Netskope's Scalable, Secured End-to-End Segmentation

Solution Brief

The Netskope solution offers VRF-based segmentation extending branches, data centers, and the cloud, boosting security, performance, and policy control. Customize your network design using flexible segment-aware topologies such as full mesh, hub-spoke, and dynamic branch-to-branch to meet business needs, including threat isolation, compliance, mergers, and beyond.

Quick Glance

- **Integrated Security Enforcement:** Minimize attack exposure through segmentation and isolation, enhancing security with integrated enterprise firewall, IPS, and URL filtering features within the SASE gateway.
- **Automated Policy Management:** Utilize automated policies to efficiently enforce segmentation-based policies, adapting them to user and device types while applying distinct per-application policies to individual segments.
- **Improved Performance:** Ensure efficient utilization of network resources by isolating congested segments and prioritizing critical applications, resulting in optimized network performance, reducing latency and ensuring a better user experience.

The Challenge

Flat networks come with significant challenges, such as increased vulnerability to cyberattacks due to unrestricted lateral movement for attackers, difficulties in maintaining compliance, and restricting changes to only one part of the network. Additionally, flat networks struggle with managing network traffic, leading to congestion and degraded performance.

Traditional segmentation approaches to overcome flat networks issues relied on switches, routers, and firewalls for network division, but struggled with implementing advanced routing and security for each segment. They often failed due to complexity, security gaps, and scalability and manageability issues.

Virtual LANs (VLANs): Restricted to local networks, no advanced security, manual configurations, and lack full visibility into users and application

Virtual Routing and Forwarding (VRF): More complex than VLANs, enforcing consistent policy across the WAN is complex and non-scalable and offers no advanced security

The Solution

Netskope Borderless SD-WAN extends segmentation across endpoints, branches, data centers, and the cloud, sharing vital segmentation information network-wide. It streamlines network access through customizable segmentation policies managed from a unified console, resulting in enhanced network performance. The solution strengthens security with embedded controls while maintaining segment isolation, protecting employees, guests, and infrastructure. Automated policy enforcement, based on user and device type, tailors per-application policies for each segment, ensuring optimal real-time routing of applications.

Flexible deployments to drive business goals

The benefit of supporting versatile segment-aware topologies like full mesh, hub-spoke, and dynamic branch-to-branch is increased flexibility and adaptability in network design and management. Here's how each of these topologies provides advantages:

Full Mesh Topology:

- **Enhanced Redundancy:** In a full mesh topology, every node (branch or location) is directly connected to every other node. This redundancy ensures that if one link or node fails, there are multiple alternative paths for communication. This minimizes downtime and enhances network reliability.
- **Optimized Traffic Routing:** Full mesh allows for efficient and direct communication between any two branches in the network, optimizing the path for data transmission and potentially reducing latency.
- **Isolation and Security:** Each branch has a direct connection to all others, but this can also support isolation if needed. Traffic between specific nodes can be controlled and secured, which is valuable for compliance and security requirements.

Hub-spoke Topologies:

- **Centralized Management:** Hub-spoke topologies are often easier to manage because they have a centralized hub (e.g., data center or headquarters) that can apply and enforce policies consistently to the spoke locations (e.g., branch offices). This simplifies network administration and security policy implementation.
- **Cost Savings:** Hub-spoke topologies can be cost-effective, as not all locations need direct connections to each other. Branches communicate through the hub, which can optimize bandwidth usage and reduce operational costs.

Dynamic Branch-to-Branch Topology:

- **Scalability:** This topology is adaptable to changing network needs. It allows branches to establish direct connections to one another dynamically when needed. This scalability is valuable as organizations expand and open new branches or need to establish temporary connections.
- **Efficient Network Utilization:** Dynamic branch-to-branch connections can be established on-demand, optimizing network resources and bandwidth usage. It ensures efficient communication paths between branches without the need for permanent connections.

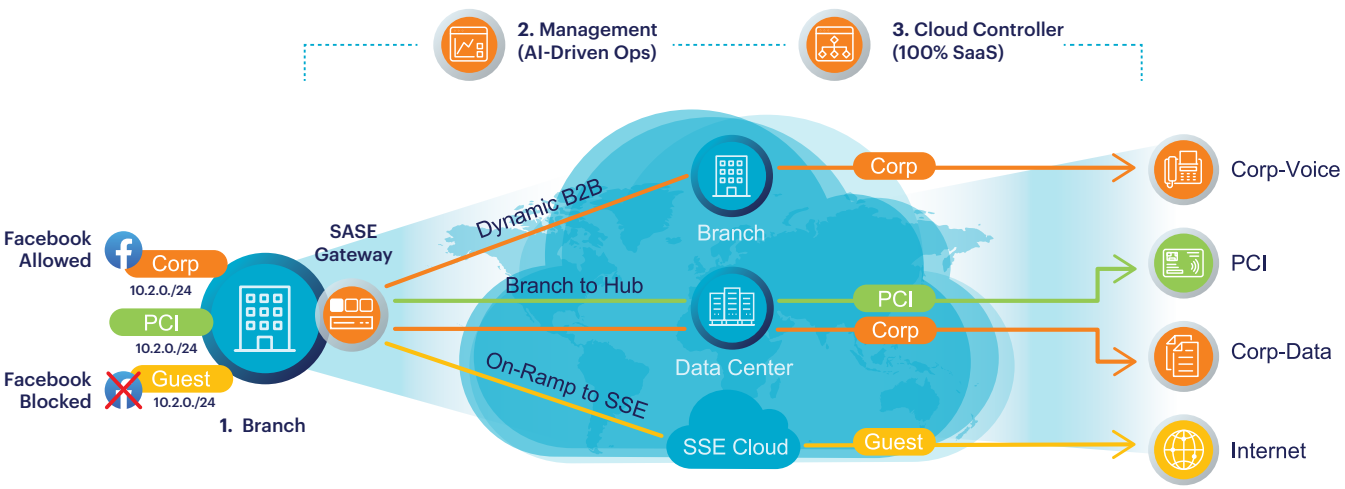
Customers gain heightened flexibility and adaptability in adopting VRF-based segmentation solutions tailored to meet their evolving business needs.

Enhanced security across your network

Netskope Borderless SD-WAN represents a new era in segmentation, delivering comprehensive security solutions across every layer from 3 to 7, while introducing direct cloud security for each tenant within every network segment. This solution harnesses a secure layer 3 IPsec connection, integrating vital security components such as authentication and encryption.

Better Security Outcomes: Our VRF-based segmentation approach takes network traffic isolation to the next level. By combining this with integrated enterprise-grade firewall, IPS, and URL filtering capabilities, a formidable security boundary is established to prevent lateral spread of threats. Extending this segmentation across various network locations creates distinct virtual routing instances, significantly reducing the risk of security breaches and unauthorized access.

Consistent End-to-End Protection: Netskope Borderless SD-WAN doesn't stop at branch locations. It seamlessly extends segmentation to encompass data centers and the cloud by efficiently sharing crucial segmentation information throughout the network. This ensures that security measures are consistently applied across the entire network architecture, offering a comprehensive defense against evolving threats.



VRF-based segmentation and integrated security prevents lateral spread of threats, extending consistent security across the network for comprehensive protection against evolving threats.

Achieving operational efficiency

Netskope Borderless SD-WAN optimizes network performance, enhances security, and ensures that network resources align with the specific needs and priorities of different segments within your organization.

Segment-aware Topologies:

Netskope Borderless SD-WAN offers the flexibility to customize network topologies on a per-segment basis. This means that you can design specific network architectures that best suit the requirements of each segment or tenant within your organization. For example, you can create a segment dealing with sensitive financial data, and another segment like guest Wi-Fi to separate the corporate user traffic and streamline traffic flows. This level of customization allows you to optimize network layouts according to the specific needs and security considerations of each segment, enhancing both performance and security.

Segment-aware AppQoE Policies (Application Quality of Experience):

Netskope Borderless SD-WAN enables the creation of application quality policies tailored to each segment. This means that you can prioritize and allocate network resources based on the unique demands of applications within a segment. For example, a segment focused on video conferencing and real-time collaboration tools can have policies that prioritize low-latency and high-bandwidth allocation for these applications, ensuring a seamless experience for users. Segment-aware AppQoE policies guarantee that critical applications receive the required resources, improving overall network performance and user satisfaction.

Segment-aware Firewall Rules:

Netskope Borderless SD-WAN allows you to define specific firewall rules for each segment, granting granular control over network traffic. This means you can apply security policies that are tailored to the distinct security requirements of each segment. For instance, a segment containing customer-facing applications may have strict ingress and egress rules to safeguard against external threats, while an internal segment may have more relaxed rules to facilitate efficient internal communications. Segment-aware firewall rules provide the necessary flexibility to balance security and operational requirements across various segments effectively.

Per-segment Bandwidth Allocation:

Netskope Borderless SD-WAN enables precise bandwidth allocation on a per-segment basis. This allows you to allocate network resources according to the bandwidth demands of each segment. For example, a mission-critical segment handling large data transfers may be allocated a higher proportion of available bandwidth to ensure smooth operations. In contrast, a guest network segment may have limited bandwidth to prevent it from overwhelming the network. Per-segment bandwidth allocation ensures that network resources are utilized efficiently, preventing congestion and optimizing network performance within each segment.

> Establish segment-specific policies to attain granular controls for optimizing network performance, enhancing application experiences, and ensuring compliance with regulatory requirements.

Per Endpoint/Host Segmentation:

Netskope segmentation solution is extended to endpoints or hosts, bolstering security precision. Configured with a specific profile, the endpoint can only access assigned applications and resources that could be located anywhere. The device-based segmentation extends to a partner's use case as well, to ensure when a partner laptop connects, it remains isolated from critical corporate segments. This novel feature establishes a strict boundary, minimizing potential damage in case of device compromise.

Simplified Management with a Unified Console:

Simplicity is at the heart of Netskope Borderless SD-WAN's approach. Our solution provides a single, adaptable console featuring a four-tier, multi-tenant mechanism. This mechanism is expertly designed to cater to the diverse deployment needs of both enterprises and managed service providers (MSPs). By centralizing security and networking policy creation and monitoring, it simplifies the management of unique policies for every network segment and tenant.

Fast-track Issue Resolution with Extensive Monitoring:

VRF-based segmentation offers per-segment metrics, including segment-aware statistics and dashboards, which provide granular insights into network performance, traffic patterns, and security. This enables proactive issue identification and swift response, ensuring optimal network operations and enhanced security.

Key Use Cases

Separating lines of business

Separate lines of business with/without firewall zones allow for stricter access controls and isolates businesses/departments and their data (e.g., investment banking vs. retail banking vs. real estate investment, etc.) from the rest of the network, reducing the risk of lateral movement in case of a security breach.

Isolating guest networks

Segmenting a dedicated guest network ensures that visitors and contractors have separate and controlled access, preventing unauthorized access to internal resources.

Merger and acquisition with overlapping IP

Segmentation allows overlapping IP addresses to allow merged/acquired organizations to interconnect and work with each other without significant architectural changes.

Meeting compliance requirements

Segmentation can help ensure compliance (HIPAA, PCI, etc.) by isolating sensitive data or systems, enabling strict access controls, and facilitating easier audits and monitoring.

> Segmentation provides a versatile approach for strengthening security, achieving compliance, optimizing performance, supporting mergers, and segregating IoT devices and guest networks.

Segmenting IoT and non-IoT devices

IoT devices can be placed in their own segment to mitigate security risks and separate them from critical IT systems. A retail store wants to separate video surveillance traffic from transactional traffic.

Application performance optimization

By assigning dedicated segments to applications with specific performance requirements, organizations can optimize bandwidth, reduce latency, and improve overall application performance.

Conclusion

Netskope Borderless SD-WAN extends segmentation seamlessly across branches, data centers, and the cloud. It simplifies network access with customizable policies from a unified console, enhancing performance and security. Automated policy enforcement, tailored by user and device type, optimizes real-time application routing. Rather than relying on ACL rules to limit network traffic, a VRF-based segmentation approach involves the complete blocking and isolation of networks. This fundamental design ensures that a compromised client in one segment cannot impact others, providing a robust and multi-layered defense. VRF-based segmentation offers per-segment monitoring metrics, delivering granular insights into network performance, traffic, and security through segment-aware statistics and dashboards. This proactive approach ensures optimal network operations and heightened security.