Network Scorecard For The Netskope NewEdge SASE Cloud

A Broadband-Testing Report

First published April 2024 (V1.0)

Published by Broadband-Testing

E-mail : info@broadband-testing.co.uk
Internet: HTTP://www.broadband-testing.co.uk

TABLE OF CONTENTS

.....i

TABLE OF CONTENTS..... 1

BROADBAND-TESTING 2

EXECUTIVE SUMMARY 3

SASE CLOUD SOLUTIONS: THE NETWORK SCORECARD 3

THE NETSKOPE SASE SCORECARD..... 4

1. Public Versus Private Cloud 4
2. Where Are The Servers? 5
3. Who Controls The Network? 7
4. What Services Run Where? 9
5. How Is The Capacity Managed?.....12
6. How Is Performance Validated?.....13
7. What Happens When Something Breaks? 14
8. How Do You Pay Them? 15

IN CONCLUSION..... 16

Figure 1 – Netskope NewEdge Global Coverage.....4

Figure 2 –NewEdge Localisation Zones.....6

Figure 3 – NewEdge Global IX Participation 7

Figure 4 –Netskope One Services.....10

Figure 5 –NewEdge Average RTTs 13

BROADBAND-TESTING

Broadband-Testing is an independent testing operation, based in Europe. Broadband-Testing interacts directly with the vendor, media, analyst, consultancy and investment communities equally and is therefore in a unique space within IT.

Testing covers all aspects of a product/service from business rationalisation in the first instance to every element – from speed of deployment and ease of use/management, through to performance and accuracy.

Testing itself takes many forms, from providing due diligence for potential investors through to public domain test reports.

Broadband-Testing is completely vendor neutral and independent. If a product does what it says on the tin, then we say so. If it doesn't, we don't tell the world it does what it cannot do… The testing is wholly complementary to analyst-related reports; think of it as analysts getting their hands dirty by actually testing what's on the latest hype curve to make sure it delivers on its claims and potential.

Broadband-Testing operates an **Approvals** scheme which prioritises products to be short-listed for purchase by end-users, based on their successful approval, and thereby short-cutting the evaluation process.

Output from the testing, including detailed research reports, articles and white papers on the latest IT technologies, are made available free of charge on our web site at HTTP://www.broadband-testing.co.uk

EXECUTIVE SUMMARY

- To paraphrase a classic quote, "not all solutions are created equal"..
- For the potential end-user of a SASE cloud, be it a branch site, remote user or even connected IoT device, the fundamental problem is in understanding and interpreting what a SASE cloud vendor actually means by their description of the infrastructure.
- Simple differences in approach, such as a vendor owning its own delivery network, rather than outsourcing – say via a public cloud service provider (CSP) can have a huge impact on the quality of the SASE delivery.
- How capacity is managed can have a huge bearing on the true scalability and flexibility of a SASE offering.
- The actual costs of a SASE solution can often be very difficult to calculate, especially over a longer time period.
- In this scorecard report we are evaluating Netskope's NewEdge SASE Cloud solution against our pre-defined criteria. In summary it met all our expectations and has no obvious weaknesses.

SASE CLOUD SOLUTIONS: THE NETWORK SCORECARD

While clearly there is no "one size fits all" solution for companies looking to invest in SASE solutions, there are a number of common factors that can be used to evaluate a vendors' SASE offering.

In a previous white paper, we defined in detail the areas that we feel are the most relevant to consider, with approximate weightings for each category. This report can be read in full here:

http://www.broadband-testing.co.uk/site/wp-content/uploads/2024/01/Network-Scorecard-For-SASE-Report-Final.docx.pdf

Briefly, the areas we have chosen to focus on are:

- Infrastructure dependencies (public vs private)
- Global footprint (server locations)
- Responsibility model (network control)
- Services menu (what services run where)
- Capacity management (scalability and adaptability)
- Performance optimisation (validating performance)

We will now focus on how Netskope's NewEdge SASE Cloud solution meets those requirements, category by category.

THE NETSKOPE SASE SCORECARD

1. Public Versus Private Cloud

The first element of a SASE solution to understand is: does the vendor actually own and operate its own delivery network or is it based on a public cloud/hyperscaler?

Netskope is clearly a firm believer in having its own network and dedicated network delivery architecture, having tried using the public cloud prior to 2018 and finding it far too restrictive and limited, both geographically and in terms of performance capabilities, the two being naturally intertwined. There is also the very real factor that a public CSP is obviously going to prioritise its own commercial traffic and services over those of a subscriber and, moreover, isn't going to being interested in resolving individual performance problems. Additionally, a SASE vendor stands to lose significant control of its service delivery by relying on a 3rd-party, especially when trying to differentiate its service offerings or troubleshoot issues.

The company has since invested more than $250m deploying its NewEdge network (see figure 1), with over 200 individuals dedicated to its platform engineering team. It is worth noting that this was the same set of individuals who previously built some of the world's largest public clouds and CDNs, including AWS and Limelight – not a bad CV. Taking a private cloud approach gives Netskope full control of its infrastructure. It means that – rather than relying on public clouds - or where not all services are available in every region - there is no backhauling of traffic required with its NewEdge architecture and the company retains complete control over all networking aspects of service delivery

Feedback from a user base exceeding 3,000 customers suggest that NewEdge was a key factor in their selection process in three key areas: it makes Netskope more accountable for end-to-end performance; it allows for more robust SLAs and – finally – it avoids the problem-related finger pointing that is common with vendors relying on 3rd-parties.

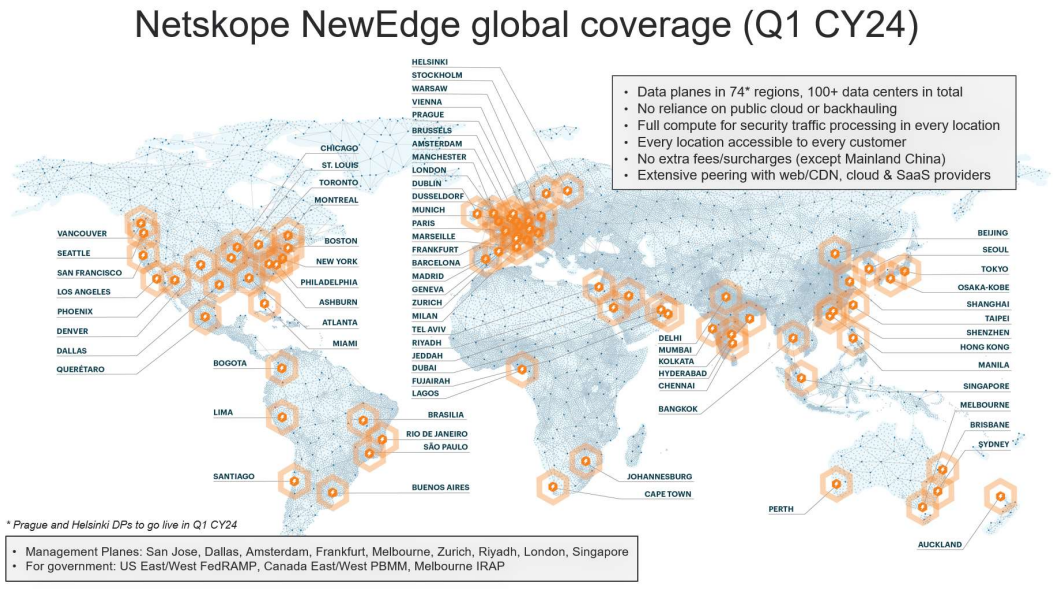


Figure 1 – Netskope NewEdge Global Coverage

Basing NewEdge on a private cloud approach - with its own dedicated infrastructure built on bare metal – give Netskope true edge compute capability and full control over deployment and expansion into new regions. From a customer perspective, it means that their requirements concerning coverage, performance, resilience, and data sovereignty can be met – Netskope is not limited in any way by a 3rd-party provider that may not have a presence in a specific required region.

Notably, Netskope supports single-click data sovereignty law compliance, allowing customers to limit which countries data can reside in and - in some cases - also restricts where their traffic can flow (or more specifically, be decrypted). For example, many NewEdge regions contain deployments with multiple DCs (Management Planes and Data Planes), to provide service resilience, allowing customers to restrict where traffic processing occurs, as well as controlling where sensitive data, such as logs and metadata are stored (e.g. Australia, Saudi Arabia, Switzerland, US, UK, Singapore, Netherlands, and Germany). Moreover, Netskope claims it is alone in providing true 100% data residency and sovereignty within the Kingdom of Saudi Arabia. The same is true for Switzerland, allowing full compliance with Swiss banking secrecy laws, as well as the newly enacted revFADP regulations.

2. Where Are The Servers?

Many aspects of a SASE solution can all too easily be taken for granted by a potential customer, not least when dealing with a huge global vendor, but the reality is that even the most basic aspects of a proposed solution should be questioned, starting with: where exactly are the servers?

The global footprint of NewEdge currently includes full compute DCs running a complete SASE stack across 72 unique regions. Based on available public domain information from other vendors, this would appear to put Netskope in a positive light; two examples we found from SASE vendors who are very well-established global security product providers suggests that one has 63 unique regions with the other topping out at around 40; factor in in reliance on the public cloud for service delivery and it's not clear, even then, whether every region offers complete service delivery capabilities. It really is important for ALL SASE vendors to be very clear and specific as to exactly WHAT they can offer WHERE. You have been warned…

Below is a list of the full compute NewEdge DCs within major geographical regions, with details on specific DC locations provided on Netskope's publicly available Trust Portal at https://trust.netskope.com/. This does not include completely isolated environments that support government compliance programs including US FedRAMP HIGH and Canada Protected B/medium integrity/medium availability (also known as Canada PBMM).

- **27** DCs in the US/Canada
- **10** in Mexico/Latin America
- **31** in Europe/Middle East/Africa
- **23** in Asia Pacific
- **6** in China (including Hong Kong)

Each NewEdge DC is fully autonomous and deployed in a carrier-neutral colocation facility with optimal connectivity. In addition to providing country-specific coverage and continuing to add new regions (such as Finland, Portugal and Czech Republic targeted for the 1H 2024), Netskope has factored n-region resilience into NewEdge by deploying multiple DCs to maintain inline processing in-region, even in failover situations. And this is ongoing; for example, in Q4 2023 through Q1 2024, new regions added include Philadelphia, PA and St, Louis, MO, both in the US, as well as DC expansion in existing regions including Delhi and Chennai, India; Madrid, Spain; Bogota, Colombia; and New York, NY. This expansion is five years in the making to date, which translates into a high investment policy – exactly what is needed, in other words. To paraphrase a classic: DCs don't grow on trees in nature. Put another way, no one ever said creating a global SASE deployment was either cheap nor easy – it involves serious financial commitment.

As illustrated in the below diagram, the NewEdge full compute DCs are further supported by Localisation Zones (LZs) which extend Netskope coverage to 220 countries/territories worldwide. LZs are another key component in ensuring performance, resilience and optimising the user experience, In regions where NewEdge DCs are not yet deployed (e.g. Turkey or Indonesia), LZs still provide a localised content experience. For example, a user in Indonesia connecting to the Singapore or Bangkok DCs would maintain content localisation and native language support (e.g. Bahasa). In this case, LZs allow the Singapore or Bangkok DCs to emulate the Indonesian locale without additional traffic backhauling. Netskope also provides LZs for regions with a single DC so that, in the event of an outage or maintenance event, content localisation is maintained for users as they connect to out-of-region DCs. Technical documentation on LZs is available at https://docs.netskope.com/en/netskope-help/data-security/netskope-secure-web-gateway/security-cloud-platform-configuration/#Localisation-zones-1.

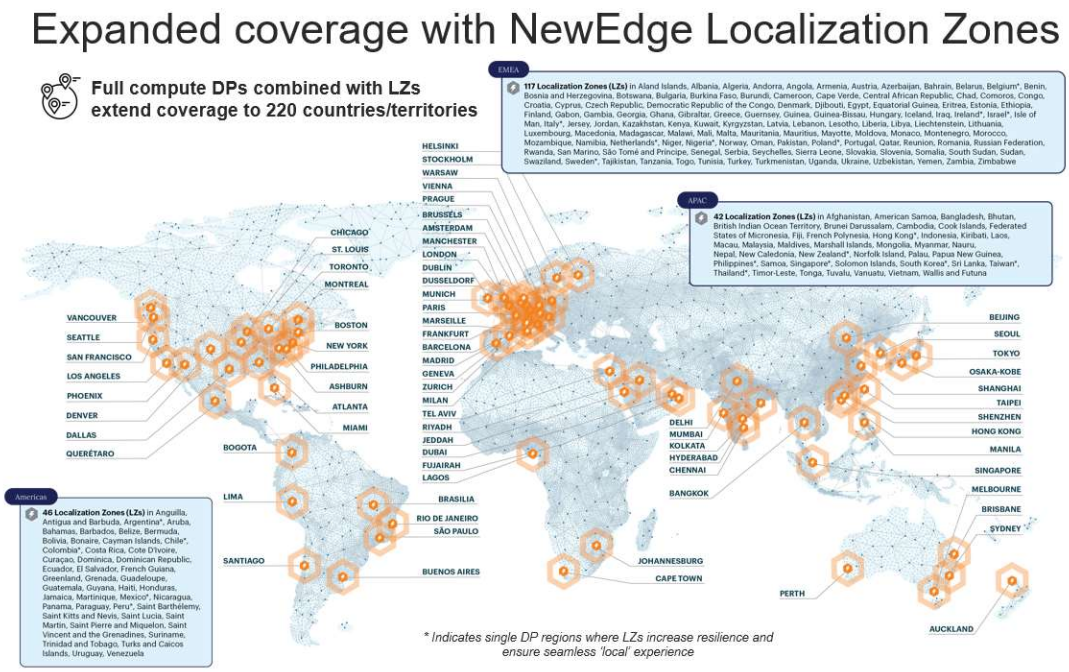


Figure 2 –NewEdge Localisation Zones

With NewEdge Traffic Management, which is based on Netskope's customised global server load balancer solution, the on-ramp of user/branch traffic is based on selecting the "nearest" DC, based on current health and lowest latency status, using an algorithm based on real-time RTT (Round Trip Time) measurements to identify multiple DCs (up to 10). This is designed to ensure optimal connectivity, as well as guaranteed performance and continuous service delivery, regardless of the network status.

This approach addresses the performance and data provenance issues prevalent with other techniques – notably Virtual PoPs - which can simply be a "front door" for accessing a non-adjacent location and often involve complex routing with an inevitable performance hit - or the "exit node" method, where egress traffic is routed internally from the DC and filtered to a node in the egress country, before exiting onto the open Internet - again creating major potential performance issues. With its combination of full compute DCs (with full transparency) and the addition of LZs, Netskope has clearly done its homework in terms of what is needed for optimising global service delivery and maintaining local content, compliance requirements and the all-important user experience – all in a fully-secured environment.

3. Who Controls The Network?

Directly related to the question of server location is "who is controlling the delivery network?" Moreover, how much control of that network does the SASE supplier have?

As part of Netskope's full control over its network infrastructure, every NewEdge deployment is standardised, by means of a "DC factory" approach, giving both rapid deployment capabilities and infrastructure consistency. In a sense, it's not that dissimilar to the standardised approach taken by giant retail or hospitality companies when rolling out new locations. For example, NewEdge DCs do not rely on non-modifiable, 3rd party vendor hardware, such as load-balancers or SSL accelerators.

To optimise network performance, every NewEdge DC is extensively interconnected with direct peering to Microsoft and Google in every region possible, as well as primary web/cloud/SaaS providers (e.g. AWS, Salesforce, IBM Cloud, Oracle etc) and ISPs. Also notable that Netskope supports public (IX) or private (PNI) peering NewEdge DCs directly with customers' networks.

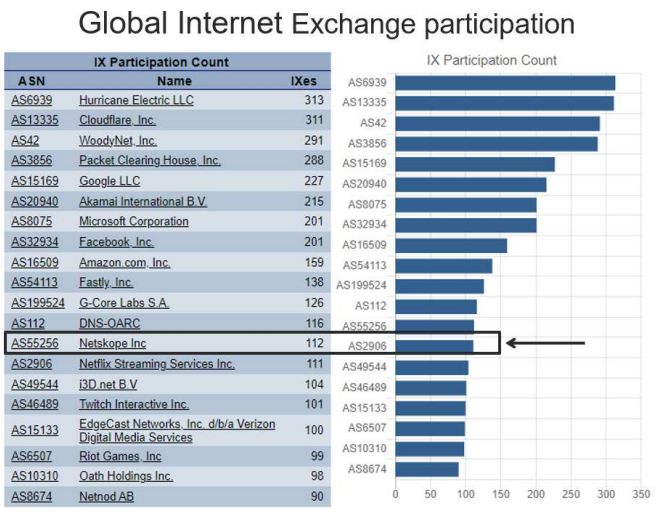


Figure 3 – NewEdge Global IX Participation

At the time of creating this report - Q1 CY24 - NewEdge had 3,200+ networks adjacencies across 640+ unique ASNs (Autonomous System Number) and was ranked as one of the 'top 15' most active participants in global participation: (Source: https://bgp.he.net/report/exchanges#_participants). **Note:** IX is a neutral infrastructure designed for immediate exchange of connections and inter-operator traffic exchange between independent Internet-based networks. So, a combination of extensive peering relationships and a widespread interconnection strategy, is Netskope's answer to avoiding the longstanding and dreaded security:performance trade-off for the users.

Again, from a customer perspective, this interconnection strategy is designed to simply the network expansion and transition from traditional MPLS-based backhaul to direct-to-net, while cutting costs on private links. It means that NewEdge can employ both hot and cold-potato routing depending on what works best for a given service, in order to achieve the best end-to-end, lowest-latency performance – another benefit of not relying on 3rd - party infrastructure and losing control over service delivery as a result For example, for web security and proxy services, Internet-bound traffic ingresses and egresses from a single NewEdge DC with no backhauling. It means that using a mix of interconnections - including both peering and premium transit - "hot potato routing" can be used to deliver the best performance in this use-case by performing security processing at the edge with the lowest possible latency. It's worth noting that this strategy also adheres to SaaS provider guidelines, such as the Microsoft 365 network connectivity principles.

Equally, for ZTNA (or VPN replacement) and SD-WAN use cases, a customer's private traffic may transit between NewEdge DCs via cold-potato routing, with NewEdge optimising the long haul (or "middle mile") across its global WAN. As an example, if a ZTNA user were in Los Angeles connecting to an application in New York, the user in LA would be connected to one of two nearest (lowest latency) NewEdge DCs in the LA region, while the application in NY would be connected to one of four DCs in the NY area, and then the "middle mile "traffic between LA and NY would be optimised across NewEdge. It's simply applied logic, but it requires that infrastructure to be in place - a technology innovation which Netskope markets as Route Control.

It also means NewEdge can extend networking capabilities directly to customers; for example, through IP ranges devoted to its Dedicated Egress IP Address (DEIP) offering. DEIP is a fully managed service, directly integrated within NewEdge, whereby Netskope-owned IPs are allocated for exclusive use by customers. This overcomes a common problem associated with cloud services, namely shared IP address space and the potential risk of compromise or misuse of these IPs, which can then have a "knock-on" effect to other customers. Technical documentation on DEIP is available at https://docs.netskope.com/en/netskope-help/data-security/netskope-secure-web-gateway/security-cloud-platform-configuration/#dedicated-egress-ip-footprint-1.

Having full network control means that Netskope can allocate dedicated IPs in every DC, as well as supporting regional inline traffic restrictions. The Netskope DEIP service includes the provisioning of additional IPs as needed such as managing versioned DC footprints as new DCs are deployed and monitoring the service to avoid port exhaustion. In addition, Netskope supports "Bring Your Own IP" (BYOIP) and allows customers to transfer their own IPs to be used for NewEdge egress traffic. Control is further extended

to customers with NewEdge Traffic Management Zones, allowing them to define where inline security traffic processing occur: for example, in selecting from 20+ predefined options (e.g. Australia, Brazil, EU, Germany, India, Japan, KSA, Switzerland, USA etc) and automatically incorporating new DCs as they come online with no customer involvement required. It is worth checking how other SASE vendors compare in terms of these capabilities.

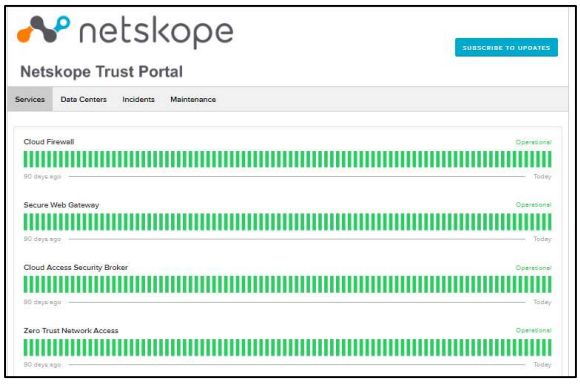
Netskope also provides a variety of methods for customer control over traffic steering to NewEdge. For example, IPsec and GRE tunnel selection can be configured without Netskope involvement, allowing DCs in specific regions to be selected along with failover options. Moreover, customers may choose to configure *their* network devices to manage traffic flows (e.g. by user, app, destination) to specific DC regions. This approach allows for interoperability with any router, NGFW or SD-WAN device, as well as Netskope's own Borderless SD-WAN solution. In addition, NewEdge supports managed and unmanaged access for remote workers and 3rd parties (such as partners, suppliers and contractors) to key SaaS and private applications using Reverse Proxy and clientless "zero trust" private access techniques. The bottom line here is flexibility – it gives the customer options.

Note: with Borderless SD-WAN, Netskope aims to address all the key feature requirements of SD-WAN around optimised connectivity and, combined with Netskope's SSE, delivers a cloud-native, fully converged and single-vendor SASE solution. At its core is the classic single pane of glass orchestrator, the global footprint of NewEdge DCs, and a "thin branch" solution that optimises and secures traffic from all locations and users (including via Netskope's very own client) to cloud and on-premise locations.

4. What Services Run Where?

It's all too easy to assume that, when a vendor cites the existence of a PoP or compute location, that it will support the complete scope of available SASE services. But this might easily not be the case.

Mentioned earlier in this paper, the first thing to re-emphasise is that every NewEdge location has full compute for real-time security traffic processing, plus a complete stack of SASE services available in these locations. This contrasts with a public cloud-based vendor offering which might typically have different services available in different regions, rather than complete, global coverage. Importantly, this full compute/stack approach eliminates the need for backhauling traffic inside the NewEdge network. The alternative typically involving building a delivery network using a mix of real and virtual appliances, with different services residing in different locations. The cost, scalability and performance implications of this approach are suitably obvious; latency can be a real issue as traffic inspection can occur multiple times. In comparison, the NewEdge architecture relies on a single-pass, microservices-based architecture,



minimising latency and performance fluctuations. Again, it's about resolving the performance:security trade-off.

Core SASE services, in addition to SD-WAN, that are delivered from NewEdge are listed below, plus the full Netskope service menu, including information on uptime and availability for all of its services publicly available on the company's Trust Portal:

- **Cloud Firewall** - Secures all ports and protocols with firewall rules for user and office egress traffic with central administration, global access via NewEdge DCs, and tying into the Netskope single-pass, SASE-ready architecture.

- **Cloud access security broker (CASB)** - Enables enterprises to quickly identify and manage the use of cloud applications — regardless of whether managed or unmanaged — to prevent sensitive data from being exfiltrated by risky insiders or malicious cybercriminals.

- **Secure Web Gateway (SWG)** - Tightly integrated into Netskope CASB, DLP and Threat Protection via common policy controls, Netskope SWG prevents malware, detects advanced threats, filters by category, protects data, and controls app use for any user, location, or device.

- **Zero Trust Network Access (ZTNA)** - In contrast to traditional VPNs that grant users access to entire network subnets and Virtual LANs (VLANs), Netskope Private Access provides "zero trust" access to applications – including those hosted on-premises, or in public cloud environments – to protect data and guard against lateral movement with application-level access controls based on user identity and device security posture.

The core services listed above are just a subset of what is available from the Netskope Security Cloud, or what the company is now branding as the Netskope One. The following diagram provides a more comprehensive overview of the complete Netskope offering that is powered by NewEdge.

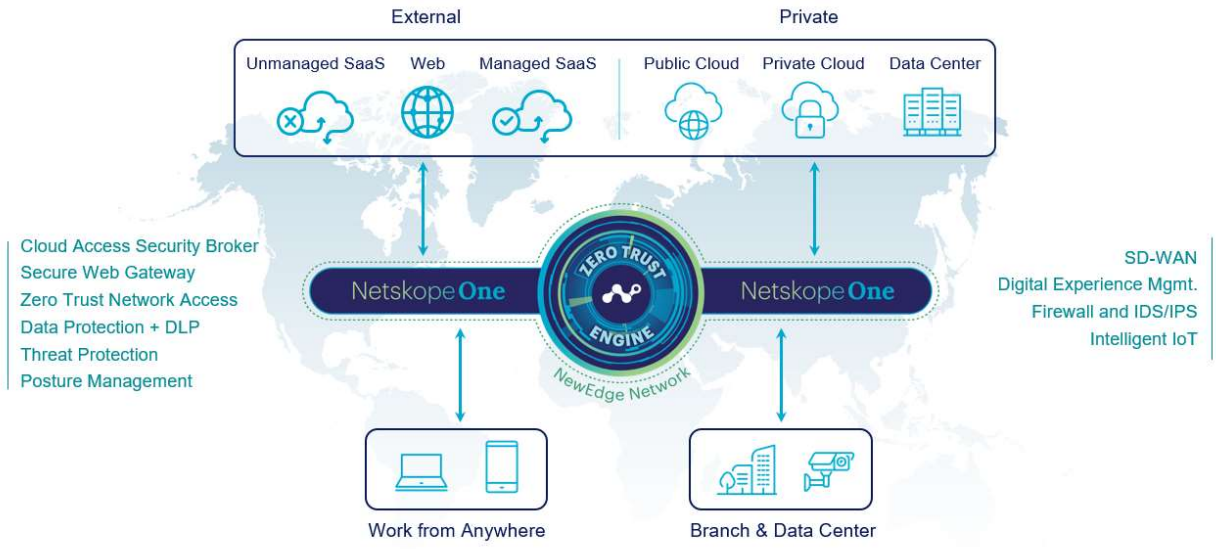


Figure 4 –Netskope One Services

With every Netskope service running essentially in all of its DC regions, the DC architecture, and specifically its traffic-processing DPs, handle end-user traffic and act as a forward proxy leveraging various steering methods, such as by tunnel type (e.g. GRE, IPSec), the initiation method (e.g. Netskope Client) or the technique (e.g. Proxy Chaining).

Each steering method is terminated in a specific way, with gateways within NewEdge specialised in terminating tunnels and handling the inner packet flows. Inner packet flows are then addressed based on the service (or services), such as CFW, SWG or CASB, for example. Both requests and responses are scanned as necessary by Netskope's DLP and Threat Protection engines (which are part of Netskope's larger data-centric and context-aware traffic processing technology called Zero Trust Engine, depicted in the diagram above). For each of the different services, events (per application, page or policy) are sent to the NewEdge MPs. The MPs house the infrastructure for the administrative interface (or Netskope Admin UI) for configuring all services and related policies, data storage (of customer-specific logs and metadata), as well as integrations with other cloud services.

Within NewEdge, as services like SWG or CASB process traffic, encrypted flows can be decrypted and inspected in real-time, at line speed, with some DCs handling upwards of one billion encrypted connections daily. Netskope understands the need for high-strength ciphers and includes native support for TLS 1.3, reducing any security risk through downgraded connections. Customers retain complete control over how specific services address traffic via comprehensive policies – for example, based on domain, category, user/group or network location – for what traffic gets decrypted, inspected or potentially exempted from processing. For services like Netskope ZTNA, NewEdge securely connects users to private resources and apps with end-to-end traffic encryption, as well as incorporating zero trust concepts so private resources remain hidden and shielded from discovery and attacks, with only authenticated users gaining access.

Earlier in this paper we addressed the global coverage of the NewEdge private cloud with a combination of full compute DCs plus LZs, but one differentiator of the Netskope solution is the availability of its full menu services inside Mainland China. While many SASE customers will have historically utilised processing locations in Hong Kong, multinational giants often have a significant number of roaming users or sites inside mainland China. This means that providing a fully optimised service here too, with local applications and content support, clearly has great potential value for many companies. It also reduces the potential compliance issues associated with shipping traffic outside of the Mainland to Hong Kong (or other regions) for processing.

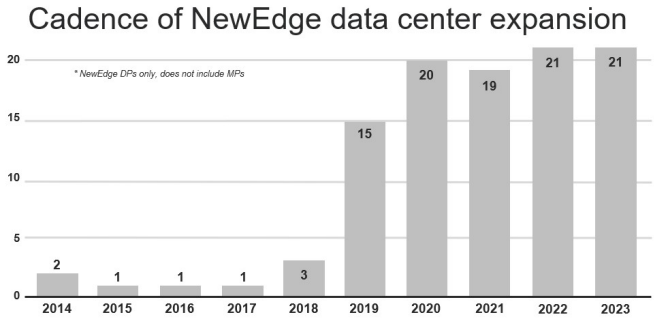
In the case of SASE vendors relying on public cloud infrastructure which may lack a presence inside the Mainland, they are unable to deliver their services in-region. In contrast, Netskope has multiple DCs deployed in the region, combined with multi-provider connectivity and high-priority international routing, plus tiered service offerings with options specifically tailored to addressing the challenges of domestic versus international traffic patterns.

5. How Is The Capacity Managed?

Of all the IT buzzwords of the past decade, "scalability" surely has to be right up there with the most overused.

As mentioned earlier in this paper and illustrated in the chart on the next page, the expansion of NewEdge has been ongoing over the last five years and represents a significant investment in expanded coverage, as well as capacity.

With Netskope's streamlined deployments and "DC factory" approach mentioned earlier in this document, the fastest NewEdge DC deployment took just eight days, from the time the rack arrived at the colocation facility to when it started receiving customer traffic. In using the same technical approach favoured by the world's largest cloud hyperscalers, Netskope can target and deploy additional capacity very quickly, when and where it's needed, without dependencies on 3rd-parties or the limitations of their global footprint. This approach also allows Netskope to do a better job on pre-planning its infrastructure expansion - for example, to stay ahead of potential supply chain issues.



We already highlighted the single-pass architecture, but it's important to re-emphasise how important it can be to scalability and capacity management. The individual security and networking functions in the Netskope Security Cloud are broken down into "microservice" building blocks and take a container-based approach, so are loosely coupled but independent, meaning it won't hog compute resource when it is not needed.

It also makes both day-to-day management and scalability of NewEdge both easier and less expensive to achieve and – once more – removes the security versus performance trade-off. It also makes capacity planning easier and, combined with NNetskope's conservative capacity management philosophy, keeps actual utilisation of NewEdge DCs at very low levels at all times, meaning capacity is always available on-demand.

It also effectively means that bandwidth is infinite, from the perspective of service delivery capabilities. Netskope focuses on using a low threshold for resource usage levels, so the idea is to always be pro-active and completely remove the bandwidth issue – even as a required metric from a management perspective. If it involves adding extra DCs, then that is the Netskope approach, rather than simply trying to balance costs against capacity issue damage limitation.

6. How Is Performance Validated?

Performance validation is fundamental in choosing a SASE provider. A vendor needs to be able to demonstrate exactly how its performance is validated and guaranteed.

Netskope's ongoing investment in global network expansion is primarily about one issue – optimising performance. We've already covered the different architectural elements of the NewEdge delivery network and why it is geared towards minimising latency and maximising service delivery and performance.

The on-ramp performance for steering traffic to NewEdge is claimed to be industry-leading. This is achieved by the selection of premium transit combined with extensive peering and an aggressive interconnection strategy to ensure NewEdge is connected to the right "eyeball networks" via T1/T2 ISPs for receiving last mile connections from users/sites, as well as on the northbound side optimising the path to web, cloud, or SaaS destinations which users are accessing. The below chart includes Netskope results for average round-trip times (RTT) in milliseconds from global Catchpoint backbone test nodes to the ingress of its NewEdge network. Netskope also provides an online Speed Test to help customers evaluate on-ramp performance with NewEdge versus alternative solutions found at https://www.netskope.com/netskope-one/newedge#speed-test.

Metro/region	Average on-ramp latency (ms)	Metro/region	Average on-ramp latency (ms)	Metro/region	Average on-ramp latency (ms)
Australia - Melbourne	3.9	India - Delhi	11.3	Spain - Madrid	2.9
Australia - Perth	1.7	India - Mumbai	12.0	Sweden - Stockholm	1.0
Australia - Sydney	5.0	Israel - Tel Aviv	4.0	Switzerland - Zürich	5.5
Austria - Vienna	1.0	Italy - Milan	1.3	Taiwan - Taipei	6.8
Belgium - Brussels	7.8	Japan - Tokyo	1.8	Thailand - Bangkok	19.4
Brazil - Brasilia	1.0	Mexico - Querétaro	1.0	UAE - Dubai	3.0
Brazil - São Paulo	4.0	Netherlands - Amsterdam	1.0	UK - London	3.6
Canada - Toronto	1.0	New Zealand - Auckland	1.0	UK - Manchester	1.0
Chile - Santiago	5.7	Nigeria - Lagos	1.0	US - Ashburn, VA	2.0
Colombia - Bogota	22.0	Peru - Lima	1.0	US - Atlanta, GA	2.3
France - Paris	3.1	Philippines - Manila	11.0	US - Dallas, TX	11.1
Germany - Frankfurt	1.6	Poland - Warsaw	3.0	US - Los Angeles, CA	2.3
Germany - Munich	1.0	Singapore	19.8	US - New York, NY	5.0
Hong Kong	1.2	South Africa - Johannesburg	1.6	US - San Francisco, CA	9.0
India - Chennai	15.6	South Korea - Seoul	1.3	US - Seattle, WA	1.2

Figure 5 –NewEdge Average RTTs

In addition to peering directly with Microsoft and Google in every location possible, NewEdge additionally has optimised connections to AWS, Box, DocuSign, Dropbox, Akamai, ServiceNow, Salesforce, among many others as mentioned earlier in the peering section of this paper. The aim is to provide single-digit millisecond latencies from NewEdge DCs to top destinations, such as Google, Microsoft and AWS, while enforcing security controls in combiner with a zero-trust approach.

	Google	AWS	Microsoft
Avg latency (ms)	**7.26**	**7.29**	**4.81**
Median latency (ms)	1.18	1.79	0.85

The chart includes Netskope results for average round-trip times (RTT) in milliseconds from all its global NewEdge DCs to these top destinations.

As well as providing its own performance data and SLA assurances (covered later), Netskope anticipates that its customers will use tools provided in order to both validate performance and potentially troubleshoot perceived problems. To provide customers visibility as well as some level of direct control over managing their customer-specific tenant optimally, Netskope offers its own integrated solution for monitoring and maintaining the user experience, as well as gaining other networking insights - Proactive Digital Experience Management (P-DEM). It provides visibility via what Netskope calls "Synthetic Monitoring Augmentation for Real Traffic (SMART)" monitoring, which combines synthetic and real user monitoring with Netskope's own platform health metrics to map out the performance of every hop in the network path from the endpoint to the destination website or application.

P-DEM has obvious appeal to networking, infrastructure and operations teams as they deploy Netskope in their environment, in many cases shifting away from physical appliances and other on-premises devices historically under their direct control (and responsibility).

7. What Happens When Something Breaks?

On a general level, it's important to understand a SASE vendors' failover, redundancy and recovery strategies.

It is a fundamental that network adaptability be factored into the design of SASE infrastructure; being able to handle unforeseen events while maintaining reliable, performant service delivery. A major cable-cut incident that occurred in Africa while creating this report is a contemporary example that illustrates NewEdge in action and therefore worth mentioning. The cable cut occurred off the Ivory Coast and caused widespread disruptions affecting several countries in the region, resulting in poor connection quality for subscribers and impacting essential services such as banking.

Using internal SaaS app monitoring data (see chart below) – including observations of traffic going to top destinations like Microsoft 365 – and utilising integrated traffic management capabilities, NewEdge initiated corrective actions for customers before the Africa cable-cut made headlines and, in most instances, before customers felt any impact. NewEdge achieved this by prioritising alternate routes to work around the cut and - for example - re-directing traffic from South Africa to Europe, bypassing the impacted region entirely.

SaaS app trend data for Cape Town DC

In addition to identifying alternate traffic paths, the majority of Netskope users were transitioned to other in-region DCs; for example, South Africa users moved from the Cape Town NewEdge DC to the unaffected alternative in Johannesburg. This autonomous rerouting of traffic and fail out of the Cape Town DC ensured most customers maintained uninterrupted access – combined with optimised performance - mitigating the disruption and maintaining uninterrupted SASE service delivery.

This real-world scenario is a great example of the benefits of taking a private cloud approach, where the infrastructure is completely under the vendor's control. Not only did NewEdge have the coverage, capacity and network connectedness required, but also used actionable insights, collected via real-time monitoring, to pro-actively address the issue, transparent to the user base. NewEdge's auto-failover capabilities meant mitigation was instantaneous, using automation to eliminate the need for human intervention. It is also a great example of how important the quality of the engineering team within a vendor is – there is no replacement for specialist knowledge and experience.

NewEdge-specific features, such as Route Control, are a fundamental part of the real-time traffic management that can still provide optimal paths and routing, even when there are major problems as outlined in the use case above. In addition, NewEdge Traffic Management (which is used to ensure users/sites are always connecting to the best NewEdge DC based on lowest latency) is key to having users/sites re-connected to the next best DC in just seconds when unforeseen events occur, thereby without impacting on the user experience.

When selecting a cloud-delivered service such as Netskope's, an important concern for customers is what contractual assurances are provided for service uptime/availability, traffic processing performance, or even security efficacy. For its inline services (e.g. CFW, SWG, inline CASB, NPA/ZTNA), NewEdge is backed by a 5x9s (or 99.999%) availability SLA. Additionally, latency SLAs commit to round-trip processing of non-decrypted or decrypted transactions in sub-10ms or sub-50ms respectively. Netskope claims the NewEdge latency SLAs are anywhere from 2-10x better than those of many rival vendors, so check these claims out. It is also worth noting that the SLA calculation employed by Netskope is calculated based on monthly '95th percentile' (not 'averages' as it claims many competitors use as their primary metric), meaning Netskope SLAs are extremely stringent. Netskope SLAs are posted on its website at:
https://www.netskope.com/support-terms

8. How Do You Pay Them?

And now we get to the crux of the matter – how is a vendors' SASE solution priced and what exactly do you get for your money?

Netskope notes that a key selling point for customers is that they have access to all NewEdge DCs, meaning a customer with a global footprint could readily utilise all NewEdge DCs simultaneously. All DCs are included as standard with the purchase of any Netskope service - the only exception being the four DCs inside Mainland China that require additional SKUs/licenses. We noted in our previously published Network Scorecard that it is not uncommon for SASE vendors to list extra fees/surcharges for access to various regions within their DC footprint – such as South America, Africa, or other parts

of Asia (in addition to China) and – in some cases – it is not clear exactly where those surcharges will be levied, or indeed what the actual cost is. Having an "all in one" approach to global pricing therefore is an obvious benefit.

In terms of Netskope service offerings, its Security Service Edge (SSE) is provided primarily on a subscription basis as a cloud-delivered service. The full breadth of inline and API-based services – spanning Cloud Firewall, SWG, inline or API-based CASB, ZTNA, Remote Browser Isolation, Threat and Data Protection, Cloud and SaaS Security Posture Management (CSPM/SSPM), and more – are available a la carte or as part of packages with various tiered offerings. For complete, single-vendor SASE components such as Borderless SD-WAN (for SD-WAN functionality combined with Netskope SSE) are available in virtual and physical appliance form factors, as well as integrated into the Netskope Client.

Depending on the individual product/service or package, pricing is primarily on a per-user, per-year basis. However, additional add-ons or options are available based on bandwidth/throughput, storage volumes, regions (e.g. Mainland China mentioned earlier) micro-features (e.g. Dedicated Egress IPs), or even specific applications. Netskope also offers complementary Professional Services, as well as Premium Support options.

IN CONCLUSION

It is clear that Netskope has invested heavily in trying to provide a fully-optimised (and secure) SSE/SASE delivery and all available statistics support that aim.

Being fully in control of its service delivery is hugely important from a customer satisfaction perspective: user experience, optimised application and service delivery, scalability, ease of management (no 3rd party finger pointing) are all clear and obvious benefits of this approach. Moreover, Netskope is showing no sign of slowing down its global expansion; Mainland China coverage is a great example of its ambition.

Overall, the Netskope NewEdge SASE Cloud fares extremely well, in terms of meeting the requirements laid out in our network scorecard, with no obvious weaknesses.