Client Connectivity Requirements

1 Overview of Service

This document should be consulted during the sales engagement with the Client and during the transition phase of the Client engagement. It provides:

- A high-level overview of how NTT Managed Services platforms connect to a Client's network environment.
- Bandwidth guidelines for NTT management connectivity into the network environment.
- Details of specific firewall ports, protocols, credentials and other client responsibilities required to establish connectivity between NTT's Managed Platforms and a Client's network environment.

2 NTT DATA's Managed Services Platform

At the heart of NTT's Managed Services is our Managed Services Platform (MSP): an integrated suite of monitoring, management and automation solutions leveraging both software packages and microservices to enable platform-driven operations of IT environments:

- **A global IT Service Management platform** for ITIL-based workflow automation.
- **Unified Monitoring and Operations** framework for integrated monitoring, event collection and correlation.
- **Operations Automation** incorporating auto-discovery, automated service activation, event enrichment, incident resolution, task fulfilment and workload management.
- **Omnichannel** technology for integrated, context-based communications with Clients.
- **AIOps and Analytics** to collect, collate, analyse and inform on the performance across technologies.
- **Privileged Access Management** for auditable, secured access to privileged accounts for the management of the Client's IT infrastructure.
- **Client Portal** to provide a single interface in the health and performance of the Client's IT environment.

3 Connecting to the NTT DATA Managed Service Platform

The standard approach for connecting to NTT's MSP based on technology options and cost, is to leverage a "Site-to-Site (S2S) IPSEC Virtual Private Network (VPN) Tunnel" with the Internet acting as the underlying transport network. In the event where this cannot be leveraged, custom connection options can be explored, however, additional costs are likely to be incurred. Technical considerations can also be explored prior to contracting with NTT.

3.1 Managed Services Platform Connectivity

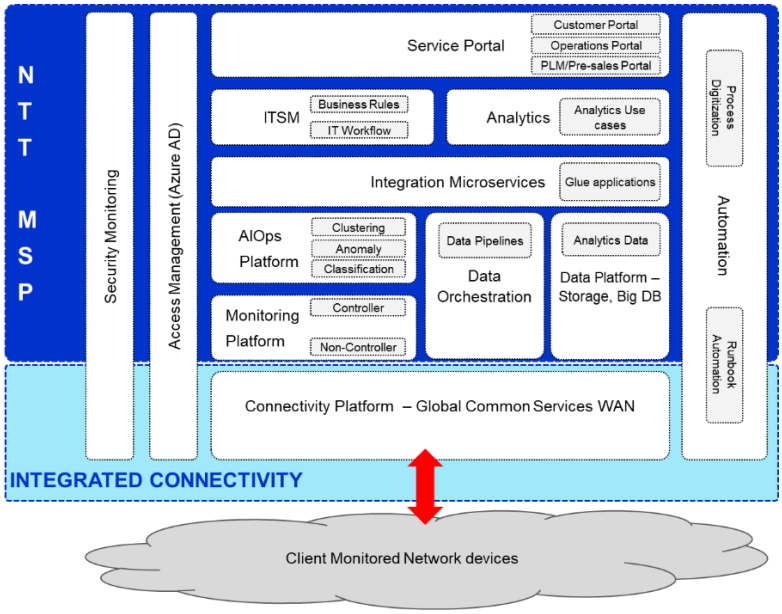
NTT's Managed Services utilise a collection of management, monitoring, configuration and connectivity applications and appliances distributed across various hosting locations. Logical separation is maintained between the management networks and workload networks of Clients.

Included in the MSP is a router from which a secured S2S IPSEC VPN link is established to the Client's environment to manage the Client's estate.

Because communication between NTT and the Client is established via a S2S IPSEC VPN, Clients are ensured that all traffic flows between NTT and their environment is encrypted and secured end-to-end. From a traffic flow perspective, all communications between the Client and NTT must pass through the VPN connection and may not be transmitted outside of the VPN tunnel.

3.2 S2S Ipsec VPN Tunnel

The following graphic illustrates the high-level conceptual architecture:



The VPN solution provides NTT with a means of securely accessing the Client's network infrastructure, contracted under the Managed Services Agreement, without exposing NTT's internal subnets to the internal networks of the Client and vice versa. The VPN will be established as a single S2S IPSEC VPN tunnel over the Internet between the Client-side device and the NTT Managed Services Platform.

It is critical that the Client provide NTT with access via routing and firewall rules to all IP addresses that NTT is meant to manage under the Managed Services Agreement. The Client is also required to provide the Client-side "termination equipment" of the IPSEC VPN Tunnel to NTT. In addition, the Client is also required to provide NTT with a dedicated /24 IPv4 address subnet from their own internal IP range (256 IP addresses). This range must be from the same CIDR block to ensure that all connections needed for the NTT MSP will be routed from the Client to the MSP. It is preferrable that the /24 IP subnet is an RFC1918 address space. Since an entire /24 subnet is required, there is no need to NAT any addresses.

The /24 IP subnet that must be provided by the client is used to create the required IP subnets within the NTT MSP to allow for the necessary connectivity between the client's managed environment and the MSP. The subnets is used within the MSP to provide IP addressing to the monitoring and management platforms among others. The addressing also ensures that the architecture within the MSP is consistent, and that routing is not complicated through requiring network address translation (NAT) if smaller IP subnet ranges were used. Using the allocated subnet allows each client's hosted environment to be an isolated routing domain and contributes to the NTT security policies in place. By having a logically consistent IP addressing structure within the MSP, automation of the environment is also ensured.

The required peer IP addresses are required to establish the IPSEC tunnel and are the Internet (public) IP addresses assigned to the link that connects the Client environment to the Managed Services Platform. The Client must provide this address information to NTT and must also provide the remote network detail to NTT as part of those requirements to establish Client connectivity. The remote network is the /24-bit IP address subnet previously described in this document.

3.3VPN Encryption and protocols

For the connection between the Client and the NTT MSP to be successfully established, the encryption algorithms, authentication algorithms and pre-shared keys must be identical (symmetrical) on both sides of the link. However, the peer IP addresses that are configured on the

device interfaces will be reversed between the two peers i.e., the remote IP address configured on the NTT side of the connection will be the local IP address on the Client-side router and vice versa.

The pre-shared key is used as part of the authentication mechanisms for establishing the secured VPN connection and is the only component required for establishing Managed Service connectivity, which will not be made available, prior to configuring the router interface(s). For security purposes, the pre-shared key will

- be provided to the client (or the authorised representative) by the NTT deployment engineer or
- be provided by the client (or the authorised representative) to the NTT deployment engineer.

at the time of configuring the VPN connection. The pre-shared key must be communicated between the NTT engineer and client (or authorised representative) verbally (for example, by telephone) and not in any written format. This is to reduce any security risks.

The pre-shared key must meet the following criteria:

- It must be at least 12 characters in length.
- It must contain at least one upper-case character.
- It must contain at least lower-case character.
- It must contain at least one numeric character.
- It must contain at least one special character.

The remote network detail must be provided to NTT as part of the requirements to establish the connectivity and is the /24-bit IP address subnet previously described in this document.

NTT prescribes to a minimum accepted encryption and security standard when establishing connectivity through the S2S IPSEC VPN. This requires that specific information is provided prior to creating the connection. These details must be captured in the Client Connectivity Requirements Workbook under the ‘Connectivity’ tab. The information on this tab relates to the protocols, encryption standards and other such related parameters to configure the S2S VPN. When establishing the VPN tunnel, Virtual Tunnel Interfaces (VTi) are preferred over Policy Based Routing (PBR). There is, however, an option to make use of VNET peering where the client has an existing instance, however this method can be complicated and results in additional costs.

3.4 SaaS Connectivity Requirements

The MSP connectivity requirements for managing a SaaS environments such as Cisco Meraki, Juniper Mist, Fortinet and so forth differs from the requirements described in the preceding paragraphs. This is because of the manner in which connectivity is established to the environment and is usually achieved through a secured Internet connection to the vendor portal such as the management dashboard. Typically, these solutions make use of an HTTPS connection between the NTT MSP and the SaaS portal via a web browser. The data is then retrieved through API or XML calls. It is also often the case that all edge devices in the SaaS environment are monitored, managed and accessed via the SaaS portal. In such instances, it is not necessary to establish a S2S IPSEC VPN between the managed estate and the NTT MSP. This does not preclude the requirement for the /24 IP subnet described in the previous sections. Only the requirement for the S2S IPSEC VPN connectivity is unnecessary. The /24 IP address space will be used to provide IP addressing for the MSP monitoring and management platforms. i.e. the /24 addressing will be used in exactly the same way as described above.

Depending on the SaaS solution in question, changes may be required on the client’s perimeter firewall(s) to allow communication between the MSP and the SaaS environment. These rules, along with all other firewall security requirements must be captured in the Client Connectivity Requirements Workbook under the ‘Security’ tab.

Although a S2S IPSEC VPN will not be required for most SaaS environments, it may be a requirement to establish a S2S IPSEC VPN connection between the MSP and the client's environment to enable operations other than monitoring the managed devices, such as firmware upgrades, if these operations cannot be performed directly through the SaaS portal. In client environments where there is a combination of SaaS technologies and non-SaaS (legacy) technologies, the S2S IPSEC VPN connectivity will need to be established as described in this document.

3.5 Privileged Access Management

Privileged Access Management is enforced for all CI's under management of NTT. This ensures that all access to managed CI's is audited and that only the required level of access is granted when accessed by authorised NTT personnel. To simplify the firewall rules that will need to be implemented in the client's environment, the PAM platform and all of its related traffic will always be sourced from the same /28 range of IP addresses. The PAM address space is allocated from the /24 IP address space provided to NTT by the client. When accessing a device from the NTT MSP, all information relating to the access is recorded by PAM for security and auditing purposes. It is therefore a requirement that NTT is granted an account by the client to access the devices to facilitate this functionality. The account may be either a system account (preferred) or a named account that has administrative access to all devices under management.

3.6 Naming Standards

There are several RFCs that deal with naming standard best practices such as RFC921, RFC952, RFC1035, RFC1178, RFC1213 and RFC2181. Each of these deal with the naming standards for different aspects of a network and the primary aim thereof is to ensure that no incompatibilities are created between the various components of network. In alignment with these practices naming standards used in NTT's Managed Service offering supports the following characters:

- A – Z (upper case and lower case)
- 0 – 9
- - (dash)
- _ (underscore)

Where names do not comply with these requirements, they will be mapped to the closest corresponding supported character. As an example:

ä	will be mapped to	a
ç	will be mapped to	c
ë	will be mapped to	e
ê	will be mapped to	e
ö	will be mapped to	o
ô	will be mapped to	o
ü	will be mapped to	u
û	will be mapped to	u
ß	will be mapped to	s

3.7 Bandwidth Requirements

The following table provides guidelines on the bandwidth requirements to establish connectivity between the Client and the NTT MSP. The standard connectivity between the systems will be established via a single unified communications link.

The bandwidth requirements depicted are guidelines for managing the number of devices listed via SNMP and it is assumed that there will be active support (operational) sessions on 10% of the total number of managed devices at any given time. It should also be noted that the values shown exclude any bandwidth requirements to facilitate device configuration backups to the NTT MSP, firmware upgrades and or any other similar features. Bandwidth requirements for configuration backups are dependent on the format of the backup file, such as whether it is a text file, binary file, database etc, size of each file and the number of files to be transmitted simultaneously over the link. SaaS solutions may require specific minimum bandwidth and may be different to the values shown below. The minimum values required by the vendor should be adjusted sufficiently to ensure that the environment is not impacted by configuration backups and or daily operational support. Consideration should also be given to the time at which the backups will be performed i.e., contention ratios across the link.

Similarly, software (and firmware) updates may also require additional bandwidth depending on the size of the software package, the number of devices to be updated simultaneously, the time at which such updates are expected to be executed and so forth. Sufficient bandwidth should be made available for these purposes to ensure that monitoring and management of the environment is not impacted during the software update process.

Number of CIs	Number of ports/interfaces	Kbps required
0-250	Up to 5600	1024
251-500	Up to 11500	2048
501-1000	Up to 22000	4096
1001-1500	Up to 33000	10240

3.8 Deployment Models

All monitoring and management will be performed remotely via NTT. i.e., no monitoring and or management infrastructure or toolsets will be located at a Client's premises and all operational tasks will be performed remotely.

4 Firewall Port Requirements

This section describes the firewall ports required for connectivity between the NTT monitoring platforms and the Client's configuration items for monitoring and management purposes. For correct connectivity, a range of firewall ports must be opened.

Note: All elements and systems inside the MSP involve their specific IP addresses being configured for firewalling purposes (on both Client and MSP configurations). Specific ports for additional management requirements may be necessary for instances where Clients have configured applications to use non-standard ports.

Where the Client gateway is firewalled, it must be ensured that ISAKMP (UDP 500) and IPsec (IP Protocol 50) is enabled bi-directionally through the firewall.

The following tables indicate the ports and protocols required that need to be configured to ensure connectivity for managing the Client's network environment, and that the correct communications can take place between the Client's environment and the MSP.

The tables below are for information purposes only.

The specific IP addressing and ports required for the Client's environment should be captured in the Security tab of the Client Connectivity Workbook.

4.1 PAM Platform to Client Infrastructure

If the Client uses custom ports for HTTP and or HTTPS access to devices, the custom ports will need to be added to the list of ports shown.

Source	Protocol	Source Port	Destination	Destination Port	Purpose
PAM Platform (MSP)	TCP	any	Wired LAN/WAN Device	22	SSH authentication
PAM Platform (MSP)	TCP	any	Wired LAN/WAN Device	3389	RDP authentication
PAM Platform (MSP)	TCP	any	Wired LAN/WAN Device	80 443	Web authentication
PAM Platform (MSP)	UDP	69	Wired LAN/WAN Device	any	TFTP device config uploads

4.2 SPEKTRA Management Platform to Client Infrastructure Requirements

Source		Protocol	Source Port	Destination	Destination Port	Purpose
Wired LAN/WAN Device		UDP	162	Management Platform (Trap Explorer)	any	SNMP Traps. Device config traps to NCM, and Cold start traps to Smarts IP-AM.
Management Platform (Device Server)		ICMP	ICMP	Wired LAN/WAN Device	any	ICMP Ping queries to Client network wired LAN/WAN devices
Management Platform (Device Server))		UDP	161	Wired LAN/WAN Device	any	SNMP polling to Client network wired LAN/WAN devices
Management Platform (Device Server)		TCP	22	Wired LAN/WAN Device	any	SSH requests to Client network wired LAN/WAN devices
Management Platform (Device Server)		TCP	23	Wired LAN/WAN Device	any	Telnet requests to Client network wired LAN/WAN devices
Management Platform (Device Server)		UDP	69	Wired LAN/WAN Device	any	TFTP requests to Client devices
Management Platform (Device Server)		TCP	80 443	Wired LAN/WAN Device	any	HTTP/HTTPS requests to Client network LAN/WAN devices

4.3 Automation Platform to Client Infrastructure Requirements

Source	Protocol	Source Port	Destination	Destination Port	Purpose
Automation Platform (MSP)	TCP	any	Wired LAN/WAN Device	22	SSH operations for Patch Assessments and Updates
Automation Platform (MSP)	UDP	Any	Wired LAN/WAN Device	161	SNMP operations for Patch Assessments and Updates
Automation Platform (MSP)	TCP	Any	Wired LAN/WAN Device	443	HTTPS operations for Patch Assessments and Updates
Automation Platform (MSP)	ICMP	ICMP	Wired LAN/WAN Device	Any	Inventory Discovery

4.4SPEKTRA Edge Backup Requirements

Source	Protocol	Source Port	Destination	Destination Port	Purpose
Wired LAN/WAN Device	TCP	Any	Edge Backup Platform	22	SFTP upload of configuration (backup)
Edge Backup Platform	TCP	22	Wired LAN/WAN Device	Any	SFTP download of config (restore)

4.5Service Experience Insights Requirements

For MCN Clients that subscribe to the Service Experience Insights offering the firewall configurations depicted in the table below apply. It should be noted that all agents use an outbound internet connection for probing traffic to targets and controller traffic to the SEI controller. For inbound connections

Static and Cloud Agents can be optionally configured as “managed targets” that respond to probing from other agents. This requires the agent to reply to inbound probing traffic.

Managed target agents do not support NAT traversal.

If the destination “managed target” agent is behind a firewall or NAT, the source agent will send probing data to the external IP and the firewall or NAT must be instructed to route the inbound traffic to the agent’s internal IP.

Set inbound firewall policy after configuring the firewall to route inbound probing traffic to the managed target.

Source	Protocol	Source Port	Destination	Destination Port	Purpose
Probing traffic: Required for agents to complete probing sessions with targets outside of the firewall					
Client SEI Agents	TCP	Any	Configured HTTP(S) targets	80 443	HTTP(S) target addresses
Client SEI Agents	TCP	Any	Configured Speed Test targets	Configured Speed Test port (Default 8080)	Speed Test target addresses
Client SEI Agents	ICMP	Any	Configured ICMP targets	N/A	• ICMP Probes to default and custom targets • ICMP Time exceeded messages from external servers should not be blocked by firewall for path tracing
Client SEI Agents	UDP	Any	Configured UDP targets	Configured UDP Port (Default 5001)	UDP target addresses
Client SEI Agents	UDP	Any	UDP/ICMP Targets for which hop trace is enabled	Configured UDP Port (Default 5001) for managed UDP targets and UDP port 33434 for other targets	Hop tracing on Linux and Mac OS (only ICMP is used on Windows OS where the agent just executes tracert command
Controller traffic: Required for Agent to connect to Service Experience Insights					
Client SEI Agents	TCP	Any	*.edgelq.com	443	Access to SEI controllers (HTTP2 must be supported when an HTTP proxy is configured)
Client SEI Agents	UDP	Any	DNS Server IP	53	DNS Lookups

Source	Protocol	Source Port	Destination	Destination Port	Purpose
Client SEI Agents	UDP	Any	any	3478 19302	Stun server - used to determine public IP Address
Required for agents to respond to inbound probing from other agents					
* or addresses of originating agents sending inbound probing traffic	TCP	80 443	Any	Any	HTTP(S) targets
* or addresses of originating agents sending inbound probing traffic	TCP		Any	Any	Speed Test targets
* or or addresses of originating agents sending inbound probing traffic	ICMP		Any	Any	ICMP targets
* or addresses of originating agents sending inbound probing traffic	UDP		Any	Any	UDP targets
* or addresses of originating agents sending inbound probing traffic	UDP		Any	Any	Enables agent to respond to traceroute sessions from Static Agents, Cloud Agents, and Mobile Agents for macOS. Mobile Agents for Windows use ICMP to execute tracert command.

5 Client and NTT Responsibilities to Enable Connectivity

5.1 Client Responsibilities

The following information is required during the Inception phase of Transition. Timelines will be agreed with the Client during Transition planning to provide the information.

- Internet connectivity to NTT's MSP including firewall, router, public IP address on the WAN interface of the router and any other Client termination equipment.
- Client termination equipment must be compatible with the IPSEC VPN encryption standards as described under the VPN Encryption and protocols section of this document.
- Ensuring that the firewall /security appliance on the Client side is correctly configured to allow communication protocols, IP address ranges, ports etc. to pass through so that the environment can be monitored and managed.
- Ensuring that all devices to be managed are configured with the relevant parameter as per the information provided to enable management thereof.
- Providing NTT with a list of all equipment to be monitored and managed.
- Providing NTT with all credentials to access devices and services, i.e., usernames, passwords, community strings and protocols. Examples are listed in the table below (non-exhaustive).

(a) SNMP based network devices

Parameter	Device Type	Description
Username	All (routers, switches, AP, WLC, WOC, ADC)	The username used to login to the device via a remote (terminal) session. This will also be applicable to SNMPv3 usernames and console usernames.
Password	All	The corresponding password for the username used to login to the device as described above.
Secret (privileged) password[1]	Routers, switches, AP, WLC	The privilege level password used to perform administrative tasks on the device. Sometimes referred to as the 'enable password' (See footnote).
Access protocol	All	The protocol used to access the device when logging in to the device using any of the listed or other methods. Usually this would be, but is not limited to, telnet, SSH, http and https. (Secured protocols are preferred over non-secured protocols).
Read-only community string	All	The text string used by SNMP management stations to query the device for information using SNMP protocol. Applicable only to where SNMP v2c is in use
Read-write community string	All	The text string used by SNMP management stations to configure (add, remove or modify) any parameters on the device by using the SNMP protocol. Applicable only to where SNMP v2c is in use.

[1] *Secret password also refers to devices/vendors that make use of role-based access to connect/monitor a device and or administer the device (e.g., HP). Where a username and password are required to administer the device, these credentials must be included as the 'privilege' level password.*

Parameter	Device Type	Description
username	Routers, switches, AP, WLC	The username used to login to the device via a remote (terminal) session.
SNMP v3 Authentication Protocol	All	The protocol used to access the device when logging in to the device using any of the listed or other methods. (SNMPv3 Authentication Protocol (MD5, SHA, Default))
SNMP v3 Authentication Password**	All	SNMPv3 Authentication Password
SNMP v3 Privacy Protocol*	All	SNMPv3 Privacy Protocol possible values (Default, DES, AES128, AES192, AES256)
SNMP v3 Security Level*	All	Mandatory SNMPv3 Security Level possible values (authpriv, authNoPriv, noAuthNoPriv)

(b) API based network devices

Parameter	Device Type	Description
API key	Cloud based SDN WAN	The API key used to login to get the devices from cloud-based SD-WAN
username	All	The username used to login to the device via a remote (terminal) session.

- Creating any accounts that may be required to manage any configuration item that form part of the managed environment.
- Providing and identifying the infrastructure that will be used for connectivity to the NTT Managed Services Platform to establish a S2S VPN if applicable.
- Configuring the interface of the Client-side router of the MSP connection.
- Providing NTT with the public IP address assigned to the interface on which the VPN connection must be configured.
- Providing NTT with a 24-bit IP address subnet from within their IP addressing space (remote network).
- Supporting and administering the Client-side circuit of the S2S VPN with the relevant carrier (i.e., the portion that lies between the MSP and the Client).
- Ensuring that all configuration items to be managed meet the minimum required specifications in terms of hardware, software, firmware, patch levels and operating systems.
- All devices to be managed are SNMP enabled or configured with API credentials, whichever is applicable, and that it is reachable from the NTT monitoring and management platforms to facilitate discovery and configuration.

5.2NTT Responsibilities

NTT is responsible for the following requirements for the connectivity of the Client in order to subscribe to Managed Campus Network Services.

- Providing, supporting, and maintaining all infrastructure in the NTT Managed Services Platform.
- Configuring and managing the MSP side of the S2S VPN connection.
- Providing the Client with all details for the connection such as the NTT IP addressing, authentication protocols, encryption protocols and methods (and any associated keys and or certificates).
- Providing the Client with details of the minimal SNMP and or API configuration requirements, whichever is applicable.
- Supporting and administering the MSP side of the S2S VPN circuit and all associated equipment.

6 Platform, Connectivity and Tooling

6.1 Management Tools

The configuration and placement of NTT's management tools are dependent upon solution requirements. The following guidelines generally apply:

- NTT will install management tools within dedicated access management zone that connect to client network. NTT may use shared management tools, but subject to the following restrictions:
  - Bidirectional connectivity is required for management tools
  - Certain managed services may require the installation of additional agents and tools to connect to client network

6.2 Connectivity to the Client Environment

NTT requires that the connection from the NTT operations facility to the Client environment is performed over one or more of the following transports:

- An IPsec VPN tunnel established between the Client platform and NTT's platform. This is the default option that provides encryption of all the communications from firewall to firewall.
- IPsec VPN must be routed with no network address translation (NAT) between NTT and the Client IP ranges in the Client platform must be assigned by NTT; and
- Client is required to provide /24 IPv4 subnet for use exclusively by NTT. The IP range has to be /24 subnet and can't be smaller.
- Client is required to provide public IP address for IPSEC connection.
- Any access methods outside of those listed above will be subject to NTT approval and may be subject to additional charges.

Below information is only applicable where Palo Alto SASE is part of the MCN Solution

- Where management of Palo Alto SASE is included in the scope of the Service, a service connection must be established between the NTT platform and every Palo Alto SASE region in scope. Client must purchase a service connection license from Palo Alto.

6.3 Service Specific Access Requirements

This clause describes any Service specific access requirements between the Client and NTT:

(a) Platform Access

To deliver the Service, the NTT must have remote access to the Client Network Environment. This access requires a high level of availability, reasonable latency and sufficient bandwidth.

(b) Identity Management

Primary management activities will be performed from NTT Management Infrastructure. The Management Infrastructure is a remote access solution that uses multi-factor authentication (MFA) and session recording to provide NTT with the necessary access to manage solutions while tracking identity and activity of each user.

The primary features of the Management Infrastructure are:

- multi-factor authentication (MFA)
- session recording
- high availability

Glossary

ACL	Access Control List
ADC	Application Delivery Controller
AH	Authentication Header
AIOPS	Artificial Intelligence Operations
AP	Access Point
API	Application Programming Interface
CI	Configuration Item
CIDR	Classless Inter-Domain Routing
CMDB	Configuration Management Database
CMS	Configuration Management System
COE	Centre of Excellence
ESP	Encapsulated Security Protocol
ESXi	Elastic Sky X Integrated (server virtualisation platform)
HTTPS	Hyper Text Transfer Protocol Secure
HUC	Hosted Unified Communications
Hyper-V	(formerly Windows Server Virtualisation (Microsoft hypervisor)
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technologies
ID	Identification
IKE	Internet Key Exchange
IP	Internet Protocol
IP-AM	IP Availability Manager
IPSEC	Internet protocol security
IT	Information Technology
ITIL	IT Infrastructure Library
ITSM	IT Service Management
ISAKMP	Internet Security Association and Key Management Protocol
Kbps	Kilobits per second
KVM	Linux Kernel-based Virtual Machine (Suse and Red Hat)
LAN	Local Area Network
MCN	Managed Campus Networks
MCP	Managed Cloud Platform
MPLS	Multiprotocol Label Switching
MSP	Managed Services Platform
NAT	Network Address Translation
NCM	Network Configuration Manager
OS	Operating System
QoS	Quality of Services
PAM	Privileged Access Management
PSTN	Public Switched Telephone Network
RSP	Remote System Probe
S2S	Site-to-site
SA Lifetime	Security Association Lifetime
SDN	Software Defined Networking
SHA1	Secure Hash Algorithm 1
SMSO	Standard Managed Services Operation
SNMP	Simple Network Management Protocol
SSH	Secure Shell

TCP	Transport Control Protocol
TDC	Topology Data Collection
TIM	Transition Implementation Methodology
TFTP	Trivial File Transport Protocol
UDP	User Datagram Protocol
UIM	Unified Infrastructure Management
VMware	Virtual Machine Ware (Virtualisation and cloud computing software)
VoIP	Voice over IP (Internet Protocol)
VPN	Virtual Private Network
VRF	Virtual Route Forwarding
WAN	Wide Area Network
WLC	Wireless LAN Controller
WOC	WAN Optimisation Controller