Managed Cisco SASE Secure Access Technology Service Description

Overview

This document provides information relating to the management and monitoring of Managed SASE-Cisco Secure Access under the MCN offering. The monitoring, configuration, limitations, and available standard service requests are outlined hereunder. The scope of the Managed SASE Cisco Secure Access is as follows:

- Secure Internet and SaaS Application Access
  - Cisco Secure internet Access (SIA) protects enterprise users that access applications over the internet.
- Secure Private Access
  - Cisco Secure Private Access (SPA) protects enterprise users that access an enterprise's internal applications.

Client Responsibilities and Pre-requisites

In addition to the pre-requisites documented in the MCN Statement of Work, the following technology specific pre-requisites are applicable.

- A standards-compliant IPSEC/GRE-capable device must be provisioned by the client at each branch and corporate network intended for connectivity to the SASE/SSE Cloud.

Technology Specific Operations

Monitors

The following technology specific monitors can be configured by default.

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
IPSec tunnel & Network tunnel group state	Discover and monitor the Network active/passive tunnel status	✓	Monitoring of IPSec tunnel and tunnel group state.	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware maintenance provider as required	180
IPSec Tunnel Utilization	Monitor the bandwidth utilization of network tunnel	✓	Online reports for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware maintenance provider as required	180
IPSec / Network tunnel error state	Monitor the in/out data packet errors of network tunnel	✓	Monitoring of IPSec tunnel errors.	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware maintenance provider as required	180
Resource connector state	Monitor Resource connector group connectivity state to cloud	✓	Monitoring of resource connector group connectivity status	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware maintenance provider as required	180
Resource connector agent state	Monitor Resource connector agent status	✓	Monitoring of resource connector	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware	180

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
			connectivity status	maintenance provider as required	
Resource connector performance	Monitor the resource connector CPU utilization	✓	Monitoring of resource connector performance	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware maintenance provider as required	180
Roaming Client	Monitor the roaming client count by VPN profiles	✗	Online reports for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware maintenance provider as required	180
VPN Connection state	Monitor the VPN client OS and agent versions.	✗	Online reports for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware maintenance provider as required	180
Reports discovery	Gather Top threats and top talker reports	✗	Online reports for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware maintenance provider as required	N/A

Configuration Management

Cisco Secure Access is a full SaaS offering; therefore, device configuration backups are inherent to the solution and are executed automatically with the built-in toolsets of the Cisco Secure Access Cloud. All the Secure Access configuration backups are stored in the Cisco Cloud itself as part of Management Orchestration.

Firmware Maintenance

Firmware maintenance for the Cisco Secure Access solution is an automated process and is included within the Cisco SASE solution. Firmware schedules and frequencies are determined and managed by the vendor. For further details in this regard refer to the vendor's relevant documentation.

Supported configurations.

Cisco Secure Access cloud POP's and connectors are managed via a centralized cloud management portal. The centralized cloud control portal manages the configurations of traffic steering types, access policies for internet and private access, security content filtering for internet and private applications and SaaS applications.

The following Cisco Secure Access features are supported:

- Network and network tunnel group of IPSec tunnels.
- Active/Passive tunnels
- ECMP for multiple tunnels with static / BGP routing
- Overlapping subnets/outbound NAT for the network tunnels
- Secure private access resource connector deployed on-premises Data Center or public cloud infrastructure.
- Cisco Secure client VPN portal configuration
- IP Pool configuration
- Management of secure client SSE agent configuration.

- Machine tunnel, standard VPN client profiles, and endpoint client posture profiles.
- PAC file enablement and upload the new PAC file.
- User and group provisioning by
  - Security Assertion Markup Language (SAML 2.0)
  - SCIM
  - Secure Lightweight Directory Access Protocol (LDAP) including Active Directory of authentication, authorization, and accounting (as applicable per design).
- Internet and private access security policies
- Advance threat protection
- Malware protection content filtering policies
- IPS policies
- Security profiles
- URL filtering policies
- Data Loss Prevention policy can monitor or block the data being uploaded to the web. As well, it can discover and protect the sensitive data stored and shared in your cloud sanctioned applications.
- Public Service Edges are supported.
- Cisco Secure internet Access and Private application access integration with client on-premises Data Center, Colocation Data Center, Public Cloud infrastructure are supported.

Limitations

The following limitations apply:

- Deployment of end-user agents are the client's responsibility, and NTT will only provide notifications or recommendations of agent updates.
- This service does not include procurement of internet or WAN circuits, or software or hardware / virtual devices. These services are available from NTT under a separate Statement of Work.
- Network architecture design and re-design are out of scope.
- Policy management and device registration is limited to client provided instructions.
- End user support is excluded. NTT will assist the Client's support team with troubleshooting end-user faults that are suspected to be attributed to the network.
- Security Incident Management (SIEM) and any related integration are out of scope. These services are available from NTT under a separate Statement of Work.
- Threat Intelligence, Forensic analysis, External Dynamic list, and IOC blocking is out of scope.
- Virtual Service edges are not supported.
- The tasks, features and services listed in this document are excluded from any underlying infrastructure.
- The Client must acknowledge that SASE/SSE is a Cloud delivered, Shared Service model. The vendor may periodically alter the administration and operating model; therefore, mutual agreement must be reached between NTT, Cisco, and the Client, and an appropriate decision must be made accordingly.

Standard Service Requests

A list of standard service requests available for this technology can be found in the MCN Request Catalogue.

Technology Transition Tasks

No technology specific transition tasks are required. A description of the standard transition tasks included for the service offering is documented in the MCN Statement of Work

Note:

Any tasks not explicitly described under the Technology Transition tasks are implicitly excluded from transition.