cradlepoint PART OF ERICSSON

Data Sheet

Ericsson NetCloud SASE

2025 - 04 - 30

Simple SD-WAN and zero-trust security for distributed WANs

The Challenge

The adoption of Wireless WANs allows fast moving organizations to take advantage of agile connectivity for temporary and fixed sites, vehicles, IoT devices and remote workers. However, as the WAN becomes more distributed and far more dynamic, a simplified, cellular-centric approach to SD-WAN and security is required.

The Value of NetCloud SASE

Optimized for LTE/5G Wireless WANs, NetCloud SASE provides the modern SD-WAN and security features to help organizations increase WAN resiliency and quality of experience while also protecting their corporate assets, applications, and users from the threat of an attack.
With a range of fully integrated services, NetCloud SASE enables organizations to:

- Dynamically construct zero trust networks in under 6 minutes
- Deliver a highly resilient, high-performance WAN with SD-WAN and intelligent bonding
- Provide secure remote access capabilities for both managed and unmanaged devices
- Protect users from web-borne threats with pre-built web security profiles
- Apply application aware traffic filtering while continuously inspecting traffic with hybrid mesh firewall and IDS/IPS capabilities
- Streamline operations with a truly unified SASE solution (one policy engine, one pane of glass and one provisioning experience) that offers powerful AI insights

NetCloud SASE Capabilities

Secure Connect – The zero trust network foundation, offering a simple-to-manage alternative to complex VPN infrastructures for securely connecting IoT devices, sites, vehicles, and remote workers. As the foundation for all other services, Secure Connect delivers a policy-governed, zero-trust network that can be easily orchestrated to enable highly secure communications from the WAN edge to the cloud.

Zero Trust Network Access (ZTNA) – Secure remote access for employees and contractors, providing a security service that integrates with an organization's existing identity provider to provide isolated user-to-resource access for authenticated users. It enables secure remote access for internal employees and third parties to resources (IoT devices and/or applications) on the wireless WAN through granular user-based access policies.

SD-WAN – A simpler, more secure SD-WAN, optimized for cellular networks. It allows organizations to provide an outstanding digital experience in environments where applications reside anywhere and require secure access from anywhere. Application-based traffic steering, intelligent bonding, and forward error correction ensure that an elevated level of resiliency and quality of experience is achieved for every user and every location.

Hybrid Mesh Firewall – Enabled with a premium license, hybrid mesh firewall provides application governance, web content filtering to align to acceptable use policies and offers continuous inspection of traffic to detect and prevent malicious activity.

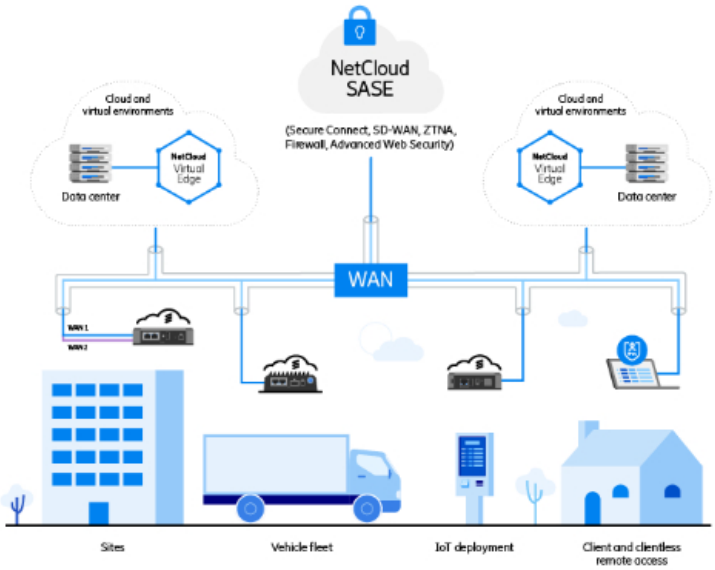
Advanced Web Security (Cloud-delivered version only) – Protects users from malicious web activity with simple pre-set web security profiles. It goes beyond allowing and denying websites, to air-gapping high-risk websites with remote browser isolation to prevent malware/ransomware spread to a user's device. Downloads from websites are also sanitized providing an extra layer of protection.

NetCloud SASE Components

NetCloud SASE comes in three flexible deployment models: cloud-delivered, customer-hosted and hybrid.

The following components are available across all three deployment models:

- **For connecting and securing sites, vehicles or IoT devices** – Ericsson WAN edge routers/ appliances provide reliable connectivity for IoT devices, vehicles and fixed/ temporary sites.
- **For connecting and securing users** – Ericsson NetCloud Client (available for Apple, Microsoft, and Linux devices) enables secure remote access to specific resources and assets on the WAN.
- **For connecting private applications** – Ericsson NetCloud Virtual Edge is a software-based solution that can be easily deployed in an AWS or Azure private cloud or an on-premises data center to allow controlled access to customer-hosted applications.
- **For management and orchestration of the end-to-end solution** –Ericsson's NetCloud simplifies the deployment, management, and ongoing troubleshooting of the network consolidating 5G, advanced networking and security into a single pane of glass.
- **For customer-hosted deployments only** – Ericsson's NetCloud Exchange Service Gateway is a scalable and reliable services delivery platform (or headend) that can reside standalone or in an active/standby configuration in a customer's data center or hosted cloud.



Why NetCloud SASE is Different

Designed for cellular-centric use cases that include roaming and mobility, with key Wireless WAN optimizations that preserve bandwidth, enhance performance, and deliver a slicing-ready solution as 5G networks evolve to 5G standalone.

Truly unified for unparalleled simplicity. Although many SASE solutions provide unified management, underneath there are still multiple disjointed products, multiple policy engines, and an inconsistent provisioning experience across the assorted services. NetCloud SASE is unified from a management, control, and data plane perspective, offering one true policy engine and one consistent provisioning experience across all networking and security services.

Zero trust built in rather than bolted on. Combines security with the network creation process to construct a zero-trust foundation that is deny-all by default. This provides the secure foundation to build additional policies from. The NetCloud SASE solution obscures all public IP addresses (even for applications and assets that connect to the zero-trust network), ensures assets and applications connecting to the network remain "dark" until explicitly defined, and restricts all access unless explicitly defined by policy.

Robust security for unmanaged devices. While most SASE solutions provide security for managed devices, unmanaged devices can still put organizations at risk. NetCloud SASE provides clientless secure access for third-party devices and leverages isolation technology to completely airgap corporate web applications from risky third-party devices – mitigating the risk of malware infection.

Common Use Cases

IoT Deployments

Secure Connect for zero-trust connectivity between IoT devices and their hosts, replacing complex VPN/Private APN architectures.

Zero Trust Network Access (ZTNA) for granting internal and third parties secure remote access to IoT devices on the WAN for maintenance and monitoring.

Add Hybrid Mesh Firewall for continuous inspection of traffic to detect and prevent malicious activity.

Vehicle Deployments

Secure Connect for securing vehicle-based communications across the WAN, replacing complex VPNs and/ or costly private APNs.

SD-WAN and intelligent bonding for providing increased resiliency, performance, and quality of experience across multiple WAN connections (cellular, satellite, and Wi-Fi as WAN).

ZTNA for secure remote access to corporate applications in the cloud or data center, or IoT devices on the WAN.

Hybrid mesh firewall for web filtering, application governance and continuous inspection of traffic.

Branch Deployments

Secure Connect for zero-trust connectivity between branches and corporate data centers and clouds, replacing complex VPN architectures.

SD-WAN and intelligent bonding for providing increased resiliency, performance, and quality of experience across multiple WAN connections (wired, cellular and satellite).

ZTNA for secure remote access to corporate applications in the cloud or data center, or IoT devices on the WAN.

Hybrid mesh firewall for web filtering, application governance and continuous inspection of traffic.

Advanced web security that provides inspection, applies controls and even isolates web sites to protect users from malicious web activity.

NetCloud Management and Operations

NetCloud SASE is fully deployed and managed through Ericsson's powerful cloud management and orchestration platform, NetCloud. With features that include zero-touch deployment, multi-layered dashboards and intuitive troubleshooting tools, NetCloud Manager is a valuable assist to lean IT organizations. Some of the key features include:

- **Virtual Expert capabilities** – Ericsson's GenAI-based NetCloud Assistant (ANA) uses Natural Language Processing to assist administrators with everyday queries about the network.

- **AI-driven insights** – An integrated AIOps dashboard simplifies the ongoing operations of the SASE network by quickly identifying performance-driven anomalies, determining the root cause, pinpointing all affected sites, users, and applications and recommending remediation steps.
- **Centralized flow level visibility** – NetCloud's Traffic Monitor dashboard is a powerful tool that lets administrators drill into every flow for detailed traffic analysis and forensics.

NetCloud SASE Services and Specifications

Secure Connect

Zero trust VPN replacement

Secure Connect offers a simple-to-manage alternative to complex VPN infrastructures for securely connecting IoT devices, sites, vehicles, and remote workers. As the foundation for all other services, Secure Connect delivers a policy-governed, zero-trust network that can be easily orchestrated to enable highly secure communications from the WAN edge to the cloud.

- **Domain name-based routing** – Translates complex IP addresses to more intuitive names to hide the network attack surface, simplifies provisioning, and creates more intuitive policies.
- **Support for overlapping IP addresses at sites** – With domain-based routing in place, overlapping IP addresses can easily be accommodated.
- **Resource-definition** – Applications and assets connecting to the network are "dark" until explicitly defined and an access policy is created.
- **Deny-all by default** – Rather than broad network access, zero trust starts with a secure foundation where access is restricted until explicitly defined by policy.
- **Blocks east/west traffic by default** – Contains breaches to where they occurred by blocking east/west and all incoming traffic to a site, unless enabled by policy.
- **Split routing from sites** – Enables Direct Internet Access from the edge router. Administrators define all the IP subnets that need to go through the SASE service; all other traffic goes direct to the internet.

PERFORMANCE			
Site Routers	**Typical Client Count**	**Throughput**	**Concurrent Tunnels**
IBR650B, IBR600C/IBR650C, IBR900, S400/S450, S700/S750, S700-FIPS/S750-FIPS	5	10 Mbps	10

NOTE: Secure Connect site performance may vary based on latency conditions.

PERFORMANCE			
Site Routers	**Typical Client Count**	**Throughput**	**Concurrent Tunnels**
IBR1700, IBR1700-FIPS	30	40 Mbps	20
R920, R920-FIPS	5	30 Mbps	10
R980	5	85 Mbps	20
R1900, R1900-FIPS, R2105/R2155, R2105-FIPS/R2155-FIPS	100	400 Mbps	20

NOTE: Secure Connect site performance may vary based on latency conditions.

PERFORMANCE			
Site Routers	**Typical Client Count**	**Throughput**	**Concurrent Tunnels**
AER2200	100	40 Mbps	20
E100, E102	5	40 Mbps	20
E300, E300-FIPS	50	400 Mbps	20
E400	50	270 Mbps	20
E3000, E3000-FIPS	100	400 Mbps	20

NOTE: Secure Connect site performance may vary based on latency conditions.
Secure Connect is not yet supported on the X10 and X20 routers.

SD-WAN

SD-WAN is a cellular-optimized network service based on a zero-trust foundation that enhances WAN resilience and quality of experience (QoE) by optimizing traffic over multiple physical or logical connections including, wired, 5G/LTE, satellite, Wi-Fi as WAN, private APNs, and 5G standalone network slices.

- **Zero trust foundation for SD-WAN** – While traditional SD-WAN technology leverages encryption and site-based VPN technology to secure traffic over multiple WAN connections, NetCloud SASE and NetCloud Exchange leverages a true zero trust foundation that minimizes the attack surface, limits the blast radius, and is deny-all by default.
- **Classification of traffic into predefined classes** – Through deep packet inspection, administrators can classify their traffic into business critical, real-time, interactive, or best effort.
- **Application-based traffic steering** – After traffic is classified, policies can be created to ensure business critical and real-time applications are prioritized across the WAN and are always traversing the highest performing WAN connection.
- **Traffic steering based on real-time WAN performance** – Using in-line traffic, NetCloud SASE and NetCloud Exchange measures latency, loss, and available bandwidth across all available WAN connections. If performance degrades beyond the predefined thresholds, traffic is dynamically steered to a better performing connection.
- **Direct Internet Access** – To enhance performance and reduce the costs of backhauling, NetCloud SASE enables direct internet access capabilities from sites and vehicles.
- **Traffic steering across 5G network slices** – Select modems can support up to eight 5G SA network slices. Leveraging NetCloud SASE or NetCloud Exchange, when a 5G SA network is in place, the ability to steer applications into the most suitable network slide is available. (For example, business-critical traffic can be steered into an ultra-reliable low latency slice.)
- **Intelligent Link Bonding** – Allows the creation of a bonded interface using multiple WAN interfaces.
  - **Flow duplication across bonded WAN connections** – Provides a highly resilient connection for mission-critical applications by duplicating traffic flows across two diverse connections, minimizing packet loss, and increasing availability.
  - **Weighted flow balancing across bonded WAN connections** – Distributes application traffic flows across diverse WAN links according to user-defined weights for improved efficiency and cost savings.
  - **Bandwidth aggregation across bonded WAN connections** – Aggregates two or more WAN links into one logical link providing more bandwidth for applications like video and large file transfers.
- **Forward Error Correction** – Most effective for chatty TCP-based applications, FEC mitigates against lossy connections by adding parity bits to an application flow to prevent application retries, thereby improving application quality of experience.
- **Networkwide application-based policies** – With NetCloud SASE and NetCloud Exchange, just a single SD-WAN policy can be applied across the entire network, including across heterogenous product types.

PERFORMANCE		
Site Routers	**Typical Client Count**	**Throughput**
IBR1700	30	40 Mbps
R920	5	30 Mbps
R980	5	85 Mbps
R1900, R2105/R2155	100	400 Mbps

The IBR1700 and R920 routers do not yet support the Forward Error Correction (FEC), Intelligent Bonding, or Fast Link Monitoring features. R2105 routers do not yet support the Intelligent Bonding feature. R2155 routers do not yet support FEC or Intelligent Bonding features. Other SD-WAN functionality is supported.

PERFORMANCE		
Site Routers	**Typical Client Count**	**Throughput**
AER2200	100	40 Mbps
E100, E102	5	40 Mbps
E300	50	400 Mbps
E400	50	270 Mbps
E3000	100	400 Mbps

The AER200 and E102 routers do not yet support the Forward Error Correction (FEC), Intelligent Bonding, or Fast Link Monitoring features. Other SD-WAN functionality is supported. All features are supported when using E100, E300, E400, and E3000 routers.
SD-WAN is not yet supported on the X10 and X20 routers.

Zero Trust Network Access

Secure remote access

Zero Trust Network Access (ZTNA) is a security service that integrates with an organization's existing identity provider to provide isolated user-to-resource access for authenticated users. It enables secure remote access for internal employees and third parties to resources (IoT devices and/or applications) on the Ericsson WAN through granular user-based access policies.

- **Identity verification** – Offers integration to any SAML 2.0 compliant Identity Management Platform, preventing identity sprawl.
- **Isolated user-to-resource access** – Users are directly authenticated to their authorized resources per session.
- **Least privilege access** – Various levels of access, ranging from visibility only to full configuration, can be granted based on the user's job function or identity.
- **Continuous monitoring for changes in context** – Changes in context are monitored, resulting in changes in access privileges if warranted.
- **Device posture visibility** – Administrators can view details on the device posture (for example, anti-virus installed and running, OS version, and device type) for any device that has the client installed.
- **Flexible user authentication** – In addition to being able to authenticate users through an Ericsson Cradlepoint router, a wide range of Windows, Mac, and Linux clients are supported to enable safe remote connectivity from anywhere.
- **NetCloud Client –** This software enables secure remote access to an NetCloud Secure Connect network. The NetCloud Client supports Windows and macOS laptops, iOS mobile devices, and Linux devices. The NetCloud Client is available to download with a ZTNA license.
- **Clientless ZTNA** (cloud-delivered only) **–** Allows contractors and third parties to security access specific resources without requiring a client. This leverages isolation technology and protects company applications from unmanaged devices.

SYSTEM REQUIREMENTS	
Operating System:	Windows

Version:	Windows 10 and 11
Processor:	Intel x86
Memory:	16 GB
Maximum NetCloud Client Count:	Unlimited (limited by NCX Service Gateway licensed throughput capacity per network)

SYSTEM REQUIREMENTS	
Operating System:	macOS
Version:	Monterey 12.x or later
Processor:	Intel or Apple M1/M2 CPU
Memory:	16 GB
Maximum NetCloud Client Count:	Unlimited (limited by NCX Service Gateway licensed throughput capacity per network)

SYSTEM REQUIREMENTS	
Operating System:	iOS
Version:	iOS 16 or later
Processor:	ARM64 or Apple Silicon
Memory:	64 GB
Maximum NetCloud Client Count:	Unlimited (limited by NCX Service Gateway licensed throughput capacity per network)

SYSTEM REQUIREMENTS	
Operating System:	Linux Ubuntu
Version:	22.04
Processor:	— Intel x86 — Minimum four core CPU
Memory:	16 GB
Maximum NetCloud Client Count:	Unlimited (limited by NCX Service Gateway licensed throughput capacity per network)

Hybrid Mesh Firewall

(Requires a Premium license)

Hybrid Mesh Firewall (HMF) is a security service that can be added to a Secure Connect, SD-WAN or ZTNA network. With application and web filtering plus integrated IDS/IPS, HMF brings in modern firewall features, without the complexity.

- **Application visibility and enforcement** – Uses policies and deep packet inspection to determine whether to block or allow traffic, including communications to or from an application.
- **IDS/IPS** – Provides continuous monitoring of all north/south and east/west traffic flows to detect and prevent malicious activity.
- **Web filtering** – Blocks access to inappropriate web content including high-risk domains that may contain malware.
- **Firewall-as-a-Service** – Simplifies firewall deployment by using cloud firewall capabilities instead of requiring local firewalls in all locations.

PERFORMANCE

Site Routers	Typical Client Count	Throughput	Concurrent Tunnels
IBR600C/IBR650C, S700/S750	5	10 Mbps	10

NOTE: Hybrid Mesh Firewall site performance may vary based on latency conditions.

PERFORMANCE			
Site Routers	**Typical Client Count**	**Throughput**	**Concurrent Tunnels**
IBR1700	30	40 Mbps	20
R920	5	10 Mbps	10
R1900, R2105/R2155	100	400 Mbps	20

NOTE: Hybrid Mesh Firewall site performance may vary based on latency conditions.

PERFORMANCE			
Site Routers	**Typical Client Count**	**Throughput**	**Concurrent Tunnels**
AER2200	100	40 Mbps	20
E100, E102	5	40 Mbps	20
E300	50	400 Mbps	20
E3000	100	400 Mbps	20

NOTE: Hybrid Mesh Firewall site performance may vary based on latency conditions.

AI-Driven Insights

(Requires a Premium license)

- **AI-driven insights** – An integrated AIOps dashboard detects performance driven anomalies and flags them to the administrator pinpointing the root cause and recommended remediation.
- **Virtual Expert capabilities** – While Ericsson's GenAI-based NetCloud Assistant (ANA) is to be available across all NetCloud Manager dashboards, more specialized functionality is only available with a NetCloud SASE Premium license.

Advanced Web Security

(Cloud deployment option only)

- **Secure Web Gateway** – Ensures web requests align organizational policies. If the request raises any red flags or is linked to a malicious website, the gateway returns a warning or blocks user access.
- **Anti-virus** – Scans incoming web traffic for known virus signatures, allowing the SWG to detect and block malicious content before it reaches a user's device.
- **Cloud Access Security Broker** – Acts as an intermediary between end users and the cloud, to control access to cloud-based applications.
- **Remote Browser Isolation** – Separates users' devices from the act of Internet browsing by hosting and running all browsing activity in a remote, isolated cloud-based container. Only a safe rendering is delivered to the end user.
- **Content Disarm and Reconstruct** – Protects against known and unknown threats contained in documents by removing executable content before the file is downloaded to the user's device.

NetCloud SASE Appliances and Specifications

NetCloud Virtual Edge

NetCloud Virtual Edge is a cost-effective and simple solution for organizations that need to connect to one or more data center or private cloud environments as part of their zero-trust network.

PERFORMANCE			
Tunnel Throughput to/from NetCloud Exchange:	300 Mbps		
Deployment Targets:	AWS	Azure	VMware
Instance:	m5.large	Standard_D2s_v5	VMware ESXi 6.7 U3 hypervisor or newer
vCPUs:	2	2	2
Memory:	8 GB	8 GB	8 GB
Minimum Disk Space:	2 MB	2 MB	2 MB
vNICs:	2	2	2

NetCloud Exchange Service Gateway

(customer-hosted deployment model only)

NetCloud Service Gateway is a services delivery platform (or headend) that can reside standalone or in an active/standby configuration in a customer's data center or hosted cloud. The Service Gateway aggregates traffic from IoT, vehicle, site, and remote work environments, enforces policy, and provides visibility into every flow.

PERFORMANCE		
Licensed Capacities:	— 250 Mbps — 500 Mbps — 1 Gbps — 2 Gbps — 4 Gbps†	
SYSTEM REQUIREMENTS (ALL CAPACITIES)		
Deployment:	AWS	Azure
Software Version:	— Up to 7.24.60: Ubuntu 18.04 — For 7.24.80 and later: Ubuntu 20.04	— Up to 7.24.60: Ubuntu 18.04 — For 7.24.80 and later: Ubuntu 20.04
Instance:	c5.2xlarge	Standard_D8S_v3
vCPUs:	8	8
Memory:	16 GB	32 GB

Minimum Disk Space:	16 GB	16 GB
vNICs:	3	3
Minimum NetCloud Exchange Service Gateway Release:	7.22.70	7.22.70
Concurrent Tunnels:	Up to 4,000	Up to 4,000

Performance testing was conducted based on requirements as defined in RFC2544 using fixed-frame 1518-byte packets. Throughput results reflect unidirectional. UDP traffic with less than 1% packet loss as tested with wired connections. At the time of release, the number of supported sites and tunnels is a 1:1 ratio. Ericsson Cradlepoint routers support multiple WAN interfaces simultaneously in SD-WAN mode.

PERFORMANCE		
Licensed Capacities:	— 250 Mbps — 500 Mbps — 1 Gbps — 2 Gbps — 4 Gbps†	
SYSTEM REQUIREMENTS (ALL CAPACITIES)		
Deployment:	KVM	VMware
Software Version:	Ubuntu 18.04	ESXi 6.7 or newer
Instance:	N/A	N/A
vCPUs:	8	8
Memory:	16 GB	16 GB
Minimum Disk Space:	16 GB	16 GB
vNICs:	3	3
Minimum NetCloud Exchange Service Gateway Release:	7.22.70	7.22.70
Concurrent Tunnels:	Up to 4,000	Up to 4,000

Performance testing was conducted based on requirements as defined in RFC2544 using fixed-frame 1518-byte packets. Throughput results reflect unidirectional. UDP traffic with less than 1% packet loss as tested with wired connections. At the time of release, the number of supported sites and tunnels is a 1:1 ratio. Each Ericsson Cradlepoint router only supports one tunnel on one active WAN interface at a time.

Ordering Guide

The NetCloud Service Gateway is a required component to implementing NetCloud Exchange services (Secure Connect, SD-WAN and ZTNA). These services can be purchased as an add-on to any compatible router with a NetCloud Branch, Mobile or IoT service plan, while the NetCloud Service Gateway is purchased based on required network capacity.
For ordering details, see the following:

- **Step 1 (required):** Select the **deployment model** NetCloud SASE cloud-hosted or NetCloud Exchange customer-hosted.
- **Step 2 (required):** Select the **NetCloud Service plan(s)** for the compatible router(s).
- **Step 3 (required NetCloud Exchange only):** Select the NetCloud Service Gateway **capacity** for entire solution (separate part number for high availability).
- **Step 4 (required):** Select the Secure Connect or SD-WAN **site (router-based) license(s)** in either Standard or Premium for each router. **NOTE**: Each NetCloud SASE license includes 500 GB for a shared data pool.
- **Step 5 (optional):** Select ZTNA in either Standard or Premium per user license(s) (selection of Standard or Premium must match Step 4).

- **Step 6 (optional):** Select the NetCloud Virtual Edge in either Standard or Premium per each additional data center or private cloud environment beyond where the NetCloud Service Gateway is located (selection of Standard or Premium must match Step 4). **NOTE**: Each NetCloud SASE license includes 500 GB for a shared data pool.
- **Step 7 (optional NetCloud SASE only):** Select additional 500 GB data credits to add to the shared data pool.

REGION	NetCloud PACKAGE	DESCRIPTION	PART NUMBER
All Regions:	NetCloud SASE Secure Connect	Standard	NCS-0K0x-SCDC
		Premium	NCS-0KPx-SCDC
		Premium Add-On	NCS-0NPx-HMFAI
	NetCloud Exchange Secure Connect	Standard	NCX-0K0x-SC
		Premium	NCX-0KPx-SC
		Premium Add-On	NCX-0NPx-HMFAI
	NetCloud SASE SD-WAN	Standard	NCS-0L0x-SCDCSD
		Premium	NCS-0LPx-SCDCSD
		Premium Add-On	NCS-0B0x-SDWAN
	NetCloud Exchange SD-WAN	Standard	NCX-0L0x-SCSD
		Premium	NCX-0LPx-SCSD
		Premium Add-On	NCX-0B0x-SDWAN
	NetCloud SASE ZTNA	Standard (Per User)	NCS-0E0x-ZTNA
		Premium (Per User)	NCS-0EPx-ZTNA
	NetCloud Exchange ZTNA	Standard (Per User)	NCX-0E0x-ZTNA
	NetCloud SASE Virtual Edge	NetCloud Standard for Virtual Edge with Secure Connect	NCS-0M0x-VESCDC
		NetCloud Premium for Virtual Edge with Secure Connect	NCS-0MPx-VESCDC
	NetCloud Exchange Virtual Edge	NetCloud Standard for Virtual Edge with Secure Connect	NCX-0M0x-VESC
		NetCloud Premium for Virtual Edge with Secure Connect	NCX-0MPx-VESC
	NetCloud SASE Data Credit	500 GB	NCS-0D0x-DC
	Service Gateway	250 Mbps	NCX-000x-SG250MBPS
		500 Mbps	NCX-000x-SG500MBPS
		1 Gbps	NCX-000x-SG1GBPS
		2 Gbps	NCX-000x-SG2GBPS
		4 Gbps	NCX-000x-SG4GBPS
	Service Gateway High Availability	Active + Standby 250 Mbps	NCX-002x-SGAS250MBPS
		Active + Standby 500 Mbps	NCX-002x-SGAS500MBPS
		Active + Standby 1 Gbps	NCX-002x-SGAS1GBPS
		Active + Standby 2 Gbps	NCX-002x-SGAS2GBPS
		Active + Standby 4 Gbps	NCX-002x-SGAS4GBPS
All Regions — Renewal:	NetCloud SASE Secure Connect	Renewal — Standard	NCS-0K0x-SCDC-R
		Renewal — Premium	NCS-0KPx-SCDC-R
		Renewal — Premium Add-On	NCS-0NPx-HMFAI-R

	NetCloud Exchange Secure Connect	Renewal — Standard Renewal — Premium Renewal — Premium Add-On	NCX-0K0x-SC-R NCX-0KPx-SC-R NCX-0NPx-HMFAI-R
	NetCloud SASE SD-WAN	Renewal — Standard Renewal — Premium Renewal — Premium Add-On	NCS-0L0x-SCDCSD-R NCS-0LPx-SCDCSD-R NCS-0B0x-SDWAN-R
	NetCloud Exchange SD-WAN	Renewal — Standard Renewal — Premium Renewal — Premium Add-On	NCX-0L0x-SCSD-R NCX-0LPx-SCSD-R NCS-0B0x-SDWAN-R
	NetCloud SASE ZTNA	Renewal — Standard (Per User) Renewal — Premium (Per User)	NCS-0E0x-ZTNA-R NCS-0EPx-ZTNA-R
	NetCloud Exchange ZTNA	Renewal — Standard (Per User)	NCX-0E0x-ZTNA-R
	NetCloud SASE Virtual Edge	Renewal NetCloud Standard for Virtual Edge — Per Self-Hosted Virtual Appliance Renewal NetCloud Premium for Virtual Edge — Per Self-Hosted Virtual Appliance	NCS-0M0x-VESCDC-R NCS-0MPx-VESCDC-R
	NetCloud Exchange Virtual Edge	Renewal NetCloud Standard for Virtual Edge — Per Self-Hosted Virtual Appliance Renewal NetCloud Premium for Virtual Edge — Per Self-Hosted Virtual Appliance	NCX-000x-VESC-R NCX-0MPx-VESC-R
	NetCloud SASE Data Credit	Renewal — 500 GB	NCS-0D0x-DC-R
	Service Gateway	Renewal — 250 Mbps Renewal — 500 Mbps Renewal Active + Standby — 250 Mbps Renewal Active + Standby — 500 Mbps	NCX-000x-SG250MBPS-R NCX-000x-SG500MBPS-R NCX-002x-SGAS250MBPS-R NCX-002x-SGAS500MBPS-R

x= 1, 3, or 5 years