netskope

Whitepaper

End-to-End Protection with Zero Trust Hybrid Security in the Next Gen SASE Branch

Secure your enterprise with the integration of on-premises and cloud-delivered security services, delivered on-demand for comprehensive end-to-end protection, eliminating the need for point products.

YESTERDAY'S LEGACY SECURITY IS NOT A FIT FOR TODAY'S SECURITY NEEDS

The enterprise perimeter is expanding due to the widespread distribution of users, devices, and applications across multiple cloud environments. Current solutions like legacy SD-WAN and individual point products are struggling to effectively address the security and optimization requirements of the modern, borderless enterprise. Disparate security measures, including on-premises IPS, Application Firewall, IoT security, as well as cloud security services like CASB and SWG, contribute to increased costs, complexity, and inconsistent security practices between branch locations and remote users.

NEXT GEN SASE BRANCH IS HYBRID- CONNECTED, SECURED, AND AUTOMATED

Netskope Next Gen SASE Branch is the solution that is enabled by Netskope's Borderless SD-WAN and Intelligent SSE. Netskope Next Gen SASE Branch converges Context-Aware SASE Fabric, Zero Trust Hybrid Security, and SkopeAI-powered Cloud Orchestrator into a unified cloud offering, ushering in a fully modernized branch experience for the borderless enterprise.

Zero Trust Hybrid Security, one of the tenets of the Next Gen SASE Branch solution, offers cloud-based SWG, CASB, and more, and seamlessly integrates with on-premises App Firewall and IPS/IDS security services—eliminating point products and offering consistent policies across all locations.

Netskope ZTNA Next further combines SD-WAN and ZTNA capabilities, fully replacing legacy VPN with one agent.

Netskope SASE gateway with integrated device intelligence discovers and autonomously categorizes both managed and unmanaged IP-connected devices within the network. Utilizing advanced AI/ML capabilities, it detects breaches and dynamically implements microsegmentation on those devices, effectively isolating and thwarting the lateral movement of threats.

Building the Next Gen SASE Branch Architecture Securely

Here are the four architectural components that will allow you to transform your network, security, and user experience with consistent and simplified policy everywhere:

Netskope One Gateway

Netskope One Gateway, a unified SASE gateway, provides secure and optimized access to all applications and supports the widest range of deployment options, from micro to large branch or data center appliances, cellular gateways and as a virtual appliance for multi-cloud networking.

Netskope One Client

The Netskope One Client, a unified SASE client, brings together SD-WAN with SSE security capabilities like SWG, CASB, ZTNA, and more, to extend secure and optimized connectivity to end-user devices, without the need for a hardware appliance.

Netskope SASE Orchestrator and Controller

Simplifies management using a cloud-native, unified SASE console to enforce SSE and SD-WAN policies across branches, remote sites, and diverse cloud environments. Stay resilient with the industry's first 100% SaaS-based controller that separates control and data plane.

Netskope New Edge

NewEdge, a fast, reliable, and converged cloud-native platform that offers the broadest geographic coverage in the industry (71+ regions). Netskope Borderless SD-WAN in NewEdge delivers high-performance cloud on-ramps and mid-mile optimizations to connect transcontinental regions. Netskope Intelligent SSE at NewEdge offers various services, including NG-SWG, CASB, ZTNA, SSPM, CSPM, FWaaS, and DLP.

With **53% of internet traffic** headed to SaaS and the public cloud, securing your users, no matter where they consume cloud services, is paramount.

ELEVATING CUSTOMERS' BUSINESS SUCCESS THROUGH COMPLINACE EXCELLENCE

Netskope's Next Gen SASE Branch relies on the robust foundation of Borderless SD-WAN. The cloud-hosted infrastructure of Netskope Borderless SD-WAN undergoes rigorous quarterly vulnerability scans and annual penetration testing. This diligence ensures that it meets the standards of a PCI Level 1 Service Provider and is HIPAA certified. Moreover, Netskope's cloud-hosted service is deployed across Tier 1 ISO 27001 certified data centers. For detailed compliance information, you can request the PCI and HIPAA Attestation of Compliance (AOC) directly from Netskope.

Securing Interconnectivity among Next Gen SASE Branch Components

Netskope SASE Controller handles all control plane functionality, acting as a BGP route reflector and distributing device information across the context-aware SASE fabric using DIMP (Device Information Messaging Protocol). Both BGP peering and DIMP messaging from the Controller to the SASE gateways happens over a secure IPsec overlay tunnel, utilizing TCP 4500.

Netskope SASE Orchestrator controls the management plane functionality of the SD-WAN. It is responsible for handling device configuration, management, monitoring, and telemetry. The SASE gateways establish connectivity with the Orchestrator via a secure TLS 1.2 web socket, utilizing TCP 443.

Netskope SASE gateways establish a secure IPsec overlay tunnel on UDP 4500 to transport user traffic between SASE gateways.

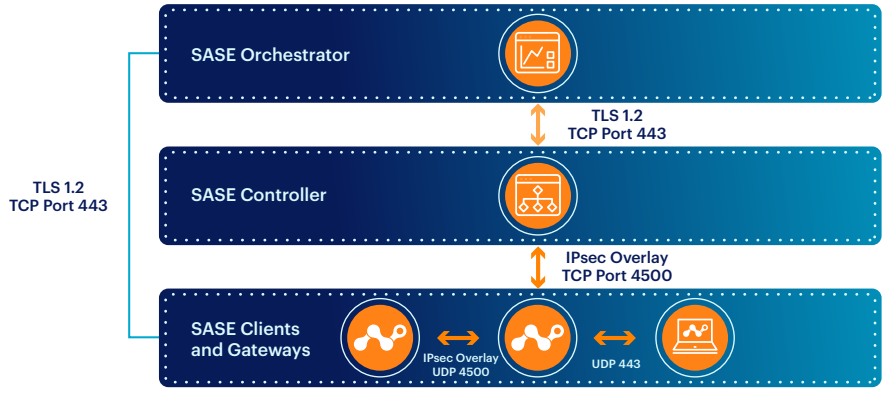

Figure 1: Secure Communication Across SD-WAN Components

Overlay Security with Borderless SD-WAN

Control and Management Plane Privacy

Unified SASE gateways are categorized as either spokes or hubs. A unified SASE gateway establish a secure TLS 1.2 connection over WebSocket TCP 443 upon activation, utilizing this connection exclusively for all Management plane communication with the SASE Orchestrator. During activation, the SASE gateways share their public key with the Orchestrator, prompting the Orchestrator to respond with the IP and public key of the Controller.

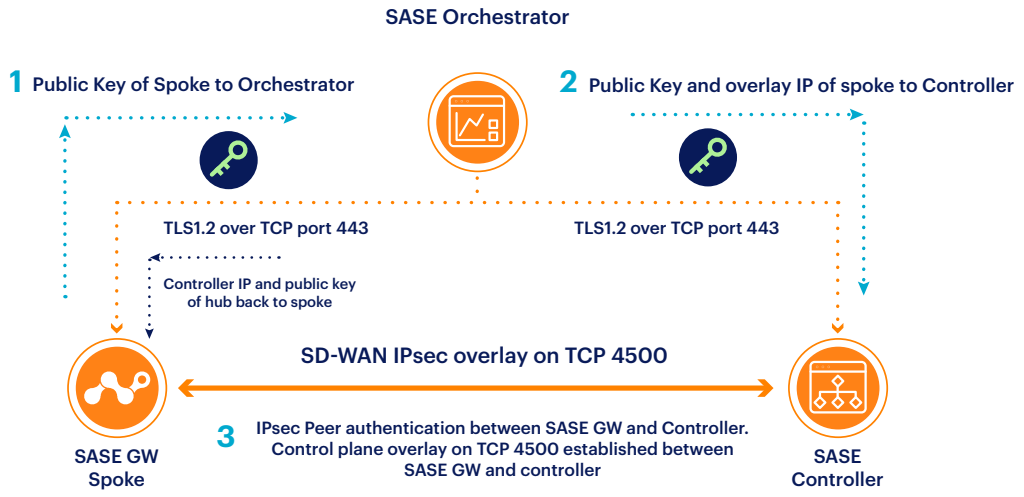

Figure 2: Control Plane Tunnel Establishment Using TCP 4500

Using the Controller's public IP and public key, SASE gateway establishes a secure SD-WAN overlay on TCP 4500 to the Controller. This overlay tunnel will be used for all subsequent control plane communication (e.g., BGP and Device Information Management Protocol) with the controller.

Figure 3: Routes and Device Information Exchange with Controller

DATA PLANE PRIVACY ON SD-WAN OVERLAY

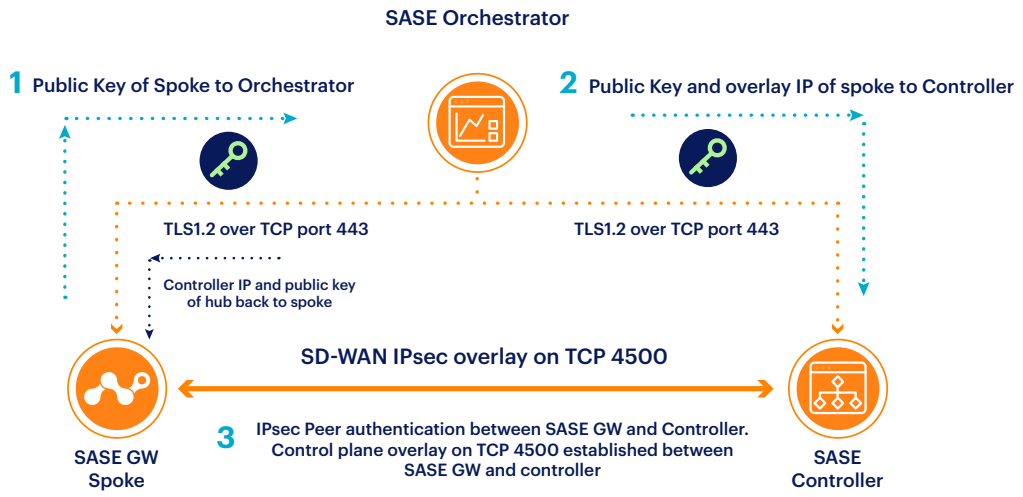

Figure 4: IKE Phase 1

Based on the configured policy, a unified SASE gateway acting as a spoke establishes SD-WAN data plane overlay tunnels to other unified SASE gateways acting as hubs/spokes.

As shown in Figure 4, the spoke leverages the public key, public IP, port, and overlay IP of the hub, as received from the SASE Controller. It then initiates the establishment of a secure SD-WAN data plane overlay tunnel with the hub, utilizing UDP 4500 and employing IKE Phase 1 and IKE Phase 2 exchanges. This established tunnel serves as the conduit for all user traffic between any two unified SASE gateways, adhering to the configured policy.

Perfect Forward Secrecy (PFS) comes pre-enabled in IKE Phase 2, as illustrated in Figure 5. This default setting ensures the initiation of a new Diffie-Hellman exchange, enhancing resistance against cryptographic attacks.

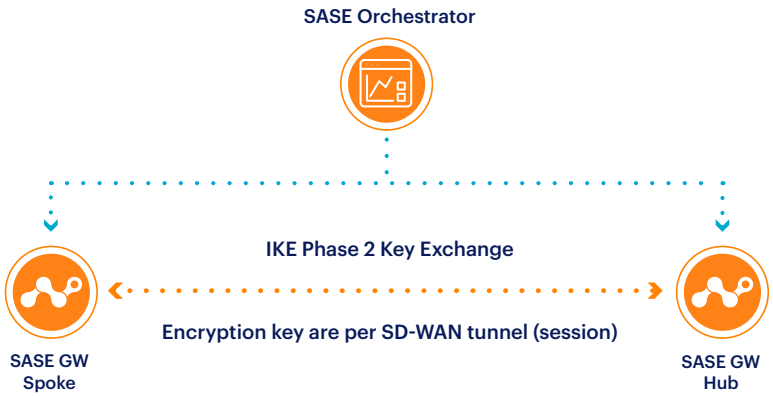

Figure 5: IKE Phase 2

Encryption and Hashing

Gateway to Gateway Security: Supported Encryption/Hashing Capabilities

Encryption Algorithm	Hashing Algorithm	IKE Version
3DES, AES-128, AES-192 & AES-256	SHA1 & SHA256	IKE v2

Data Integrity On SD-WAN Overlay

The SASE Controller identifies the public IP of a unified SASE gateway, even when it traverses a Network Address Translation (NAT). This public IP is then shared with all other unified SASE gateways in the network through the Device Information Messaging Protocol (DIMP). The Authentication Header (AH) value is computed based on the post-NAT public IP, ensuring the integrity of packets is maintained even across the NAT.

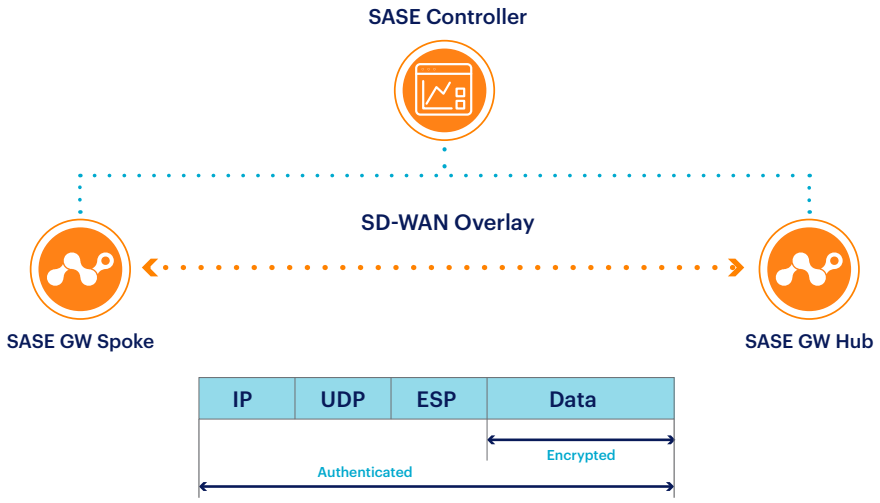

Figure 6: Data Integrity on SD-WAN Overlay

Replay Protection on SD-WAN Overlay

The IPsec ESP protocol ensures replay protection through the use of sequence numbers within the SD-WAN overlay. Each encrypted packet on the overlay is assigned a distinct sequence number. SASE gateways employ a sliding window mechanism to identify maliciously injected or out-of-sequence packets. Specifically, packets with sequence numbers falling below the sliding window's designated range are dropped.

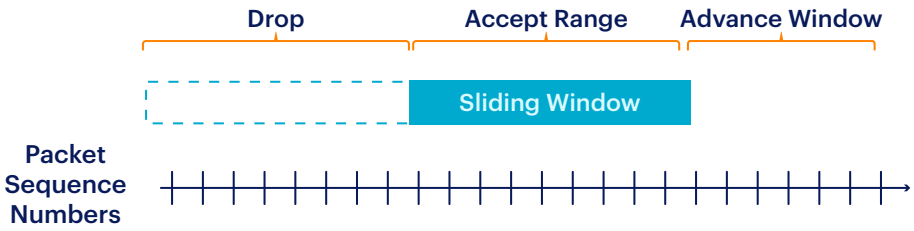

Figure 7: Anti-replay Protection in SD-WAN Overlay

Additionally, unified SASE gateways discard packets with duplicate sequence numbers, as they may potentially be replayed packets.

A substantial **65% of threats** now originate from the cloud, so protecting organizations requires a comprehensive, high-performance security solution.

HYBRID SECURITY WITH BORDERLESS SD-WAN

Security within Borderless SD-WAN includes the incorporation of both on-premises and cloud-delivered security services. On-premises security features can be activated on the unified SASE gateways as on-demand services, while cloud-delivered security is seamlessly enabled through automatic tunnels to the closest Netskope NewEdge data centers that are automatically determined by the geolocation of a unified SASE gateway.

Figure 8: Hybrid Security with Borderless SD-WAN

On-Premises Security Features: Stateful Application Firewall and IDS/IPS

Stateful firewall and IDS/IPS features are available on-premises in unified SASE gateways.

These features can be enabled on the unified SASE gateways to inspect intra-site (east-west) and inter-site
(site-to-site) traffic.

Stateful Application Firewall

The integrated application-aware stateful firewall is activated and set up through the gateway policy. Users have the flexibility to configure firewalls for both intra-site (east-west) and inter-site (north-south) traffic. Matching criteria options include VLAN, IP/Port/DSCP, protocol, application, application category, and identity-user group, offering versatile policy customization for enhanced security.

Intrusion Prevention System (IPS)/Intrusion Detection System (IDS)

The IPS/IDS operates within a distinct container on a unified SASE gateway, governed by the gateway policy. Tasked with scrutinizing all traffic traversing a unified SASE gateway, the IDS/IPS engine diligently identifies potential threats or attacks. When operating in IDS mode, the unified SASE gateway issues alerts for detected threats without taking action on user traffic. Conversely, in IPS mode, the system generates alerts and promptly blocks identified malicious traffic. Rule updates from the database are synchronized with the SASE gateway periodically, ensuring the latest threat intelligence is applied.

Protecting From External Attacks With Netskope Intelligent SSE

Netskope unified SASE gateways seamlessly and securely connect to the closest NewEdge data centers to route all of the Web and SAAS traffic efficiently. Automated through APIs, the IPsec tunnel configuration simplifies and straightforward policy rules on the SASE gateways effortlessly on-ramp all of the Web and SAAS traffic to the NewEdge data centers for securing inspection and processing. Based on the configured high-availability policies, IPsec tunnels are automatically established from the SASE gateway to the primary and secondary NewEdge data centers. Notably, WAN link or site failover occurs by default, maintaining continuity of operations without requiring additional configuration.

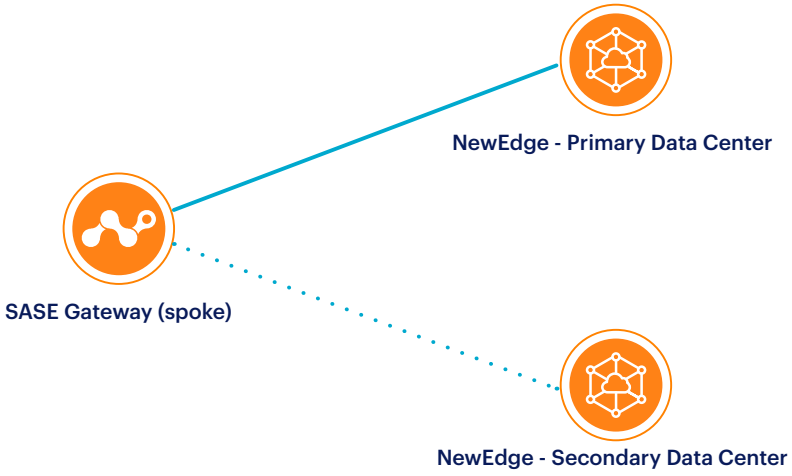

Figure 9: SASE Gateway to New Edge with Single Internet Connection

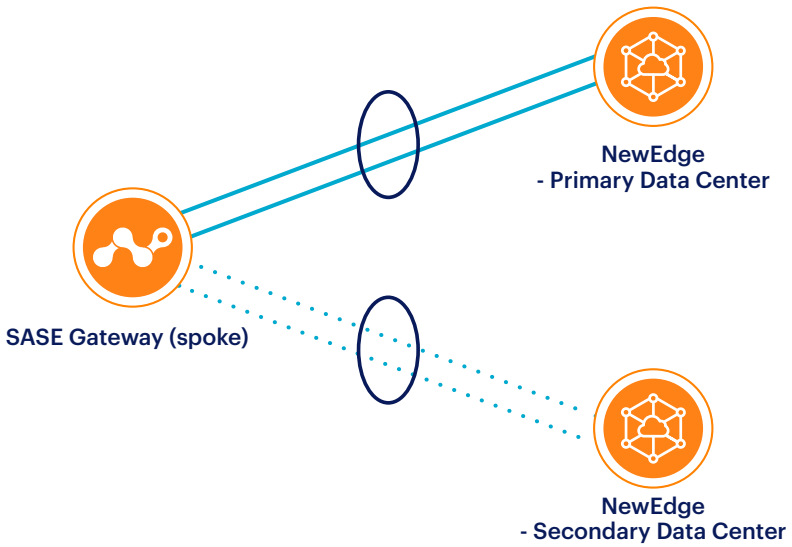

Figure 10: SASE Gateway to New Edge with Dual Internet Connection

Secure End-to-End Segmentation at Scale

Network segmentation remains a crucial component for bolstering cybersecurity, ensuring regulatory compliance, mitigating risks, and protecting endpoints and user data. Over time, the approach to implementing segmentation has evolved. Through the strategic separation and precise control of data flows, network segmentation strengthens an organization's defensive posture and provides adaptability to meet evolving operational demands. Driven by customer requirements, the following business use cases, centered around segmentation, are supported.

- **Simplify Compliance:** Segregating routing information on a per-segment basis bolsters security measures for each segment, facilitating compliance with standards like CDE/PCI and ensuring the protection of sensitive data.
- **Policy Management:** Minimizing network congestion involves preventing the performance of one segment from affecting another, ensuring consistent and optimal performance for specific applications. For example, the usage of in-store guest Wi-Fi on its dedicated segment does not interfere with the speed of credit card transactions that are occurring on a separate segment.
- **Seamless Mergers & Acquisitions:** During events like M&A, segmentation safeguards the network even when IP addresses overlap, ensuring continuity and security.

Segment-based policies offer enhanced flexibility and deliver better outcomes

- **Per-segment Network Topology:** Ensures efficient data routing and load distribution tailored for each segment.
- **Per-segment Dedicated Bandwidth Allocation:** Administrators can assign bandwidth based on the requirements of individual segments.
- **Per-segment App-QoE Policies:** Enable detailed management of application performance specific to each segment.
- **Per-segment Firewall Rules:** Individualized firewall rules for enhanced security for each segment.
- **Per-segment Monitoring and Statistics:** Segment-aware statistics and dashboards provide granular insights into network performance, traffic patterns, and security.

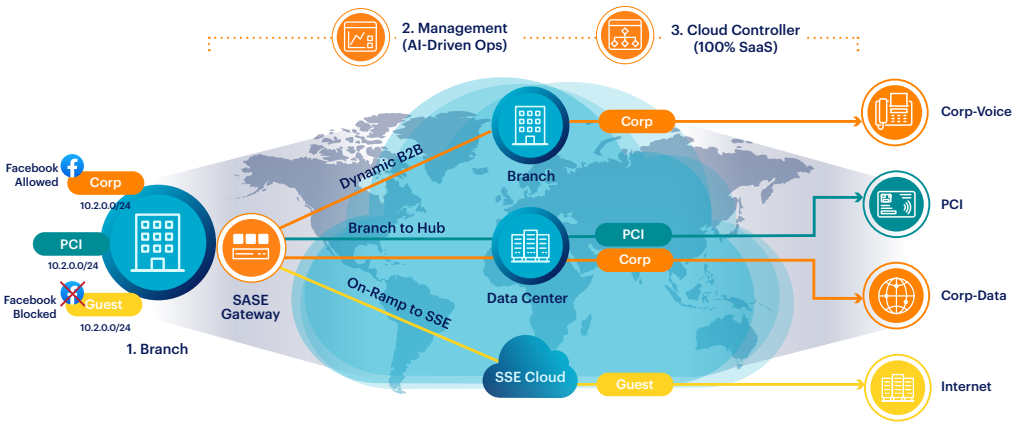

Figure 11: Segmentation Use Cases and Per-segment Policies

Key Features at a Glance:

- **Centralized Control:** The centralized SASE Controller streamlines the creation and deployment of traffic policies across the network.
- **Segment Creation & Isolation:** Administrators have the capability to define segments based on traffic nature (e.g., VoIP, guest Wi-Fi, corporate data), with each segment securely isolated from the others.
- **Policy-driven Management:** Tailored policies for each segment ensure a consistent approach to traffic handling.
- **Transport Agnostic:** Borderless SD-WAN provides the flexibility of choosing connections (MPLS, Broadband, LTE) based on the policies established for each segment.
- **Tunnel Overlays:** Leveraging tunnel overlays, Borderless SD-WAN assigns segment IDs to data packets, maintaining logical separation even when segments share the same physical connection.

Securing Borderless SD-WAN Deployment

In some deployments unified SASE gateways will be positioned behind a firewall, requiring certain ports to be open in inbound and outbound directions. As a best practice, it is recommended that the following ports be opened on the firewall based on the deployment.

Required Ports and Protocols

SASE Gateway Spokes	SASE Gateway Hubs
Allow outbound rules on firewall: • Gateway spoke to Orchestrator - TCP 443 • Gateway spoke to Controller - TCP 4500 • Gateway spoke to Gateway hub - UDP 4500 • Endpoint Client to Gateway hub - UDP 443 • Gateway spoke to link monitor - UDP 8841	**Allow outbound rules on firewall:** • Gateway hub to Orchestrator - TCP 443 • Gateway hub to Controller - TCP 4500 • Gateway hub to link monitor - UDP 8841 **Allow inbound rules on firewall:** • Gateway spoke to Gateway hub - UDP 4500 • Endpoint Client to Gateway hub - UDP 443

Cloud-Native, Multi-Tenant Management To Enable Role-Based Access Control (Rbac) Features

Netskope Borderless SD-WAN employs a cloud-native, multi-tenant, microservices-based architecture. This design facilitates hierarchical role structures and streamlines portal access management for SPs/MSPs through various tiers, namely Operator, Master MSP, MSP, and Customer Tenant.

Additionally, there is integration capability with Identity Access Management (IAM) systems, including Azure and Okta, paving the way for streamlined identity management.

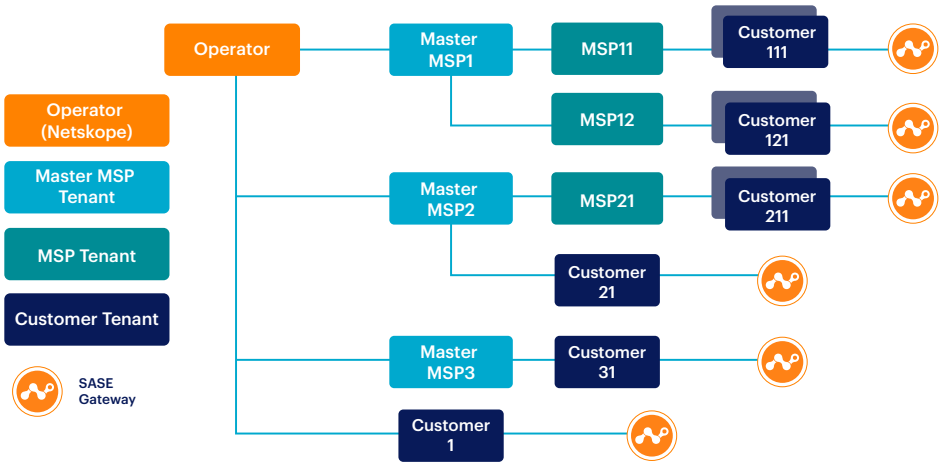

Figure 12: SASE Orchestrator Multi-Tenancy: MSP Hierarchy

Predefined Roles with Detailed Role Assignment

Customer Level Roles:

- **Admin:** Manages customer-level global settings, users, Gateways, firmware upgrades, configurations, policies, and services.
- **Operator:** Holds all the privileges of an Admin, except for user management.
- **Monitor:** Has read-only access to view global settings, configurations, stats, events, and device health.

Managed Service Provider (MSP) Roles:

- **Admin:** Can create, manage, and delete all tenant types, their policies, and users, but lacks authority over Master MSP.
- **Operator:** Manages Customer tenant users and their policies; has read access to MSP settings.
- **Monitor:** Has read-only access to both MSP and Customer tenant information.

CONCLUSION

Protect your enterprise with seamlessly integrated on-premises and cloud-delivered security services, eliminating point products and delivering consistent policies across all branches and remote locations.

Ensure communication security across all Borderless SD-WAN components, including Netskope SASE Orchestrator, Controller, SASE Hub, a unified SASE gateway, and a unified SASE client.

Establish secure end-to-end segmentation at scale with segment-aware policies to bolster security, ensuring regulatory compliance, mitigating risks, and protecting corporate data.

Implement hybrid security with on-premises and cloud-delivered services on demand for comprehensive protection against internal and external threats.

Utilize cloud-native, multi-tenant management to enable streamlined role-based access control (RBAC) features, facilitating portal access management for enterprises and service providers.

Embrace a holistic security approach seamlessly bridging on-premises and cloud environments, safeguarding your organization against evolving threats. With comprehensive protection and efficient management, Netskope empowers your enterprise to thrive securely in an interconnected landscape.

Interested in learning more?

Request a demo

Netskope, a global SASE leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. Fast and easy to use, the Netskope platform provides optimized access and real-time security for people, devices, and data anywhere they go. Netskope helps customers reduce risk, accelerate performance, and get unrivalled visibility into any cloud, web, and private application activity. Thousands of customers, including more than 25 of the Fortune 100, trust Netskope and its powerful NewEdge network to address evolving threats, new risks, technology shifts, organizational and network changes, and new regulatory requirements.

Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.