SOLUTION BRIEF

Fortinet and Nile Security Solution

Securing the Enterprise Wired and Wireless Networks with FortiGate and Nile Service

Executive Summary

Network IT demands more capability and reliable security from fewer components to save on cost and simplify the environment. Nile's wired and wireless connectivity, coupled with security from Fortinet FortiGate Next-Generation Firewalls, helps deliver industry-leading enterprise security for any edge at any scale architecture. Organizations can weave security deep into their hybrid IT through this partnership to ensure complete visibility and threat protection.

Challenge

Segmenting and securing the enterprise network against intrusions while protecting IT assets and sensitive data has created immense complexities for today's enterprise networking architectures. Data breaches and cyberattacks are rising at an alarming rate—2021 experienced 50% more cyberattacks per week on corporate networks compared to 2020.[1] The most recent cyberattacks use lateral movement to gain deep access to the network through east-west propagation across hybrid environments. Network segmentation, alongside other security strategies, such as zero trust, can be used to mitigate these attacks.

Joint Solution Description

Nile's enterprise network architecture for wired and wireless connectivity integrates with FortiGate NGFWs, simplifying and centralizing policy enforcement while securing the network against unauthorized access and malware proliferation. This network design drives a zero-trust enterprise network using a FortiGate NGFW as the single point of policy enforcement.

The Nile technology seamlessly integrates with FortiGate NGFWs to provide customers with powerful security capabilities to prevent unauthorized network access and protect against sophisticated threats like malware and external hackers. Organizations can strengthen their network security posture by leveraging enterprise-class complementary capabilities from Nile and Fortinet.

Joint Solution Components

Fortinet FortiGate Next-Generation Firewall

FortiGate NGFWs deliver industry-leading enterprise security for any edge at any scale with full visibility and threat protection. Organizations can weave security deep into their hybrid IT architectures to build security-driven networks for ultrafast, end-to-end security leveraging Fortinet's patented SP7 security processing units, consistent real-time defense through FortiGuard services, and operational efficiency and automated workflows for optimized user experience.

Joint Solution Components

- Nile Service
- Fortinet FortiGate NGFW

Joint Solution Benefits

Security

- Centralized enterprise policy enforcement with NGFW
- Prevent malware proliferation with dedicated north-south traffic flow
- End-to-end enterprise network MACSec encryption
- Zero-trust access with IEEE 802.1X for wired/wireless with MAB support

Enterprise Campus Network

- Complete enterprise network system delivery
- Guaranteed network performance backed by SLAs
- End-to-end operations day 0 → day N
- Automated life cycle management, software updates, and security patches

FORTINET FABRIC-READY

Nile Service and Features

The Nile solution is architected around the principles of zero trust, trusting no one, and authenticating everything. IEEE 802.1x authentication for wired and wireless devices ensures that your devices are authenticated across your site. To further bolster security, end-to-end MACSec encryption protects network data, abolishing any malicious snooping. Nile's unique TPM-certificate authentication for each Nile element prevents rogue devices or man-in-the-middle attacks from gaining access to the network and its data. Finally, with zero-trust isolation, traffic only flows north to south, eliminating malware proliferation.

Centralizing Specialization

Building upon the principles of zero trust, all traffic within the Nile network flows north-south, (i.e., Nile prevents peer-to-peer communication to prevent the spread of malware.) The Nile network leverages the Fortinet firewall to apply **segmentation** and **access policies** that customers can control and evolve for client communication. Prevention of peer-to-peer communication also deters malware proliferation. You can see in **Figure 1** that the Nile Service Block (NSB) interoperates with FortiGate NGFWs to provide client-to-client segmentation and prevent unauthorized access to enterprise resources.

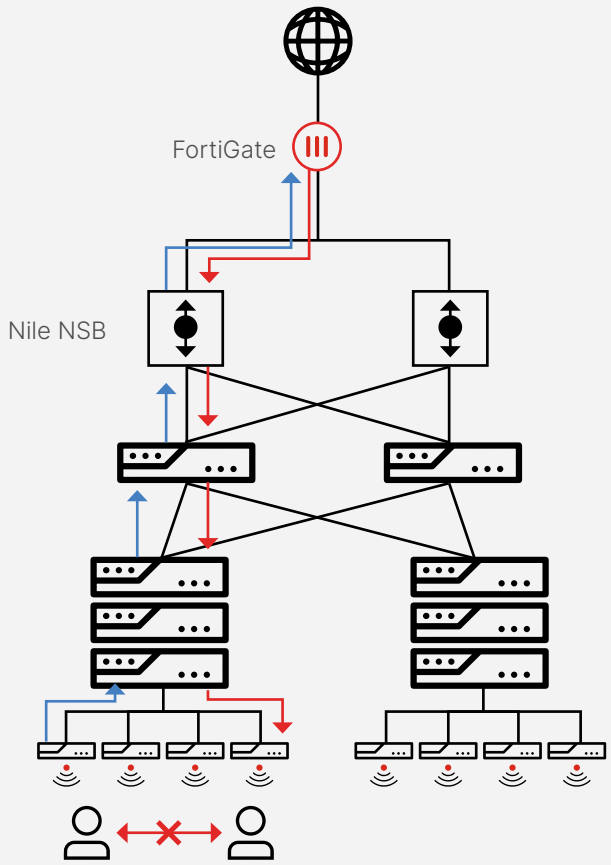

Figure 1: Nile service block interoperates with FortiGate

Flexible Routing

Customers have the option to use Open Shortest Path First (OSPF) or static routes between Fortinet firewalls and an NSB. This provides IT leaders with the flexibility to choose either or both methods depending on their network size and in-house expertise. Many organizations today use static routes and add default static routes for WAN interfaces. For faster traffic convergence, Nile recommends using OSPF on the FortiGate NGFWs.

Link Monitoring

Link monitoring capabilities help monitor the status of the link between an NSB and the Fortinet firewall when a static route is configured. This capability probes the link before forwarding the traffic on that link, thereby eliminating traffic black-holing and improving network reliability and performance.

High-Availability Design

FortiGates are built with redundancy capabilities for enhanced reliability and increased performance to avoid the firewall being a single point of failure. Simple integration with the NSB and the FortiGate NGFWs is possible through active-active or active-passive clustering modes.

Summary

Fifty-two percent of networking professionals say network security is a top concern when managing the network.[2] The integration of Nile and Fortinet is critical in strengthening and simplifying network security. The Nile Service provides seamless interoperability with Fortinet NGFWs and leverages all FortiGate capabilities. IT teams can feel confident that centralized enterprise policy enforcement using next-generation firewalls will protect the network from malware proliferation.

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 simplifies the entire network operations experience by taking on the responsibility of lifecycle management, including network planning, site survey, procurement, and installation, and extending into hardware refreshes, software updates, and security patches. With Nile, you get a NaaS experience that is rich in performance, foundationally secure, and effortlessly simple—all delivered in a simple pay-per-user model.

For more details, contact Nile for the integration guide. To learn more about how Nile secures your network from end to end, visit Secured by Nile. Nile and Fortinet are continuously innovating to support dynamic policy capabilities in the near future to enhance user and device security within an enterprise.

[1] "Corporate Cyber Attacks Up to 50% Last Year," Cyber Security Intelligence, January 18, 2022.

[2] IDC: Network as a Service Enables Flexible Consumption of Secure and Agile Enterprise Networks.

October 14, 2022 6:19 PM
1740499-0-0-EN