nile | SOLUTION BRIEF

Nile & Graphiant

A Secure Branch Network Solution

Building out an enterprise-wide network that offers a secure, high performance networking often involves setting up branch locations such as retail stores, bank branches, and medical clinics.

While smaller in scale than a corporate office, all branch locations share a common set of requirements:

- Reliable wired and wireless access
- Multiple network segments, internet
- Internet and cloud accessibility
- Strong Zero Trust principles to prevent cyber-attacks

To meet these needs, the following are required:

Access Points and Switches:	Provide both WiFi and wired access for employees, guests, IT, and IoT/OT devices. They must support segmentation and Zero Trust architectures for enhanced security.
Edge Routers:	Connects branches to the enterprise network, Internet and cloud services, enabling business-to-business (B2B) communication via partner network connectivity.
Firewalls:	Protect the branch from external, as well as internal threats and attacks.
WAN Connectivity:	In the form of one or more ISP circuits to provide reliable WAN connectivity for the branch.

Challenges

Setting up a branch location with all relevant functionality comes with a large and evolving set of challenges today that range from working with 5 to 6 vendors to acquiring all necessary equipment, to sourcing different technologies to solve for different connectivity and security use cases.

WLAN/LAN and Access Management

Problem	Explanation
Complex Manual Configuration	• Traditional LAN/WAN and access solutions often require manual configuration and repeated tuning. • Time-consuming, error-prone, and difficult to scale as networks evolve.
Lack of Visibility and Monitoring	• IT teams struggle to monitor and maintain full visibility over devices and traffic. • Lack of visibility leads to connectivity issues, performance degradation, security breaches, and unplanned outages.
Manual Software Upgrades	• Minimizing security risk across the LAN/WAN requires vigilant attention to software patches and upgrades to protect against emerging vulnerabilities.
Minimal Zero Trust	• Traditional LAN solutions often lack sufficient built-in zero trust security endpoint device isolation to mitigate these risks.
Limited Scalability	• Service expectations often require manual intervention for scaling to meet demand, causing inefficiencies. • This is complicated by hardware requirements, deployment issues, complicated licensing and a heavy reliance on different vendors.

Edge Router and Firewall Management

Problem	Explanation
Enterprise Connectivity: MPLS	• In addition to managing an on-premises device, MPLS is expensive and operationally complex. • Deployment and changes are slow and require provider involvement.
Enterprise Connectivity: SD-WAN	• SD-WAN is complicated at scale due to the large number of required tunnels. • No SLA guarantees available, which can impact performance and reliability.
Separate Solutions for Different Connectivity Use Cases	• **Enterprise Network:** Requires SD-WAN and MPLS. • **Cloud Connectivity:** Needs multi-cloud solutions and backhaul to co-location for DirectConnect/ExpressRoute. • **Partner/SSE Connectivity:** Requires IKE-based IPsec tunnels with static or dynamic routing. • Complex extranet design requirements.

Budget Constraints

Problem	Explanation
CapEx Heavy Upfront Purchases	• Historically requires heavy capital expenditure (CapEx) for upfront networking hardware and software purchases.

Lifecycle Management

Problem	Explanation
Hardware Equipment Issues	• Network upgrades traditionally require extensive evaluation, hardware and software upgrades, and integration effort. • Both MPLS and SD-WAN solutions historically require significant equipment upgrades or downgrades based on capacity requirements during contract renewals. • Networking problems include CapEx, maintenance, and dealing with obsolescence.
Software Problems	• Traditional problems include patching, upgrades, firmware tracking, and licensing complexity.

Nile and Graphiant: Building the Next-Generation Branch

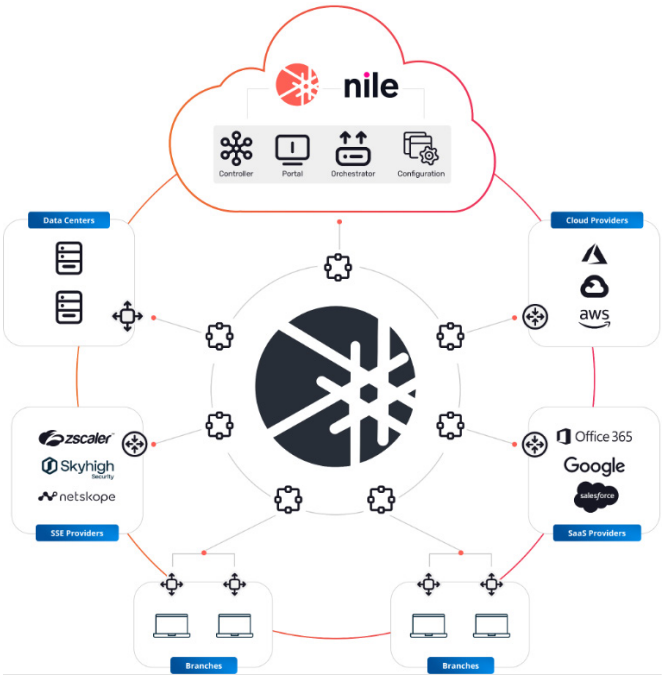
The **Graphiant** and **Nile Campus NaaS (Network as a Service)** solutions seamlessly integrate to provide a next-generation unified branch solution, addressing all LAN and WAN connectivity and security needs, while simplifying deployment and IT operations. Delivered as-a-service, this joint end-to-end solution offers flexibility that adapts to evolving business needs and overcomes the limitations of traditional branch offerings.

The Nile Access Service offers high-performance WiFi and wired access with built-in Zero Trust features that provide robust Layer 3 network segmentation, per-endpoint isolation of users and devices (employee, guest, IoT/OT), and strict identity-based policy enforcement. Modern network architecture with AI-driven automation and standardized deployment model delivers today's only financially backed service and performance guarantee.

Graphiant's Network Edge provides fast, scalable, MPLS-like enterprise connectivity that is easy to provision and is dramatically more cost-effective than legacy MPLS or SD-WAN solutions.

The joint Branch-as-a-Service model delivers fully managed branch infrastructure, with Graphiant and Nile handling provisioning and operations. This reduces operational complexity and costs, as the organization primarily manages custom integration projects and granular policy adjustments, as well as user interaction.

The as-a-Service model also allows new branches to be added easily and integrated into the network without expensive CapEx budget requirements and long-term lifecycle commitments, simply by committing to adjusted as-a-Service consumption increases.



Benefits for Customers

The unified branch solution from **Graphiant** and **Nile** provides customers with a simplified, secure, and cost-effective approach to managing enterprise connectivity, security, and branch operations. Key benefits include:

High-Performance Network Connectivity

- Performance guaranteed WiFi and wired connects that deliver seamless roaming, ultra-responsive voice and video connections, and fewer end-user complaints.
- Autonomous networking with AI-driven self-tuning and self-optimization capabilities that eliminate manual configuration, for uninterrupted user experience gains.

Robust Network Security

- **Campus Zero Trust security** with built-in Layer 3 segmentation, per-endpoint isolation, device profiling, and granular policy enforcement capabilities that prevents unauthorized communication, eliminates lateral movement, and delivers enhanced internal and external threat prevention.
- Built-in SSO, SCIM, and RADIUS support eliminates the need for complex NAC solutions, integration projects, and dedicated IT resources. Optional orchestrated SSE integration available for Universal Zero Trust enforcement.

Simplified Enterprise WAN Connectivity

- A single **Graphiant Edge** device at each branch handles all connectivity use cases, including enterprise network, cloud, and B2B partner connections.
- **Seamless Integration** with LAN-side routing protocols (OSPF, BGP) and encrypted, high-performance connections that guarantee SLA performance and reliability.
- Scalable, **multi-VRF segmentation** for efficient traffic management across branch offices and enterprise networks, without the complexity of tunnel management.

Effortless Cloud Connectivity

- **Graphiant Gateway** simplifies multi-cloud, B2B, and IoT cloud networking with secure, high-performance connections to **Cloud Service Providers (CSPs)** through **carrier-neutral facilities.**
- Direct, private connections between enterprise branches and cloud services via the **Graphiant Core** eliminate the need for costly MPLS or complex SD-WAN configurations.

Optimized B2B Partner Connectivity

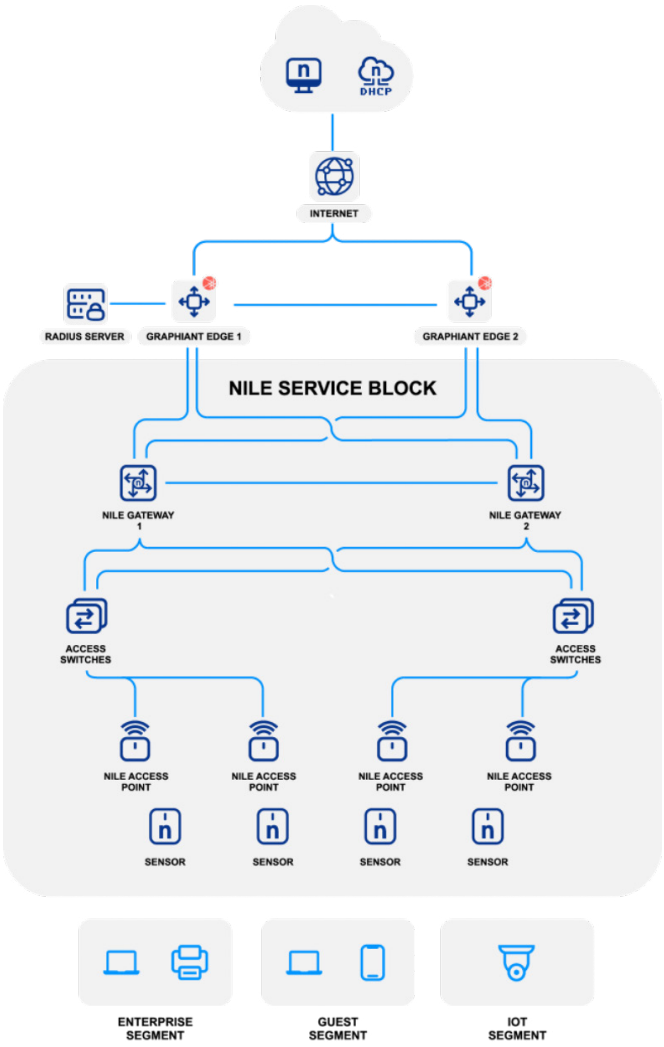
- **Multi-Tenant Stateless Core** provides an easy, subscription-based model for B2B connectivity, enabling automatic provisioning and high-performance, secure connections.
- **Simplified Security** with automatic encryption and resilient connections, removing the need for complex MPLS or insecure public internet-based extranets.

Comprehensive Next-Generation Firewall (NGFW)

- Built-in **NGFW** functionality at the **Graphiant Edge** provides stateful inspection, **DPI-based application identification**, and the ability to match traffic based on applications for enhanced security.
- Seamless integration with **SIEM solutions** for advanced network-wide security features and centralized monitoring.

Scalable Security with SSE Integration

- **Graphiant Edge** and **Gateway** enable easy integration with Secure Service Edge (SSE) providers, allowing enterprises to send traffic for advanced threat analysis without needing individual IPsec tunnels from each branch.
- **Fewer IPsec sessions** to SSE providers, reducing complexity and enhancing scalability while maintaining security across all branch locations.



This end-to-end service model simplifies the deployment and management of enterprise corporate and branch networks but also offers flexibility, scalability, and Zero Trust security to meet today's evolving business needs, while reducing operational complexity and costs.

About Graphiant

Graphiant is a Silicon Valley-based provider of next-generation Edge services. The Graphiant Network Edge is an “as-a-Service” solution providing connectivity for the enterprise WAN, hybrid cloud, network edge, customers, and partners. Graphiant NaaS combines performance, security, agility, and affordability to enable network architects to build enterprise-grade networks at the speed of business.

About Nile

Nile is transforming the enterprise network landscape with a groundbreaking AI-powered networking architecture that delivers secure, modernized connectivity and IT operations. For the first time, organizations can access campus networks entirely as a service, benefiting from integrated Zero Trust security, intelligent IT efficiencies, and a performance guarantee backed by financial assurance for connectivity, coverage, and availability.