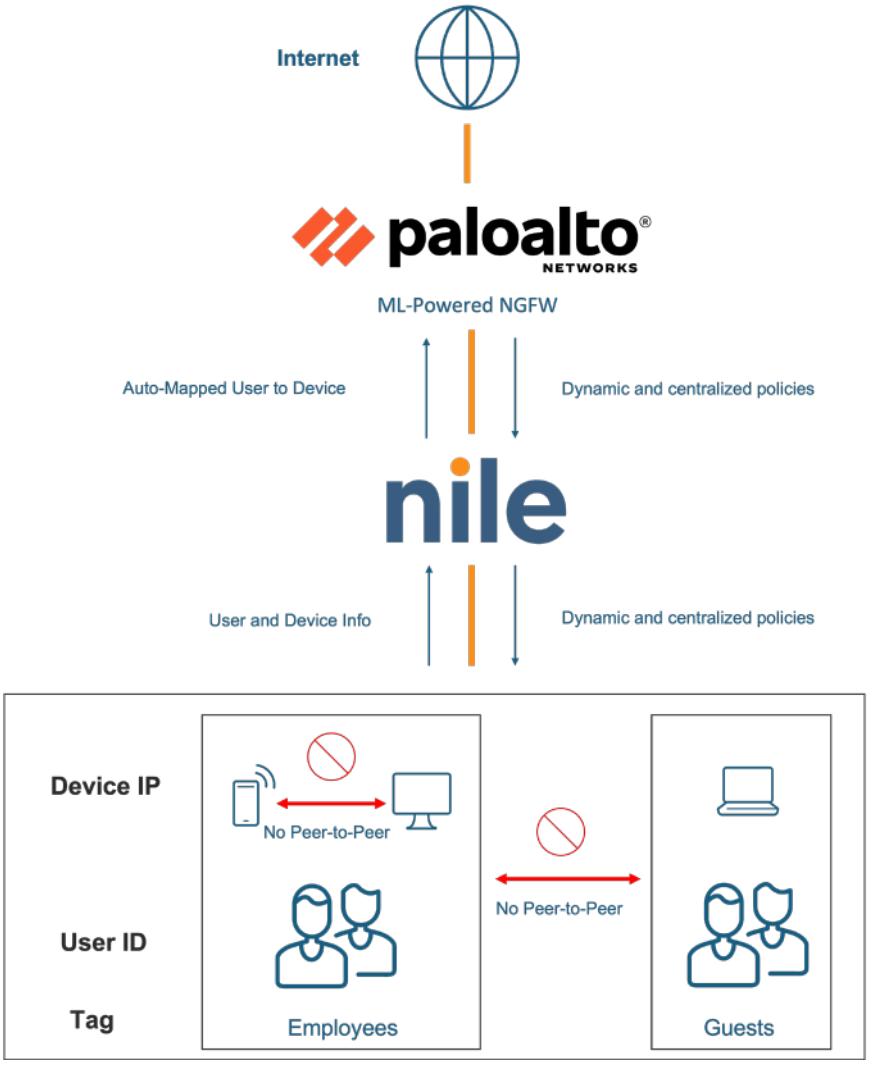
- Simplified and centralized
- Comprehensive protection
- Granular segmentation
- Highly redundant network

Protect against malware proliferation

The joint solution presents a robust framework designed to effectively safeguard against the proliferation of malware. With the Nile Access Service architecture, all direct peer-to-peer communications are blocked by default, significantly mitigating the risk of malicious hosts spreading throughout the network. By utilizing PAN NGFWs as a centralized enforcement point, IT teams gain comprehensive visibility and control to address network threats and dramatically minimize the risks associated with malware propagation across different users and devices, thereby bolstering overall network security.

Create granular intent-based segmentation

When accessing the network powered by Nile, every user or device is automatically mapped based on their identity and role. This mapping is transmitted to PAN NGFWs, empowering security operators to create dynamic and granular policies based on the intent of each user or device. This ability to create granular segmentation policies enable organizations to exercise precise control over all users and devices. Additionally, by eliminating the need for manual policy definition, the chances of misconfigurations and inefficiencies that hinder achieving a highly secure network are significantly reduced.

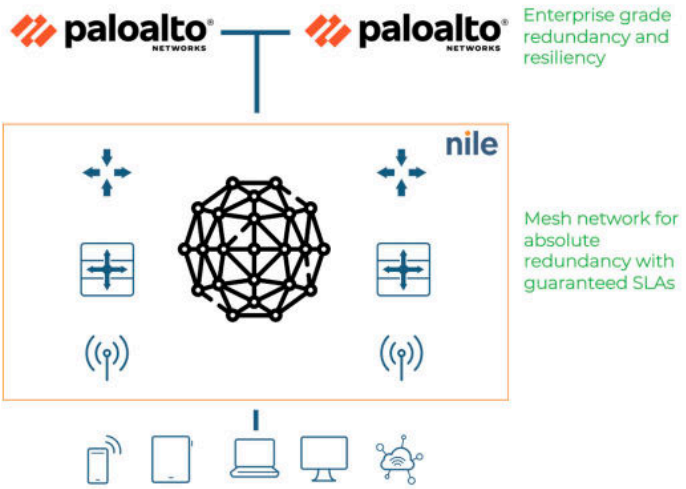


Edge-to-edge authentication

The Nile Access Service leaves no room for trust without first verifying every user, device, and application that attempts to connect into the network. Each Nile service component is required to authenticate before authorized to join the service network, eliminating the possibility of unauthorized or rogue devices being connected. Access capability within the service enable seamless authentication for users and devices, irrespective of the underlying wired or wireless architecture employed by organizations. PAN NGFWs further strengthens the secure access architecture by introducing edge authentication. This enhancement verify users and devices attempting to access internal sources, bolstering the overall security of the network infrastructure.

High Performance and Availability Design

The Nile solution offers enterprises a performance guarantee accompanied by easily verifiable Service Level Agreements (SLAs). Each Nile Service Block (NSB) is meticulously engineered with complete redundancy and resiliency, enabling the provision of multiple pathways to ensure guaranteed availability, capacity, and coverage for every user and device within the network. Furthermore, PAN NGFWs, also built with full redundancy, synergize seamlessly with Nile, resulting in a joint solution that enhances network reliability and augments overall performance for organizations.



About Palo Alto Networks

Palo Alto Networks is one of the leaders in cybersecurity. They look to innovate to outpace cyberthreats, providing next-generation cybersecurity to customers globally. Their cybersecurity platforms and services are backed by industry-leading threat intelligence, committed to helping ensure each day is safer than the one before.

About Nile

Nile delivers the enterprise network entirely as a service. Re-engineered from the ground up to guarantee network performance, backed by easily verifiable SLAs. Nile completely manage the entire network lifecycle. With Nile, you get a NaaS experience that is rich in performance, foundationally secure, and effortlessly simple—all delivered in a simple, scalable, and flexible pay-per-user model.

[i] "What's Next in Cyber," a 2022 Global Survey conducted by Palo Alto Networks