nile

Zscaler & Nile

Unified network access and policy enforcement for users and IoT whether on-premises or remote.

Zscaler & Nile

Quick Glance – Integration Highlights

- Provides universal cloud-based SSE controls to campus connected devices
- All campus traffic automatically routed to Zscaler Internet Access instance for policy enforcement
- Strengthen your security posture on all fronts
- Simple 2-minute activation, with automated orchestration

The Market Challenge

With today's hybrid work model, organizations are looking to network offerings that include zero trust principles for the campus only to find legacy solutions that do not match the protection of cloud-based SSE solutions. These older network solutions lack a means to protect in-office devices due to loosely distributed controls, and universal policy enforcement model.

Organizations are forced to implement and manage separate solutions for the campus that include on-premises firewalls, NAC servers and more. They want the same protection and benefits for the campus or branch that is provided to their remote users, where uniform policies and enforcement are utilized.

The Solution

Together Nile and Zscaler have partnered on a modern security services edge solution for campus and branch deployments that allows organizations to enforce policies for users, as well as IoT/OT devices that match that of SSE ZTNA solutions. Customers gain the benefits of cloud-based security where the network plays a key role in protecting data and assets without add-on solutions, additional agents and complex integration projects.

The AI-powered Nile Access Service with built-in Nile Trust Service features solves today's growing campus security challenges by providing a highly secure network that includes per-host isolation of all wired and wireless devices and Layer 3 segmentation by design. The addition of Nile's Trust Service for SSE feature ensures all traffic is forwarded to Zscaler's Secure Internet Access solution. Local East/West traffic can be handled by Zscaler or Nile depending on device type.

Solution Components / Key Features

Enhanced policy enforcement via Zscaler Internet Access (ZIA) for all endpoint devices regardless of connection - on campus or remote.

Per-host isolation without the use of VLANs via Nile Access Service's built-in granular campus zero trust access control and Layer 3 segmentation.

Simplified IoT and BYOD security as all traffic can be forwarded to ZIA for inspection or selectively allowed via Nile Access Service's microsegmentation feature.

Encryption of all on-premises traffic for each connected wired or wireless device that traverses the Nile Access Service.

Easy to leverage connectivity that utilizes existing LAN to WAN services from Nile Access Service to local Zscaler Internet Access instance.

nile

Zscaler & Nile

Value Statement

This combination of cloud and campus zero trust security offers a new and efficient security model that provides seamless, secure, reliable access regardless of device or location with comprehensive universal zero trust approach. The campus is no longer the weakest link.

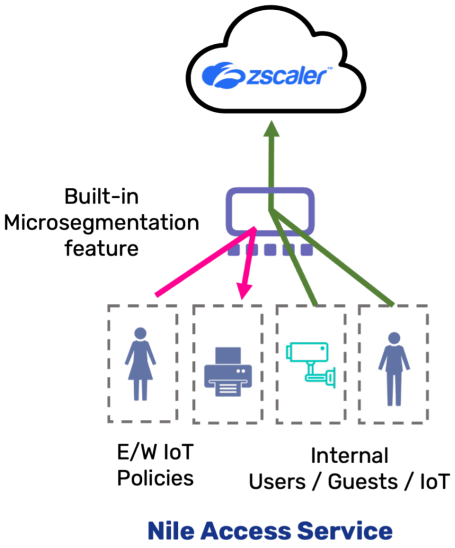
Use Case 1

Unified policy enforcement

Next-level campus zero trust isolation and network security is achievable via innovative cloud and on-premises integration. By channeling all traffic through a north-south pipeline, organizations can ensure consistent policy enforcement regardless of device type or location.

The solution isolates individual users and devices, allowing no communication unless explicitly permitted by policies enforced by the Zscaler Internet Access (ZIA). Data flows between devices or users are encrypted and tunneled individually for inspection, guaranteeing only authorized flows between source and destination are permitted.

With Zscaler and Nile, your network is fortified, ensuring uncompromising protection for your valuable data and assets.



Use Case 2

A secure hybrid work model

With today's hybrid work, managing disparate policy enforcement solutions for users connecting remotely versus when they're in a corporate office or branch is cumbersome. This joint solution for the campus and remote user access delivers a next-gen campus zero trust features that complement those of today's modern SSE solutions. With the isolation of individual devices, layer 3 segmentation, and Zscaler Internet Access policy enforcement users gain a common experience.

The result is a combination of campus zero trust and SSE features that deliver universal zero trust security, policy enforcement consistency, and scale - without the complexity.

Use Case 3

Zero Trust IoT security

IoT devices are no longer weak links within networks as this joint solution eliminates legacy VLANs and associated security risks, IoT vulnerabilities, and lateral movement initiated threats. Per-device isolation and forwarding of traffic to your Zscaler Internet Access instance offers a new class of IoT security. All without software agents or complex configuration steps.

Organizations gain the advantage of unique campus zero trust wired and wireless segmentation benefits, and the ability to leverage universal policy enforcement via Zscaler's unique SSE capabilities. IoT devices are longer targets used to easily spread malware throughout your organization.

nile

Benefits

Benefits	Outcomes
Improved security posture	Unified security with consistent protection for all users, devices, and apps, regardless of location
Enhanced visibility and control	Deep network and security event insights for improved decision-making and responses to threats
Scale and flexibility	As organizations evolve, a unified solution easily scales to accommodate new use cases, and applications
Unified policy management	Centrally manage both remote and LAN based security functions, with universal enforcement
Cost and IT efficiency	Single framework that reduces the need for separate solutions, ongoing maintenance, and support costs

Conclusion

Deliver enhanced user and IoT device network security with Zscaler and Nile

Experience a new universal zero trust solution that replaces legacy security that leverage VLANs and firewalls. All connections are authorized based on shared user identity, business policies, and context; including location, device status, and authentication and authorization privileges. The net results are reduced risk, an improved user experience, and simplified management and deployment.

For more information, visit **nilesecure.com/solutions/nile-access-service**.

nile

Zscaler & Nile

About Nile

Nile is disrupting the enterprise network market by delivering natively secure connectivity and modernized IT operations via a new AI networking architecture, delivering campus networks entirely as-a-Service. For the first time in the industry, customers gain integrated zero trust security, intelligent IT efficiencies, and a financially backed connectivity, coverage, and availability performance guarantee.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile and secure. The Zscaler Zero Trust Exchange, a SASE-based platform, is the world's largest inline cloud security platform, protecting thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications over any network.

nile