MCN - Managed Software Defined WAN (SD-WAN) Service Description

Overview of Service

All SD-WAN devices which are managed as part of the Service will be supported in accordance with the NTT processes described in the *Managed Campus Networking Statement of Work.*

Technology specific tasks associated with the SD-WAN technology stack are described in this section. The scope of the Managed SD-WAN service is as follows:

- SD-WAN supported router (refer to the MCN Supported Technology List documentation)
- Other devices released by the vendor that operate on the same software.
- Control Plane (SD-WAN Controllers such as vManage and Unity Orchestrator) hosted either in the cloud, or on premise.

Further detail on these service offers can be found in the specific sub-sections below.

Client Responsibilities and Prerequisites

- The Client must be in possession of an active hardware service contract for the network device(s) under management with the vendor, or a vendor approved third party such as NTT Uptime Support Services.
- The Client must grant authority to NTT's engineers to contact the device vendor (or third party) directly for the purposes of the managed service.
- Administrative access to the SD-WAN cloud based control plane, or the on-premise instance of the SD-WAN Control Plane is required to manage the described devices.
- Any management of licenses, if required.
- Any software or firmware operating on the device must be a version currently supported by the vendor.
- Simple Network Management Protocol (SNMP) or Application Programming Interface (API) key, as required, must be enabled and configured for devices to be managed as part of the service.

Service Specific Operations

SD-WAN Monitors

Monitoring will be performed in accordance with the process described in Event Management (see *Managed Campus Network SoW*).

The following monitors are configured by default for all Managed SD-WAN control plane elements and endpoint devices;

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Ping / Network	Time taken for responding to a ping from a poller, and packet loss	✓	Graphs for ping response time Graphs for packet loss percentage	Engineering teams will resolve the issue	60
Device Availability	Up / down status of all elements of the control plane (i.e. vSmart, vBond, vManage, Unity Orchestrator etc.)	✓	Information whether the device is operational and reachable	Engineering teams will resolve the issue	180
CPU	CPU usage of the host on which the control plane elements reside	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client if needed.	180
Memory	Memory usage of the host on which the control plane elements reside	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client if needed.	240
Interface status	Interface operational state	✓	Established whether an interface is operationally up or down	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client if needed.	60
HTTP port status	Monitors http page (port TCP80) load time and response status. (Aruba Silver Peak)	✗	Establish if TCP port 80 is responsive to requests.	Engineering teams will resolve the issue	60
HTTPS port status	Monitors https page (port TCP443) load time and	✗	Establish if TCP port 443 is responsive to requests.	Engineering teams will resolve the issue	60

© 2023 NTT DATA, Inc. | NTT Ltd. and its affiliates are NTT DATA, Inc. companies.

	response status. (Aruba Silver Peak)				
Disks	Monitors Silver Peak appliance disk health. (Aruba Silver Peak)	✓	Monitors the appliance disks at the device level	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client if needed.	420
Disk Usage	Monitors Silver Peak appliance disk usage. (Aruba Silver Peak)	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client if needed.	420
Tunnels	Monitors the appliance WAN tunnels at the device level. (Aruba Silver Peak).	✓	Monitors WAN tunnels at the Orchestrator for operational status	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client if needed.	420
SSL Certificates	Monitors SSL validity information across all common SSL ports. (Aruba Silver Peak)	✓	Monitors validity of SSL information.	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client if needed.	1800

Limitations:

With respect to Aruba Silver Peak SD-WAN, Single Sign-On (SSO) to Aruba Central from Orchestrator is not supported.

Service Requests

Note
Please note that NTT applies a fair use policy in the execution of these requests.
For more information related to the Fair Use Policy please refer to the *MCN Statement of Work*.

As part of the Service, the fulfilment of the tasks listed in the table below are included.

SD-WAN Service Requests

Task	Description	Included
Creation of users / groups	Creation of users and groups in the Control Plane element, including password maintenance, for Client read-only accounts.	✓
Management of network interfaces (ports)	Creation and changes in the network interface parameters (IP addresses, gateways).	✓
Log subsystem configuration	Management of log information, resending to a syslog server (if any), including to Client syslog servers when requested by the Client.	✓
Configuration Management: data restoration	Restore device configuration from backup, either as an automatic process from the SD-WAN Control Plane or as a mix of automatic and manual processes from configuration backups stored external to the SD-WAN Control Plane.	✓

Configuration Management - Backup and Restore

An integral part of the Service is the management of the backup policy and execution of restore requests. The following tasks are included as part of SD-WAN Control Plane and Device management service:

Task	Description
Restore of System Configuration	Restore of system configuration from the backup policy
Configuration Backup Policy implementation	When the service is initially delivered, a Configuration backup policy will be implemented.

Cloud hosted SD-WAN Control Plane elements

Device templates used on SD-WAN endpoints are backed up automatically by the SD-WAN Controller element of the Control Plane.

If backup of a device configuration to a remote location is required, the remote location and access to the location and infrastructure to which the configuration must be backed up, will need to be provided by the Client and provided that the vendor makes such backup option available.

© 2023 NTT DATA, Inc. | NTT Ltd. and its affiliates are NTT DATA, Inc. companies.

Ongoing SD-WAN device management

SD-WAN physical and virtual devices are managed via a centralized control plane. The centralized control plane in a SD-WAN environment controls all endpoints, providing centralized functions like automated template provisioning and updates, de-commissioning, single screen administration and web-scale reporting.

This control plane has two deployment and licensing approaches.

- A Vendor Cloud hosted control plane, where the vendor provides an instance of the control plane as a SaaS solution
- An on-premise hosted control plane where it is the client's responsibility to host the control plane. In this scenario, the following configurations are supported;
  - A control plane running on client provided infrastructure, at a client location.

The control plane deployment is dependent on the model selected for the SD-WAN solution.

NTT will manage the SD-WAN control plane for the devices included in the solution, as explained in this section, including the following activities;

- Management of Configuration Templates
- Configuration of SD-WAN Control Plane and device monitoring such that NTT is able to monitor the availability and health of the Client's environment.

The following information is captured in alerts from the SD-WAN Control Plane elements;

- Availability of Control Plane elements
  - SD-WAN Controller (e.g. vSmart, vBond, vManage, Unity Orchestrator)
- Device hostname
- Device serial number
- Device last check time (date and time)
- IP address

Periodic Maintenance Tasks

As part of the Service, the following periodic maintenance tasks are included for Managed SD-WAN Control Plane elements and endpoint devices;

Task	Frequency	Description
Firmware review	Continuous process	Notify the Client of outstanding critical firmware upgrades which address vulnerabilities that may affect the Service, such as security exploits or bugs. In case the Client chooses to proceed with the upgrade, following the process defined for firmware patching in *the Managed Campus Networking Statement of Work*. Upgrade of firmware is not considered the same as patching, but as an installation of a new operating system version for the device.
Configuration management	Weekly	Review of the correct execution of the associated configuration backup; in case of an error with the execution of a backup configuration, resolution will follow the process for Incident Management.
Patch review	Continuous process	In addition to the patching policy defined in the Operate section of the Managed Campus Networking Statement of Work, the following specific conditions apply for SD-WAN device and control plane patching; • Must be operating a software version(s) currently supported by the vendor. • Must not have any advisories issued relating to any feature, configuration, or hardware that are specific to the device in question. • Within compliance of the vendor recommended version of software outside of these parameters and that addresses a specific issue. All software patches and upgrades of SD-WAN endpoints are conducted using the SD-WAN Controller component of the SD-WAN control plane. i.e. vManage, Unity Orchestrator etc.

Keeping up-to-date on firmware allows administrators to utilize the latest features and ensures that the latest security enhancements are running on their hardware. Admins can upgrade to the latest stable or latest beta firmware. NTT will communicate with the Client to proceed with firmware update:

- For all the networks in scope
- For a series of networks of the total scope
- For all the devices of a certain type
- For all devices in a certain version
- For an individual device

The firmware upgrade will not be executed unless:

- It was previously agreed as part of the Patching Design sessions with the Client (as an example, all the critical security patches must be applied within 24 hours of firmware release); or
- It was approved by the Client specifically.

The firmware upgrade will be executed at an agreed time by NTT engineers. The firmware upgrade process can happen out of business hours if required.

© 2023 NTT DATA, Inc. | NTT Ltd. and its affiliates are NTT DATA, Inc. companies.

Unsupported Configurations

The managed SD-WAN service does not include procurement of internet or WAN circuits, or SD-WAN software or hardware / virtual devices. This service does not include proactive network management of the internet WAN circuits nor is NTT the design authority for the SD-WAN network. These services are available from NTT under a separate statement of work.
Orchestrator-SP and Orchestrator Global Enterprise level are not supported (multi-tenancy).

Managed SD-WAN endpoints

Supported Technologies

For a listing of supported Router and Security Appliance models and their respective sizing, consult the MCN Supported Technology documentation.

> **Please note specific models and variants will not be available in all countries. Pease consult with your local team for guidance**.

Supported Configurations

- Single router: A standalone router or a set of standalone routers (managed independently from each other);
- Set of routers in high availability configuration: Two or more routers of compatible models in an HA configuration - either active / passive or active / active;

SD-WAN Endpoint Service Specific Operations

Cisco SD-WAN Endpoint monitors

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Application Aware Routing Policy & Metrics · Data packets transmitted and received, throughput by policy · Loss · Latency · Jitter	Data packets transmitted and received.	✗	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client, or Client's carrier if needed (if Carrier Coordination service has been purchased).	N/A
Transport Performance · Loss · Latency · Jitter	Data packets transmitted and received	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client, or Client's carrier if needed (if Circuit Coordination service has been purchased).	N/A
Bi-Directional Forwarding Detection (BFD) session metrics · Max & total sessions · Up & down sessions · Flap sessions	Bi-directional forwarding detection session metrics per device	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client, or Client's carrier if needed (if Circuit Coordination service has been purchased).	N/A
Transport Location (TLOC) BFD session metrics · Max & total sessions · Up & down sessions · Flap sessions	Bi-directional forwarding detection session metrics per Transport Location (TLOC)	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client, or Client's carrier if needed (if Circuit Coordination service has been purchased).	N/A

Control Plane Performance (vManage) · System load average · CPU · Memory · Disk usage · Processes · NTP peers	Control Plane metrics for the relevant areas	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client.	N/A
Detailed Overlay Management Protocol (OMP) stats · Packets sent / received · Hello sent / received · Routers sent / received / installed · TLOC's (Transport Locations) sent / received / installed · vEdge peers · vSmart peers	Metrics for the SD-WAN Overlay Management Protocol	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue.	N/A
WAN Edge Inventory · Deploy status of the device · Validity status of the device	WAN Edge device health and status	✓	N/a	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client, or Client's carrier if needed (if Circuit management service purchase).	N/A
Hardware Component Health · CPU · Memory · Fans · Power Supplies	WAN edge device hardware health	✓	N/A	Engineering Teams will diagnose and try to resolve the issue, contacting the hardware maintenance provider as required.	N/A
OSPF · Neighbour state · Interface change · State changes	OSPF Routing protocol health and metrics	✗	N/A	Engineering Teams will diagnose and try to resolve the issue.	N/A
BGP · Neighbour state · Messages	OSPF Routing protocol health and metrics	✗	N/A	Engineering Teams will diagnose and try to resolve the issue.	N/A

Aruba Silver Peak SD-WAN Endpoint monitors

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Ping / Network	Time taken for responding to a ping	✗	Graphs for ping response time	Engineering teams will resolve the issue	60

	from a poller, and packet loss		Graphs for packet loss percentage		
Device Availability	Up / down status of the end-point	✓	nformation whether the device is operational and reachable	Engineering teams will resolve the issue	60
Next Hop	Monitors WAN next hops of Aruba Silver Peak appliance	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client. (or Client's carrier if Circuit Coordination service offering has been included).	120
HTTP port status	Monitors http page (port TCP80) load time and response status. (Aruba Silver Peak)	✗	Establish if TCP port 80 is responsive to requests.	Engineering teams will resolve the issue	60
HTTPS port status	Monitors https page (port TCP443) load time and response status. (Aruba Silver Peak)	✗	Establish if TCP port 443 is responsive to requests.	Engineering teams will resolve the issue	60
Disks	Monitors Silver Peak appliance disk health.	✓	Monitors the appliance disks at the device level	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client if needed.	120
Memory	Memory usage of the Aruba Silver Peak appliance	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client if needed.	120
System Alarms	Monitors ongoing Aruba Silver Peak alarms	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client if needed.	120
SSL Certificates	Monitors SSL validity information across all common SSL ports.	✓	Monitors validity of SSL information.	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client if needed.	1800

SD-WAN Endpoint Service Requests

Note
Please note that NTT applies a fair use policy in the execution of these requests.
For more information related to the Fair Use Policy please refer to the *MCN Statement of Work*.

As part of the Service, the fulfilment of the tasks listed in the table below are included.

SD-WAN Endpoint Service Requests

Task	Description	Included
Update / modify an access control list (ACL)	Updates to, or modification of, an access control list (ACL)	✓
Change IP address	Changing of an IP address	✓
Application Policy	Application family profile add / change / deletion.	✓
Application Family	Add / delete applications from a specific SD-WAN Application Family	✓
SD-WAN Application Definition	SD-WAN application definition creation, modification or removal	✓
CoS / QoS changes	Class of Service (CoS), Quality of Service (QoS) changes	✓
Ethernet port configuration	Ethernet port configuration changes including speed, duplex, VLAN assignment.	✓
OS Configuration	Modify an OS configuration option.	✓

DHCP Updates	Updates to DHCP configuration at client sites, including; • Changes to DHCP helper, relay server • Reserved ranges • Changes to DHCP DNS • NTP changes	✓
IPSEC VPN tunnel changes	Changes to an IPSEC tunnel from the SD-WAN environment to another device.	✓
Manual failover between underlay links	Manual failover between underlay network circuits, on request of the client.	✓
Stateful Firewall Changes	Changes to stateful firewall rules (if utilized on edge devices), including; • Enabling stateful firewall • Creation of new firewall rules • Changes to existing firewall rules • Removal of rules • Setup of firewall diagnostics Note: feature availability will vary depending on software license version	✓
IPS Changes	Changes to Intrusion Prevention Software rules (if utilized on edge devices), including; • Enabling IPS in detect or protect mode • Change from protect to detect mode, or vice versa • Change IPS log target • Add or remove IPS signature from whitelist / blacklist • Change in security mode between Balanced, Connectivity or Security modes (ie; changes between Vendor provided signature sets) • Changes Note: feature availability will vary depending on software license version	✓
URL Filtering Changes	Changes to URL filtering software rules (if utilized on edge devices), including; • Enabling URL filtering per overlay VPN • Addition or removal of URL to a whitelist or blacklist • Change whether certain web categories / web reputations are allowed or blocked • Change block action (ie; change content of blocked webpage or redirect URL) • Changes to alerting and logging approach (ie; alert based on blacklist / whitelist or reputation / category). Note: feature availability will vary depending on software license version	✓
Anti-malware Changes	Changes to Anti-malware software rules (if utilized on edge devices), including; • Enabling AMP hashing • Changes to the log target • Enabling of ThreatGrid (cloud based file analysis) • Changes to ThreatGrid file type Note: feature availability will vary depending on software license version	✓
DNS Security	Changes to on box DNS Security policies (if utilized on edge devices), including;	✓

	• Enabling on box DNS security policies • Changes to domain bypass list Note: feature availability will vary depending on software license version	
TLS / SSL Decryption	Changes to TLS / SSL decryption rules (if utilized on edge devices), including; • Enabling TLS / SSL decryption • Updates to Enterprise CA certificates Note: feature availability will vary depending on software license version	✓

Firewall and Security Service Requests

IDS/IPS, URL filtering and other advanced security features' correct operation is heavily dependent on the application(s) being protected, which means that the ones applying the intelligence on the security policy must be the customer's relevant contacts.

The scope of the management of the IDS/IPS and advanced security features of the SD-WAN appliances will be LIMITED TO APPLY CHANGES based on the client's request.

NTT expects the client will identify the changes to be performed based on the client's SIEM platform (or equivalent log management tool used by the customer uses). On the client's SIEM, the reason why applications are blocked generating false positives, or not blocked when they should be, would be identified by the customer. As part of the ongoing management of the advanced security features of SD-WAN devices, review of all security logs for an unidentified error or false positive is not included in the service. This is an activity for the client to perform. While NTT will make all attempts to reduce the number of false positives, it will not be responsible for authentic users being denied access to the customer application, as a result of client defined security policies.

> Please note enablement of IPS, URL Filtering, AMP, DNS Security and TLS / SSL Decryption functionality, as well as creation of new overlay VPN networks, is treated as a project task and is a separately chargeable activity.

Optional Tasks (additional charges will apply)

Task	Description
Deployment of new physical locations	Deployment of new SD-WAN endpoints. Must be conducted with support of regional NTT entity
New overlay VPN setup	Creation of new overlay VPN's can be conducted, however will be treated as a chargeable project

Disclaimer

While NTT will help the client resolve Security issues, NTT does not take responsibility for any loss as a result of a security incident.

NTT will use reasonable efforts to resolve problems as quickly as possible.

Service Transition

Tasks included in the Standard Transition

As part of the Service, the following tasks are included in the setup fee:

- Inventory of the device;
- Review of the existing configuration templates;
- Review of the configuration of network interfaces;
- Review of the control plane deployment, including high availability and redundancy configuration (for on-premise deployments)
- Review of firmware upgrades and their installation if agreed with the Client as detailed in section *Managed Campus SOW*
- Change of the credentials required by the administrative and supervisor users required for management by NTT and the Client;
- Review and change the configuration of syslog or SIEM parameters (if a syslog or SIEM exists);
- Review and documentation of the device configuration;
- *In highly available environments*: Review and documentation of the service high availability, clustering or stack configuration;
- Creation and review of monitoring;
- Initial configuration of in-SD-WAN control plane backup strategy (if required);
- Initial configuration of external-to-SD-WAN control plane backup strategy (if required);
- Initial configuration of a SD-WAN on-premise control plane backup strategy
- Implementation of security standards; and
- Documentation of the device.

Tasks excluded from the Standard Transition

The following tasks are excluded from the service transition and require further services.

- Physical activities at the premises where the device is installed;
- Audit and review of the physical premises where the device is installed;
- Review of the configuration or actions of other connected devices not under management;
- Analysis and redesign of the network topology is an activity that can be conducted as a chargeable engagement, if not included as part of the Statement of Work; or
- Remediation Activities to be conducted after the audit may be chargeable, if not included as part of the Statement of Work.

© 2023 NTT DATA, Inc. | NTT Ltd. and its affiliates are NTT DATA, Inc. companies.