

Unlock App Performance with Borderless SD-WAN that Fuels Next Gen SASE Branch

Work From Anywhere Without Limits: Consistent Experience Across
Any User, Device, Application and Location: Branch, Home, Hotel, Cafe
and On the Go!

TABLE OF CONTENTS

INTRODUCTION	3
CONTINUOUS MONITORING	4
Automated Bandwidth Discovery	4
Automated Underlay Link Monitoring	4
Automated Overlay Path Monitoring	4
CONTEXT AWARENESS—APPLICATION AND APPLICATION RISKS	5
Automated Cloud App Detection and Prioritization Using Cloud Confidence Index	5
Automated Legacy Application Detection and Prioritization Using Deep Packet Inspection (DPI)	5
Custom Application Supports To Align with Business Needs	5
First-Packet App Detection	5
DYNAMIC APPLICATION STEERING	6
Enhanced Path Selection Capabilities	6
Bandwidth Aggregation	6
Sub-Second Failover Capabilities	7
MITIGATING NETWORK DEGRADATION WITH ON-DEMAND REMEDIATION	8
UDP Remediation	8
TCP Optimization	8
Enhanced AppQoE	8
Inbound QoS in Next Gen SASE Branch	9
Hierarchical QoS in Next Gen SASE Branch	9
Dynamic AppQoE	9
Per-Traffic Class Policing	9
DSCP Marking	9
OPTIMIZING CLOUD TRAFFIC WITH NETSKOPE NEWEDGE: ENHANCING PERFORMANCE AND RELIABILITY	12
SUMMARY	13

INTRODUCTION

Applications serve as the cornerstone of the digital economy, linking technology and business directly to revenue generation. The reliance on cloud applications is increasing among modern businesses, with projections indicating a significant rise to 72,000 by 2024 from 21,000 in 2021, as reported by [Ascendix](#). Even minor disruptions to application performance or availability translate to lost revenue.

Hybrid work models, adopted by [74% of businesses](#), necessitate ubiquitous application access. Users require seamless and optimized connectivity from headquarters, branch offices, homes, and mobile devices. However, traditional SD-WAN deployments often exclude remote users, hindering productivity. Shipping bulky appliances to remote locations further exacerbates costs.

Netskope Next Gen SASE Branch solution incorporates all of the elements of the Netskope One SASE platform—One Client, One Gateway, One Network, One Engine, and One Console—aligning with current trends and effectively tackling associated challenges.

By converging its three integrated layers—Context-aware SASE Fabric, Zero Trust Hybrid Security, and SkopeAI-powered Cloud Orchestrator—into a unified cloud offering, Netskope Next Gen SASE Branch solution delivers a fully modernized branch experience for the borderless enterprise where users and applications are widely distributed yet interconnected with Netskope’s One Network.

Next Gen SASE Branch is powered by Netskope Borderless SD-WAN technologies, engineered to ensure optimal application performance by efficiently optimizing and securing user-to-application traffic.

Leveraging multiple WAN links simultaneously reduces outages from blackouts or brownouts while also maximizing available bandwidth. This ensures a seamless experience for users accessing on-premise applications, SaaS, UCaaS, and cloud services. Netskope Borderless SD-WAN establishes optimized overlay paths between unified SASE clients, unified SASE gateways, data centers, and Netskope NewEdge for fast processing of all user and application traffic. These optimized overlay paths are continually monitored and adapt to changes, ensuring an uninterrupted user experience. All path selection and AppQoE capabilities are available in both the Netskope One Gateway (a unified SASE gateway) and the One Client (a unified SASE client).

Let’s explore how the Next Gen SASE Branch, powered by Borderless SD-WAN, delivers highly reliable, secure, and high-performance connectivity for every user, device, site, and across multiple clouds.

CONTINUOUS MONITORING

Netskope Borderless SD-WAN ensures continuous monitoring of network performance, allowing for proactive identification and resolution of potential issues that are resolved by the following:

Automated Bandwidth Discovery

Upon detection of a WAN link by Netskope's unified SASE gateway and configuration of the bandwidth set to Auto, the unified SASE gateway initiates a speed test to automatically identify both upstream and downstream bandwidth capacities of the link. This automated process streamlines network management, optimizing resource utilization and enhancing overall network efficiency.

Automated Underlay Link Monitoring

Each unified SASE Gateway establishes a connection to a cloud-hosted link monitoring service that is available in a geographically-closest region, and sends and receives probes to this service on all active WAN links. These probes are used to dynamically measure loss, latency and jitter and are sent every 100ms to monitor the overall health of all available WAN links.

Automated Overlay Path Monitoring

Netskope unified SASE Gateway sends probes on the overlay tunnels to measure loss, latency and jitter on each overlay path, with probes being sent every 30 seconds, and a burst of 30 jitter probes sent every minute when user traffic is present on the overlay path. These probes help identify the optimal path to a peer, ensuring the best application performance. In addition, when a path is being used for flows with SLA enabled, silent probes are sent even when no user traffic is present on the overlay path. (500 silent probes are sent at the rate of 100 pps every 30 seconds.) These probes help to ensure a faster failover of sensitive traffic such as VoIP calls.

CONTEXT AWARENESS—APPLICATION AND APPLICATION RISKS

Automated Cloud App Detection and Prioritization Using Cloud Confidence Index

Context awareness for Borderless SD-WAN is facilitated by the Netskope One Zero Trust Engine that enables full context sharing of user, device, and app trust across Netskope Intelligent SSE and Borderless SD-WAN services. By leveraging the Netskope One Zero Trust Engine, Borderless SD-WAN can recognize over 80,000+ applications. IT administrators are not required to configure QoS policies for these applications individually. Hence, Netskope provides a Cloud Confidence Index (CCI) for every application, offering an enterprise-readiness score. Each application receives a score between 0 and 100 and is categorized into one of five Cloud Confidence Levels (CCL): Poor, Low, Medium, High, or Excellent. Out of the box, Netskope supports smart QoS defaults based on Netskope CCI scores, serving as intelligent defaults. This eliminates the need for manual labor by the network operations team, resulting in much more efficient operations. (For example, Zoom, with a CCI of 88, is marked as high priority by default, while SureVoIP, with a CCI of 36, is treated as low priority out of the box.) These automated smart QoS defaults can be overwritten for any application in the Borderless SD-WAN orchestrator in line with business needs.

Automated Legacy Application Detection and Prioritization Using Deep Packet Inspection (DPI)

For legacy applications, Netskope's unified SASE gateways and unified SASE clients utilize Netskope's DPI engine to enable application-aware, per-flow steering, optimizing application performance. With capabilities to identify over 3,000 unique applications, Netskope employs diverse classification techniques including pattern matching, advanced analytics with machine learning for encrypted traffic, and statistical and domain-based classification.

Custom Application Supports To Align with Business Needs

Netskope Borderless SD-WAN also provides users with the flexibility to define custom applications based on IP/port range, protocol, and domain name. These custom applications can then be referenced by policies to achieve the policy-based forwarding of packets belonging to the custom apps. For monitoring purposes, traffic flows belonging to the custom app will be automatically aggregated and shown alongside the name of the custom application in the monitoring dashboard, simplifying analysis.

First-Packet App Detection

First-packet detection is crucial for intelligently steering SaaS or custom-defined applications, enhancing both performance and user experience. For SaaS applications that publish their IPs (e.g., Zoom, Office 365, RingCentral), a local database is leveraged to identify the application upon receipt of the first packet using the published IP address.

Netskope's unified SASE gateways and unified SASE clients implement first-packet identification by learning from prior flows through DNS caching and by automatically updating SaaS providers' IPs (Zoom, Teams). First-packet detection enables granular and secure breakout of internet-bound traffic to the correct path based on app-driven business and security policies. First-packet identification also optimizes steering by identifying applications at the first packet; traffic can be steered over the most appropriate link in-line with configured application steering policies. By quickly identifying applications at the outset, security policies and enforcement measures can be applied more effectively.

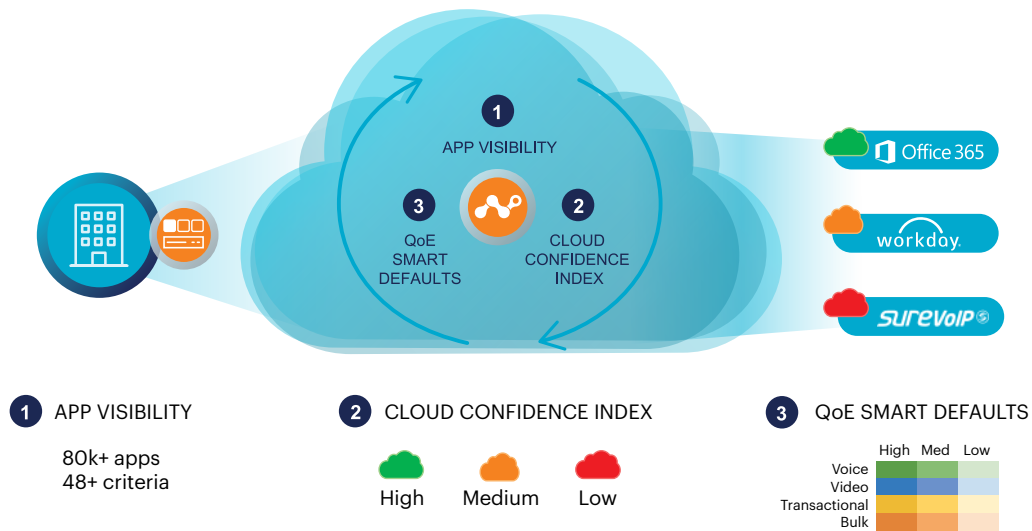


Figure 1: Context sharing of user, device & app trust across Netskope SSE & SD-WAN services

DYNAMIC APPLICATION STEERING

Enhanced Path Selection Capabilities

Netskope Borderless SD-WAN builds a transport-agnostic overlay across any network (MPLS, internet, cellular, satellite, etc.) by leveraging one of the layers of the Netskope Next Gen SASE Branch called Context-aware SASE Fabric. Path conditions such as packet loss, jitter, latency, and available bandwidth are continuously monitored between Netskope unified SASE gateways and the cloud. Additionally, underlay links can be configured in various states (Active, Hot Standby, Cold Standby, and Metered) to adapt to dynamic network conditions. Applications are automatically steered onto the appropriate links based on application priority and link conditions. Netskope Borderless SD-WAN also provides VRF-based end-to-end segmentation, allowing customers to define path selection rules per segment, further enhancing network control and optimization.

Bandwidth Aggregation

Both unified SASE gateways and unified SASE clients, allow multiple WAN links to utilize all available links to transmit traffic concurrently. This occurs by default when no Active or Backup path is specified using WAN tags in the AppX rules. Load balancing is then applied to both overlay and direct internet breakout traffic, considering the number of active flows and the packet queue delay on each path or link.

Sub-Second Failover Capabilities

In unified SASE gateways and unified SASE clients, once an application is identified, per-flow traffic steering is executed according to the AppX policy configuration and real-time link conditions. The sub-second failover allows applications to swiftly switch to a better link in the event of link failure (blackout) or degradation (brownout) on overlay paths.

Additionally, with Netskope's intent-driven policies, customers can customize the AppQoE rules. For instance, setting a particular app as Voice/High priority automatically ensures the selection of the best path, QoE, and UDP optimization for high-priority voice traffic. These intent-driven policies greatly improve operations by eliminating manual configuration and ongoing maintenance when links are added or changed at the branch.

This path selection functionality is available at both unified SASE gateways and unified SASE clients, which converges SD-WAN and Secure Service Edge (SSE) capabilities.

With the laptop running a unified SASE client, end-users can utilize multiple links, such as both Wi-Fi and LTE tethering from the phone, as WAN transports, enabling the deployment of active/active or active/standby paths. Additionally, customers have the flexibility to define policies based on processes running on the laptop that is powered by a unified SASE client. For example, customers can lower the traffic priority of the Netflix process.

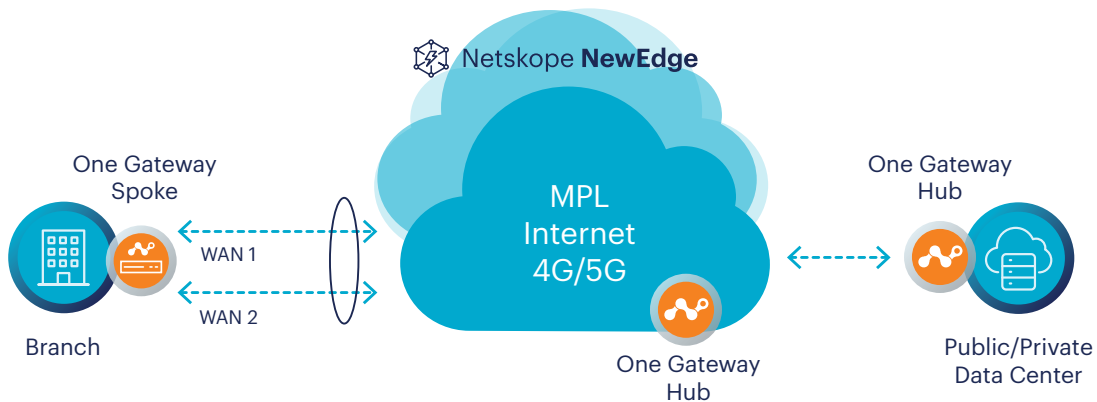


Figure 2: Bandwidth Aggregation in Next Gen SASE Branch

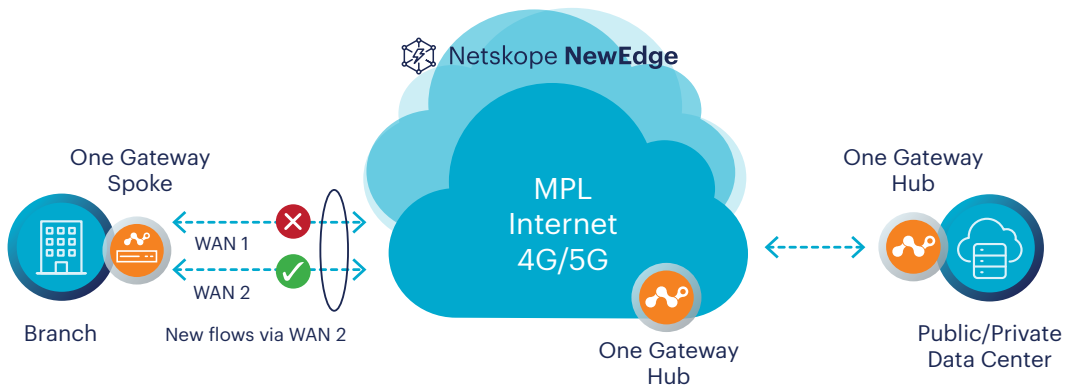


Figure 3: Sub-Second Failover Capabilities in Next Gen SASE Branch

MITIGATING NETWORK DEGRADATION WITH ON-DEMAND REMEDIATION

When faced with a single degraded WAN link or if all WAN links experience degradation (i.e., packet loss), the unified SASE gateways or unified SASE clients use remediation mechanisms to mitigate poor network quality.

UDP Remediation

For UDP-based applications like voice and video conferencing (e.g., RingCentral, Zoom), Borderless SD-WAN employs Forward Error Correction (FEC) techniques such as packet duplication to counter the effects of packet loss. Real-world tests have demonstrated the effectiveness of this approach, with voice quality mean opinion score (MOS) remaining above 4 (indicating high quality) and video frame rates holding steady even under degraded network conditions.

TCP Optimization

For sites with high-latency WAN links, Netskope unified SASE gateway provides TCP optimization to reduce latency and increase the average throughput of select TCP traffic as configured in the AppX policy. The link latency is remediated on demand for these critical TCP applications by enabling the Transparent TCP Proxy feature on the unified SASE gateway.

In the example below, a user is downloading a 2 GB file via SMB (Server Message Block) over a WAN link with a latency of 400 ms, operating at an average speed of 250 KB/s. However, with Netskope unified SASE gateway, the file download occurs at a speed of 1.31 MB/s resulting in approximately a 5x faster download speed.

Enhanced AppQoS

A traffic class is defined with a combination of priority (high, normal, or low) and service class (voice, video, transactional, or bulk), creating a 4x3 matrix with 12 traffic classes. The application/category and scheduler weight can then be mapped onto these traffic classes. All applications within a traffic class will receive aggregate QoS treatment, including scheduling and policing. Each application in a given traffic class is ensured a guaranteed minimum bandwidth during congestion based on the scheduler weight (or percentage of bandwidth). For example, Zoom is automatically designated as high priority/Voice and Video with a CCI of 88, whereas SureVoIP, with a CCI of 36, is classified as low priority/Voice. These AppQoS Smart Defaults for QoS are universally applied out of the box to 80K+ applications, eliminating shadow IT issues stemming from visibility gaps and improving network efficiency.

In the absence of congestion, applications are permitted to burst up to the maximum aggregated bandwidth. Bandwidth capping policies can be implemented for all applications within a given traffic class. The business policy incorporates predefined smart defaults that map to 80K+ applications to traffic classes, allowing customers to immediately benefit from application-aware QoS without the need to define a policy. Customers also have the option to create policies for their custom applications. Each traffic class is assigned a default weight in the scheduler, as illustrated in the provided figure, and these parameters can be adjusted within the business policy.

Inbound QoS in Next Gen SASE Branch

Furthermore, Netskope SASE extends context-aware QoS benefits to cloud, web, and SaaS traffic using multiple internet links and an SD-WAN overlay via NewEdge. This also enables advanced capabilities like inbound QoS from Cloud toward the Branch. For example, when customers attempt to access Hulu traffic, outbound request traffic is minimal, and most of the traffic is inbound. In traditional WAN setups, by the time traffic reaches the edge router, it is too late to determine whether the link lacks sufficient bandwidth, potentially leading to WAN link congestion. Netskope SASE's inbound QoS ensures that a streaming application like Hulu does not exceed the configured inbound bandwidth.

Hierarchical QoS in Next Gen SASE Branch

Netskope unified SASE gateway and unified SASE client support a four-level hierarchical QoS, Weighted Fair Queuing, and Low Latency Queuing. The four levels encompass Aggregate (all overlays), Segments (VRF), Traffic Class, and group of applications. This enables customers to exercise granular control per Segment/Traffic Class/Application, allowing them to set Bandwidth Allocation, Rate-Limit, or Weight (Prioritization). Customers have the option to utilize the built-in application database or define custom applications based on IP/port/domain.

Dynamic AppQoE

Netskope offers advanced Dynamic AppQoE, where a different QoE policy is applied dynamically based on events like a link going down. For example, consider a scenario where you have a broadband and a cellular link. Let's say Netflix consumes 5% of the bandwidth when all links are available. If the broadband link goes down, the traffic is automatically rerouted to the available cellular link. However, since cellular is the only available link, the customer may want to apply a stricter QoE policy (e.g., adjusting Netflix dynamically from 5% to 0%). This allows other high-priority traffic like voice/video to be routed without impacting the user experience. Additionally, Netskope SASE provides dynamic cellular usage control, enabling users to define metering thresholds on WAN links and restrict cellular usage only for business-critical apps via policy. Metering can be done at the interface level and directly for SIM cards, with built-in life-cycle management for SIM cards to add bandwidth on-demand.

Per-Traffic Class Policing

An IT administrator may want to police high-priority business collaboration traffic on the aggregated overlay tunnel to ensure that a service provider's offered SLA is honored. Policing is applied by default for traffic classes marked as real-time.

DSCP Marking

At the Netskope unified SASE gateway or unified SASE client, when traffic is received, the customer's designated DSCP values can either remain unchanged or be adjusted before they are transmitted through the tunnel. Additionally, the outer DSCP value on the tunnel header can be altered or replicated from the inner packet.

This packet duplication remediation feature is utilized on traffic that is classified as high priority/Voice.

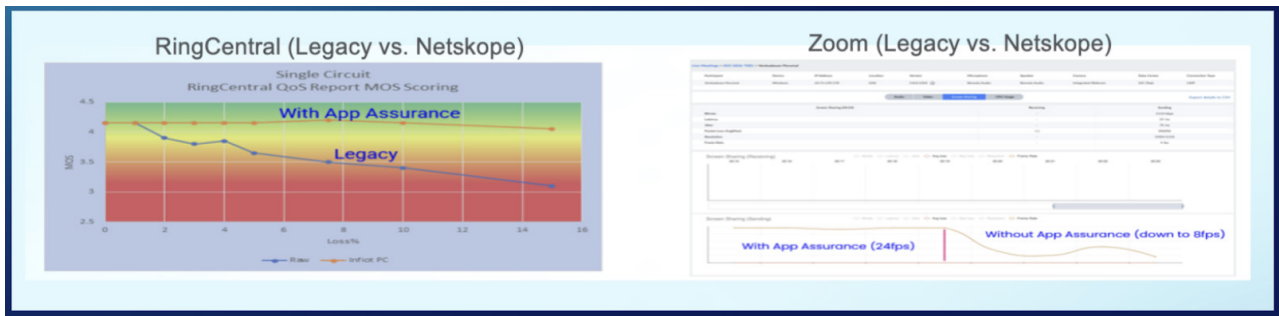


Figure 4: UDP Remediation

Figure 5: Configuration to Enable TCP Optimization with Netskope SASE Orchestrator

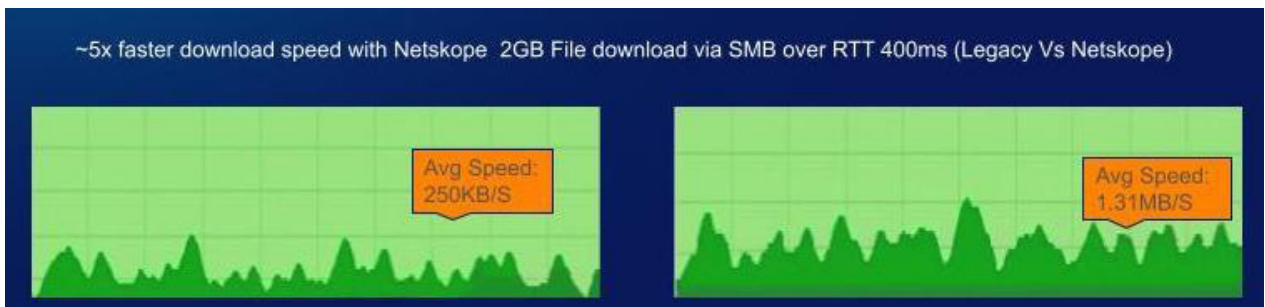


Figure 6: TCP Optimization Results

Bandwidth Guarantee & Queuing

		High	Medium	Low
Voice	Realtime	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Guaranteed	10	3	1

Figure 7: How Policy is Applied on Real-Time Traffic Classes

Editing Policy spoke-policy


VoIP


Match Criteria — Priority — Path — Preferred Exit — Finish


Select Priority


- High
- Medium
- Low
- Drop
- Auto


Traffic Class


 AUTO


 VOICE


 VIDEO


 TRANSAC


 BULK

Rate Limit

DSCP Marking

Inner Pack...
 as-is

Outer Packet
 46-EF

Figure 8: How DSCP Marking Configuration for Inner and Outer Packet

OPTIMIZING CLOUD TRAFFIC WITH NETSKOPE NEWEDGE: ENHANCING PERFORMANCE AND RELIABILITY

Moreover, Netskope's Next Gen SASE Branch solution extends its capabilities to the cloud by seamlessly integrating Borderless SD-WAN within NewEdge. This integration extends context-aware Quality of Service (QoS) benefits to cloud, web, and SaaS traffic, while also providing advanced features such as inbound QoS.

Additionally, all benefits including active-active links, sub-second failover, TCP/UDP optimization, and first-packet detection ensure optimized performance across all cloud and SaaS applications. First-packet detection enables precise and secure breakout of internet-bound traffic, directing it to the appropriate path based on application-driven business and security policies. This eliminates the risk of wasted bandwidth and performance bottlenecks for SaaS and web traffic.

NewEdge is a purpose-built private SASE cloud that currently includes over 100 data centers in 74+ metro regions around the world and provides a localized experience available in every country globally (via 200+ Localization Zones). NewEdge boasts 3,200 network connections to 650 ASNs and participates in over 100 internet exchanges, ranking among the top 15 most connected networks. This reduces reliance on transit providers, leading to optimal performance, low latency, and increased availability, thereby enhancing user and application performance. Netskope NewEdge employs STM (Synthetic Transaction Monitoring) and RUM (Real User Monitoring) metrics to identify underperforming autonomous systems and segments along the path, triggering automated fixes. In addition, BGP routing optimization selects the best peering network from the active PoP for the user's connection to the application. NewEdge is high-performing, typically offering single-digit millisecond latency for the vast majority of the world's knowledge workers.

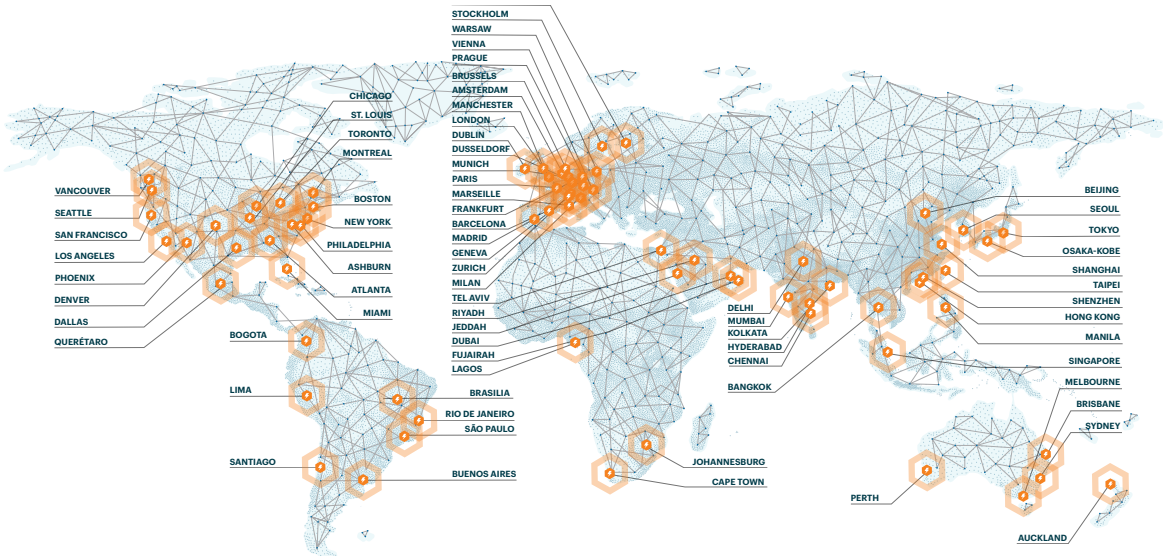


Figure 9: Netskope NewEdge Network (as of 06-11-2024)

SUMMARY

In conclusion, the rapid expansion of cloud applications and the shift toward hybrid work models have underscored the critical need for reliable and secure connectivity solutions. Traditional SD-WAN deployments, while effective in some contexts, often fall short in providing seamless access for remote users, leading to productivity challenges and increased costs.

The Netskope Next Gen SASE Branch emerges as a comprehensive solution tailored to meet the evolving demands of the borderless enterprise. By integrating Context-aware SASE Fabric, Zero Trust Hybrid Security, and SkopeAI-powered Cloud Orchestrator into a unified cloud offering, Netskope not only addresses the current challenges but also streamlines operations by seamlessly consolidating networking and security in one converged platform called Netskope One.

The Netskope One platform embodies its unified elements in the Next Gen SASE Branch, enabling infrastructure modernization. Powered by Borderless SD-WAN, this solution optimizes application performance and ensures uninterrupted user experiences by intelligently managing traffic across multiple WAN links Forward Error Correction techniques. Moreover, its ability to establish and adapt overlay paths between various endpoints, data centers, and the Netskope NewEdge platform enhances agility and resilience in the face of evolving network conditions.

As businesses continue to embrace digital transformation and hybrid work models become the norm, Netskope's Next Gen SASE Branch stands as a beacon of innovation. It offers a path toward a fully modernized branch experience where connectivity is optimized, seamless, secure, and scalable. With its holistic approach to networking and security, Netskope empowers organizations to navigate the complexities of the digital economy with confidence, enabling them to focus on driving growth and maximizing revenue generation.

Interested in learning more?

Request a demo

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.

©2024 Netskope, Inc. All rights reserved. Netskope, NewEdge, SkopeAI, and the stylized “N” logo are registered trademarks of Netskope, Inc. Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index, and SkopeSights are trademarks of Netskope, Inc. All other trademarks included are trademarks of their respective owners. 07/24 WP-747-3