Managed Cisco Digital Network Architecture Center (DNAC) Technical Service Description

Overview of Service

All Cisco DNA devices which are managed as part of the Service will be supported in accordance with the NTT processes described in the *MCN Statement of Work.* Technology specific tasks associated with the Cisco DNA technology stack are described in this section. During management, NTT will allow read-only client access to DNA center but does not currently support co-management as this causes issues in terms of responsibility and change audits.

The scope of the Managed Cisco DNA Service is as follows:

- DNA Center Appliance
- DNA Center Features
  - Golden Image Management
  - Upgrade Pre and Post-Checks
  - Leveraging DNA Center Automation
  - Cisco DNA Analytics and Assurance
  - Policy and Cisco Software-Defined Access (SD-Access) which may also be synchronised with Cisco ISE.
  - Cisco Smart Licensing
  - My Cisco Entitlements
- Cisco DNA Expansion Pack products:
  - ISE is supported as a separate Technical Service Description (Refer to the MCN - Managed Cisco Identity Services Engine (ISE) Service Description documentation)

Client Responsibilities and Prerequisites

- The Client must be in possession of an active software and hardware contract with the vendor for the Appliances under management, or a vendor approved third party such as NTT Uptime Support Services.
- The Client must delegate authority to NTT engineers to contact the firewall vendor (or third party) directly for the purposes of the managed service.
- Any procurement of licenses and subscriptions (such as Cisco DNA Advantage or Cisco DNA Essentials subscriptions), if required.
- Any software or firmware operating on the device must be a version currently supported by the vendor.
- Administrative access to the on-premise instances of the DNA Center is required to manage the described devices.
- Administrative access to the DNA Center portal is required to manage the described devices.

Service Design

The complete service is defined by the combination of the following items:

- **Base Managed Campus Network Service Operations**- service delivery operations that are common to all Managed Campus Network Services. See *MCN Statement of Work*
- **Common Operations**- service delivery operations that are common to all services within the category of Network Management. See *MCN Common Network Management Service Description*
- **Service-Specific Operations**- service delivery operations that are specific to this Service. These operations are additive to the *MCN Statement of Work* and Common Operations

Supported Technologies

Includes Devices covered by the DNA Center Compatibility Matrix as listed on the vendor's website:

- DNA-enabled Wired & Wireless LAN including
  - Wired Switches
  - Wireless Access Points (AP's)
  - Wireless LAN Controllers (WLC's)
  - Routers
- DNA-enabled Security Appliances
- Cisco DNA Traffic Telemetry Appliances
- Terminal Services Gateways (Device Management Only - e.g. Image management, Distribution, Updates per specific customer requests)
  - Cisco 1100 Terminal Services Gateway
- Voice Gateways (Device Management Only and Updates per specific requests - no support for Voice Circuit Configuration within this service)
  - Cisco VG Series Voice Gateways
- Integrations
  - IPAM Module Integrations - Bluecoat and InfoBlox (Licenses and Management of IPAM tools themselves are not included through DNAC)

Configurations Not Supported

- The managed Cisco DNAC service does not include procurement of internet or WAN circuits, or DNA software or hardware / virtual devices. These services are available from NTT under a separate Statement of Work.

Sensitivity Label: General

- Cisco DNA Center Cloud (Deprecated Product)
- Full Management of Cisco DNA Expansion Pack products (apart from ISE) are not currently supported. (See product-specific sections below for full details). Only Installation, Registration, Prechecks and basic Enablement and Product Integration/Connectivity (e.g. entry of Management API keys and Tokens into DNAC) are supported for the following:
    - Cisco Stealthwatch
    - Cisco Umbrella
    - Cisco DNA Spaces
    - Cisco ThousandEyes

Setup and Deployment

Tasks associated with new environment installation and configuration

As part of the Service, the following tasks are included in the setup fee for all Cisco DNA supported devices:

- Automated Inventory of devices
- Registration of supported devices to Cisco DNA Center
- Software Image Management (SWIM)
    - Update of DNAC Image Repository and Creation of Golden Images for the different Cisco device types (Note that this doesn't include creation of the images as part of this Managed Service)
    - Creation of SMUs (Software Maintenance Updates) as required for initial deployment
    - Deployment of initial configuration data to devices using Golden Images where available
- Creation of Administrative and Supervisor users required for management by NTT and the Client
- Creation of Cisco Credentials for DNA Centre
- Setup of initial access into DNAC - configuration of network interfaces and DNAC Network Profiles
- Initial Configuration of SD-Access Fabrics and Transit/Peer Networks
- Creation of DNA Policies and Default Access Rules for Users/Devices/Applications Access (Policy Creation for Group Based, IP Based and Application Based Access Controls)
- Register Cisco Plug and Play
- Configure Proxy Certificates
- Configure Certificates and Private Keys for Remote Connectivity to Devices
- Install SSL keys/certificates associated to protected sites for the advanced services that need them
- Configuration of syslog parameters (if an external syslog or SIEM service exists)
- Configure Debugging Logs
- Configuration of High Availability (HA) - if 2 devices exist at specific locations
- Configure Cisco AI Network Analytics Data Collection
- Monitoring setup
- Configuration backup setup
- Configuration management setup and implementation of security standards
- Device documentation
- Baseline Compliance Reports
- Configuration of log relaying and other log management mechanisms if contracted
- Enable/Disable Cisco AI Network Analytics Data Collection
- Configure the Machine Reasoning Knowledge Base
- Configure IP Address Manager connection if required.
- Configure SNMP Properties
- Configure Image Distribution Server connection
- Installation and Registration (but not detailed configuration) of the following Applications:
    - Cisco Stealthwatch
    - Cisco Umbrella
    - DNA Spaces
    - ThousandEyes

Tasks excluded from new environment installation and configuration

- Rack mounting or physical installation of the device(s)
- Physical setup (cabling of Ethernet and power chords) and labelling of the device(s), or
- Configuration of other connected device(s) not managed by NTT
- Security hardening against a specific baseline is not included (this can be completed as a Professional Services engagement)
- Creation of New Images - only existing images (such as from the vendor or pre-created) will be Added to the Image Repository and Deployed.
- Configuration of Applications and Application Policies - such as for Stealthwatch, Umbrella, App Hosting, Application Visibility or other additional DNAC Apps. Only basic setup and DNAC connectivity to these apps will be implemented as part of this Managed Service. See relevant Applications section (e.g. Stealthwatch) for full details of supported Application tasks.
- Configuration of Smart Account (Smart Licensing Account) and Smart Licensing for DNAC Appliances (The client is responsible for Software Licensing)
- Configure Integration and Data Sharing with Cisco Prime
- Configure vManage/vEdge through DNAC

- Disaster Recovery Design, Configuration and Plans
  - Configure Recovery Sites
  - Configure Witness Sites
  - Failover designs
- Direct Integration of DNAC into Customer's ITSM

These tasks can be completed by the relevant NTT country or regional team as required.

Tasks associated with taking over an existing installation

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

- Device Discovery and Inventory of devices
- Registration of supported devices to Cisco DNA Center
- Configure Image Distribution Server
- Software Image Management (SWIM)
  - Review of the existing Cisco Device Golden Images and SMUs (Software Maintenance Updates) and Add-ons.
  - Upgrade Pre and Post Checks (for Golden Image Distributions and SMU/Add-On Activations)
  - Deployment of initial configuration data to devices using Golden Images where available
- 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 *Platform Maintenance* of the *Base Service Description*
- 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
- Deliver recommendations after the initial review by NTT network engineers
- *In highly available environments*: Review and documentation of the Service high availability, clustering or stack configuration
- Creation and review of monitoring
- Implementation of security standards
- Device documentation
- Baseline Compliance Reports
- Configure Synchronisation of DNA Center with Cisco ISE
- Subscribe to System Event Notifications
- Configure Cisco Device Controllability
- Configure IP Address Manager
- Enable/Disable Cisco AI Network Analytics Data Collection
- Configure the Machine Reasoning Knowledge Base
- Configure IP Address Manager connection if required.
- Configure SNMP Properties
- Configure Image Distribution Server connection
- Installation and Registration (but not detailed configuration) of the following Applications:
  - Cisco Stealthwatch
  - Cisco Umbrella
  - DNA Spaces
  - ThousandEyes

Tasks excluded from taking over of an existing installation, 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
- Security hardening against a specific baseline is not included (this can be completed as a Professional Services engagement)
- 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
- DNAC Site Design
- Configuration of Applications and Application Policies - such as for Stealthwatch, Umbrella, App Hosting, Application Visibility or other additional DNAC Apps. Only basic setup and DNAC connectivity to these apps will be implemented as part of this Managed Service. See relevant Applications section (e.g. Stealthwatch) for full details of supported Application tasks.
- Roles Based Access Control (RBAC) policy definition for client DNAC access: This is a consultancy task which must be contracted in addition to the Service

Ongoing Cisco DNAC Device Management

Cisco DNAC Management Portal and Appliance

Cisco DNAC-enabled physical and virtual devices are managed via the Cisco DNA Center platform, which acts as a centralized control plane. The Cisco DNA Center platform controls all endpoints, providing centralized functions like automated Golden Image deployment and updates, de-commissioning, single screen administration, reporting, monitoring and alerting.

NTT will manage the DNA Center Portal for the devices included in the solution as explained in this section, including the following activities:

- *Application Policy Updates for Intent-based Networking (Including Creation of Applications and Application Sets)*
- *Management of Golden Images and SMUs (Software Maintenance Updates) - Including Importing Images, Distributing and Activating Images to and on devices.*
- *Configuration/Golden Image Monitoring and Compliance Reporting*
- *Proactive Upgrades to Images (within client-defined standard Change Request process)*
- *New Image Notifications*
- *Configuration Management and Remediation*
- *Configuration of out-of-the-box Cisco DNA Center appliance reports to be sent to the Client*
- *Configuration of monitoring information as per Client needs and DNA Center capabilities*
- *Troubleshooting and issue reproduction with DNA Center time travel alongside DNA and NTT correlation and Root Cause Analysis (RCA) tooling.*
- Enable and Configure Synchronisation of DNA Center with Cisco ISE
- Establish Cisco Integrated Management Controller (IMC) Connectivity to support System Health reports.
- Licenses and contracted subscriptions configuration

Specific Tasks Not Included with DNA Center Management

- End User support, or
- Optimization and Recommendations of Images
- Proactive Vulnerability Monitoring, Vulnerability Reporting, Support and Recommendations/Remediation
- Update Planning
- Software Image change Impact Analysis
- Management of Images if stored in an external repository (only DNAC native SWIM storage supported).
- Creation of Images for Deployment
- Configuration Change Impact Analysis

DNAC Specific Monitors

The following monitors are configured by default (DNAC Event Notifications will be configured to support monitoring in NTT Tools):

Monitor	Description	Alerts	Performance Info	Resolution

Cisco DNAC Devices	Health scores for Cisco DNAC devices		Health scores of CPU, memory, interface, and reachability scores as well as issue counts.
			
			Specifically these scores incorporate
			• System Resources (memory utilization and CPU utilization)
			• Data Plane (uplink availability and link errors)
			• Control Plane (reachability).
			• Wireless
			  ○ Radio Utilization
			  ○ Interference
			  ○ RF Noise
			• Wireless Controllers
			  ○ Free Memory Buffers (MBufs)
			  ○ Work Queue
			  ○ Packet Pools
			  ○ Link Errors
				Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed

Sensitivity Label: General

Monitor	Description	Alerts	Performance Info	Resolution
Cisco DNAC Clients	Health scores for Cisco DNAC clients	✓	Overall client health information by client type (wired and wireless) as well as client counts.	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed
Cisco DNAC Networks	Health scores for Cisco DNAC networks by category including device counts by condition.	✓	Health Score By Network	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed
Cisco DNAC Issues	List of global issues, issues for a specific device, or issue for a specific client device's MAC address.	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed
Disk (if any)	Disk usage in %	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed
Interfaces	Status of device interfaces (virtual or physical), Connection status, client count, sent / received packets and bytes, errors, throughput	✓	N/A	Engineering Teams will solve the issue
Sessions	Check the number of current/active sessions in the device	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed
Device Status & Operational State	Operational status of the device	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed
HA Status (if any)	Check the status of High Availability	✓	N/A	Engineering Teams will solve the issue
Certificates	Monitoring of SSL certificate expiry	✓		Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed

Service Requests

DNAC controls a large variety of devices and therefore includes several technologies. As part of the Service, the fulfilment of the tasks listed in the table below are included. For information about additional supported service requests, refer to the associated Switch, Router and Wireless LAN Controller Technical Service Descriptions.

Digital Network Architecture Center Service Requests

Task	Description	Included
User, Authentication and Role Management		
Create, Edit and Delete DNAC Internal User Profiles	A user profile defines a user's login, password, and role (permissions). You can configure both internal and external profiles for users. Internal user profiles reside in Cisco DNA Center and external user profiles reside on an external AAA server.	✓
Create and Update Roles	Cisco DNA Center supports role-based access control (RBAC), which enables a user with SUPER-ADMIN-ROLE privileges to define custom	✓

Sensitivity Label: General

Task	Description	Included
	roles that permit or restrict user access to certain Cisco DNA Center functions.	
Enable and Configure 2FA (2 Factor Authentication)	The Cisco DNA Center implementation of two-factor authentication supports the use of a token client (that generates single-use token codes after the appropriate PIN is entered), a token server (that validates token codes), and an authentication server to manage user access. Authentication can be handled using either the RADIUS or TACACS+ protocol.	✓
Perform Password Resets		✓
Establish, Update or Remove DNA Center integration with Cisco ISE	If using external server for authentication and authorization of external users, external authentication in Cisco DNA Center is required	✓
Configure External Authentication		✓
Update Account Lockout Settings	Configure the account lockout policy to manage user login attempts, the account lockout period, and the number of login retries.	✓
Update Password Expiry Settings	Configure the password expiration policy to manage the password expiration frequency, the number of days that users are notified before their password expires, and the grace period.	✓
DNAC System Configuration		
Enable Data Anonymisation		✓
Cisco DNAC Authentication & Policy Server Configuration	Additions, changes to, or removal of AAA servers for user authentication. (NOTE: If Cisco ISE is used to perform both policy and AAA functions, please see MCN - Managed Cisco Identity Services Engine (ISE) Description V1.0.0 DRAFT	✓
Configuration of an external IP Address Manager (IPAM) service	Additions, changes to, or removal of an IPAM service into Cisco DNA Center, if Cisco ISE is not used.	✓
Configure Cisco AI Network Analytics Data Collection	Enabling or disabling Cisco AI network analytics data collection from wireless controllers as well as site hierarchy to the Cisco DNAC appliance.	✓
Cisco Machine Reasoning Knowledge Base Updates	Configuration of automatic updates to Machine Reasoning Engine (MRE) knowledge packs, or triggering of a manual update to the MRE knowledge pack.	✓
Certificate management	• Renew Certificates within DNAC, Includes changing role of certificates and Certificates Lifetimes • Addition, removal and modification of SSL certificates associated to the device and services	✓
Establish or Update Cisco Integrated Management Controller (IMC) Connectivity to support System Health reports.	IMC is required for DNAC System Health Reports against each DNAC Controller	✓
Create and Manage DNAC Sites	• Create and manage sites, assign devices to sites, obtain site information, site count, and site membership. • Sites are hierarchical collections of other sites and 'buildings'.	✓
Create and Manage DNAC Fabric Networks	• A fabric network is a logical group of devices that is managed as a single entity in one or multiple locations. • Having a fabric network in place enables several capabilities, such as the creation of virtual networks and user and device groups, and advanced reporting.	✓

Sensitivity Label: General

Task	Description	Included
	• Other capabilities include intelligent services for application recognition, traffic analytics, traffic prioritization, and steering for optimum performance and operational effectiveness.	
Cloud Access Key configuration	Addition or removal of cloud access keys as part of the cloud device provisioning application package in Cisco DNA Center (supported for AWS only)	✓
Changes to Device Controllability	Enabling or disabling device controllability via Cisco DNA Center (that is enabling or disabling centralized control of network infrastructure for network devices)	✓
Configuration of additional logging	Configuration of additional device and audit logs, and pushing of logs to a client provided log target (syslog server, SIEM platform).	✓
License Management		
Change DNA License Levels	Change the level of Cisco DNA Center licenses to Essential or Advantage	✓
Register/Deregister Device Licenses and License Reservations for DNAC		✓
Export License Information for Review	Export of license information from a Cisco DNA Center environment for client reporting or audit purposes. License information will be exported in PDF or Microsoft Excel format.	✓
Change Device Throughput for Smart License-enabled routers		✓
Transfer Licenses between Virtual Accounts		✓
Modify License Policy	You can modify the reporting interval at which the network devices will report their feature usage to CSSM.	✓
Backup, Restore and HA		
Management of failover	Only in HA or clustering configurations: management of failover policy to allow the service to continue working if a device error occurs	✓
Management of disk space	Evaluation and study of actions for freeing and optimising disk space (if disk is present in the device). This doesn't include backup servers or other devices not managed by NTT.	✓
Bandwidth Management and connectivity features	• This is per the underlying capabilities of the DNAC devices as described in the relevant Device-specific Technical Service Descriptions.	✓
Forward logs to an external SIEM service	Changes in the settings to forward logs to an external SIEM and SOC solution, destination, port, and/or information being sent	✓
Forward logs to a managed log management service	Changes in the settings to forward logs to an associated (and managed) log management system.	✓

Configuration Management - Backup and Restore

An integral part of the Service is the management of the backup policy. The following tasks are included as part of Cisco DNAC Device Management:

Task	Description
Configuration Backup Policy implementation	When the Service is initially delivered, a configuration backup policy will be implemented to backup only the automation data

Automation data consists of Cisco DNA Center databases, credentials, file systems, and files. The automation backup is a full backup performed weekly.
Configuration backup excludes backing up of assurance data which consists of network assurance and analytics data.

To support automation data backup, the backup server must support SSH or rsync. Recommended disk space for automation data backup is 180GB for large deployments.
This needs to be evaluated based on the DNAC appliance type and the number of devices managed.
Backup and Restore between versions of DNA Center is not supported - this is a DNAC limitation.

Unless specified in the Statement of Work, the Client is responsible for providing suitable infrastructure to facilitate backup and restore activity.
For details of backup and restore, consult MCN Managed Configuration Backup Service Description.

Cisco DNAC-supported Switches

Cisco DNAC switches provide wired switching functionality in Cisco DNAC controlled networks.

Supported Switches

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

Supported Configurations

- Single switch: A standalone switch or a set of standalone switches (managed independently from each other)
- Set of switches in high availability configuration: Two or more switches of compatible models in an HA configuration

Specific Tasks Associated with Installation of a Switch

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

- Creation of VLANs
- Creation and configuration of spanning tree
- *In stack environments* : service clustering

Switch Specific Monitors

The additional monitors which can be configured for switch management are:

Monitor	Description	Alerts	Performance Info	Resolution
Uplink Port Status	Check port status	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed
Uplink Port Usage	Check uplink port bandwidth usage	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed

Switch Service Requests

Task	Description	Included
Creation and management of VLANs	Creation, change and deletion of VLANs configured in the device and its nodes	✓
Management of spanning tree	Management of the spanning tree protocol to handle link redundancy	✓
Management of port channel / ether channel	Creation, change and removal of port channel interfaces	✓

All of the above tasks will be performed according to the Change Management process

Cisco DNAC-supported Routers

Monitors

The following monitors can be configured by default:

Monitor	Description	Alerts	Performance Info	Resolution
Interface Status	Check interface's status	✓	N/A	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client if needed
Interface Usage (1)	Check interface's bandwidth usage	✗	Graphs for the parameter measured over time	N/A
VPN (2)	VPN up or down	✓	N/A	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client if needed

Sensitivity Label: General

(1) Only monitoring, no alerting
(2) Only supported if both VPN endpoints are managed by NTT (additional charges may apply)

Router Service Requests

Task	Description	Included
Creation and management of routes	Creation, change and deletion of routes configured in the device and its nodes	✓
Management of dynamic and static routing protocols	Creation, change and deletion of BGP, OSPF, EIGRP static table entries	✓
Creation and management of VLANs and or interfaces	Creation, change and deletion of VLANs / interfaces configured in the device	✓
Creation and management of VPNs (site-to-site)	Creation, change and deletion of VPNs in the device. Connection to and configuration of the remote is excluded.	✓
Creation and management of NAT's	Creation, change and deletion of NATs in the device	✓
Management of policy-based routing (PBR)	Creation and management of policies for PBR	✓
Management of port channel / ether channel	Creation, management and configuration of ether channels	✓
Management of VRF policies	Creation, change and deletion of the VRF's in the device	✓

Supported Routers
A listing of supported Router models and their respective sizing can be viewed in the DNAC Supported Technologies section.

Supported Configurations
The following configurations are supported:
- Single router: A standalone router
- Set of routers for high availability: Two or more routers with high availability configurations using HSRP/GLBP/VRRP or dynamic routing protocols (BGP, OSPF, EIGRP, etc.)

Supported Environments
The following environments are supported:
- Client premises
- Colocation data centre

Limitations
The following limitations apply:
- 2x VRF (Virtual Router Forwarding) policies are included in the standard set up and management fees

Cisco DNAC Wireless Controllers and Access Points (Including IOT variants)
Cisco DNAC-enabled Wireless infrastructure provides the cloud based control plane, as well as wireless Access Points (AP's) that form part of a Cisco DNAC network.

Supported Configurations
- Cisco DNAC-enabled APs will only be managed from the DNA Center Appliance.

Specific Tasks Associated with Installation
As part of the Service, the following tasks are included in the setup fee:
- Creation of SSID's, VLANs and WLANs
- Creation and configuration of new wireless networks
- Creation and configuration of security policies
- Addition of APs to networks
- Connection to external user directory or database
- *In HA environments* : Service clustering

Specific Tasks Not Included with Installation
- End User support, or
- Management of the AP's if these AP's are not in-scope

Wireless Controller Specific Monitors
The additional monitors which can be configured for Wireless Controller management are:

Sensitivity Label: General

Monitor	Description	Alerts	Performance Info	Resolution
Availability	Device is available	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed
Uplink Port Usage	Check port's bandwidth usage	✗	Graphs of the parameter measured over time	N/A
Port Errors	Existence of a problem or error in a port	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed
AP Radios	Monitors AP radio performance metrics	✗	Graphs of the parameter measured over time	
High Availability	Monitoring wireless controller high availability (if deployed)	✓		Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed
Authentication and Authorisation	Monitors RADIUS accounting server, and authentication servers status and configurations	✓		Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed

Supported Wireless Devices

A listing of supported Wireless Access Point models and their respective sizing can be viewed in the DNAC Supported Technologies section.

Cisco Identity Services Engine (ISE)

The service associated with Cisco ISE is described in the MCN - Managed Cisco Identity Services Engine (ISE) Service Description documentation.

Cisco DNA-supported Security and Routing Appliances

Cisco ASA and Firepower appliances provide managed security and routing functionality.

Supported Security Appliances

A listing of supported Routing and Security appliance models and their respective sizing can be viewed in the DNAC Supported Technologies section.

Supported Configurations

- Cisco physical or virtual appliances
- Single devices
- HA security appliance configurations - 2 compatible physical or virtual security appliances in an active / passive configuration, both connected at the same time

Tasks Associated with Installation

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

- Registration of the device to Cisco DNA Center
- Creation of DNA Policies and Default Access Rules for Users/Devices/Applications Access
- Enable and Configure Synchronisation of DNA Center with Cisco ISE
- Establish Cisco Integrated Management Controller (IMC) Connectivity to support System Health reports.
- Subscribe to System Event Notifications
- In HA environments, setup of HA services
- Initial licenses and contracted subscriptions configuration
- Install SSL keys/certificates associated to protected sites for the advanced services that need them
- Configuration of error pages and error page groups
- Configuration of Web Filtering, URL Content Filtering and WebCaching
- Configuration of Intrusion Detection Services
- Configuration of Geo-based security
- Configuration of Intrusion Prevention Service
- Configuration of log relaying and other log management mechanisms if contracted

Routing & Connectivity Related Tasks:

- Routing configuration in the DNA Center Portal.
- Dual uplink port configuration
- LTE failover configuration
- Configuration of Intelligent Path Control policies
- Configuration of Branch Routing (route redistribution) policies

- Modification of existing Traffic shaping, Bandwidth Management and Quality of Service configuration

Optional Tasks

The following tasks may be provided at additional charge, unless specified in the Statement of Work:

- Security policy definition: this is a consultancy task which must be contracted in addition to the Service
- Analysis of the Clients applications, consultancy, audits and advisory services are not included in the setup fee
- SIEM and SOC services
- Hardware, Software and/or support around it

Security Appliance Specific Monitors

The following monitors are configured by default:

Monitor	Description	Alerts	Performance Info	Resolution
Disk (if any)	Disk usage in %	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed
Interfaces	Status of device interfaces (virtual or physical), Connection status, client count, sent / received packets and bytes, errors, throughput	✓	N/A	Engineering Teams will solve the issue
Sessions	Check the number of current/active sessions in the device	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed
Device Status & Operational State	Operational status of the device	✓	N/A	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed
HA Status (if any)	Check the status of High Availability	✓	N/A	Engineering Teams will solve the issue

Client Requirements for Managed Cisco Security Services

As a general approach, the following will happen when a IDS/IPS device starts its managed service:

- The installation process will configure all the policies as desired by the Client
- This will generate a huge number of false positives, so on the first days of the Service the security policy should be loosened
- Additional rules are added little by little to strengthen the security policy
- This will eliminate false positives and provide a more secure environment for the Client's applications; and
- Once stabilised, no more changes would be required until new versions of the Client's applications are released and deployed. At that moment, the process can start again.

Because of the above expected results, it is important that the starting point of the firewall policy operation counts with the relevant Client contacts to adapt the firewall policy to the Client's applications. This activity is not something the engineers managing the devices will do. In the case of issues once the policy has been activated, the only expected outcome from the engineers will be complete deactivation of the policy or (if possible) changing the policy from "Block" to "Alert", "Log" or whatever non-blocking option is available. 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 Client application.

Requests Not Included with the Service

IDS / IPS

IDS 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 Client's relevant contacts. The scope of the managed IDS and advanced security features will be limited to applying changes based on what the Client requests. NTT expects the Client will identify the changes to perform based on the SIEM (or whatever the log management tool the Client uses). On the SIEM, the reason why applications are blocked generating false positives, or not blocked when these should, would be identified by the Client. As part of the ongoing management of an Advanced Security device, it is not included in the review of all the logs for an unidentified error or false positive. 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 Client application.

SIEM Services

A SIEM independent log management system or SOC threat analyst team is not included as part of the Cisco DNAC Management Service. This means that the detection of vulnerabilities, threats and similar security activities are limited to the features included in the devices under management and that NTT will not include additional tooling. As such, the following is not part of the Service unless additionally contracted:

Sensitivity Label: General

- Log Management Service
- Log Correlation Service
- Threat Correlation, Collaborative Intelligence, Monitoring and Analysis of Logs with SOC analysts to detect and/or investigate alerts

All of the above tasks will be performed according to the Change Management process defined in the *MCN Statement of Work*.

Cisco Stealthwatch

Cisco Cisco Stealthwatch Service Requests

Task	Description	Included
Install Stealthwatch Security Analytics	Install the Basic Stealthwatch Package in DNAC	✓
Register Stealthwatch		✓
Enable Stealthwatch Analytics		✓
Set Up the User Datagram Protocol Director		✓
Configuration of DNAC events related to Stealthwatch		✓

Limitations

The following limitations apply:

- Stealthwatch will only be deployed to devices per specific instructions from the client. NTT will not create policies or deploy to devices unless given specific instructions by client or representative of client.
- Stealthwatch will only be monitored in terms of DNAC-enabled and API-visible Events.

Cisco Umbrella

Cisco Umbrella Service Requests

Task	Description	Included
Install the Basic DNAC Umbrella Package	Installation of Umbrella package within DNA Center.	✓
Configure DNAC with client provided accounts and keys to connect to Umbrella	Includes Configuration within DNAC of Umbrella Accounts, API Keys, Legacy tokens management keys, secrets, organisation Ids and local bypass domains.	✓
Add Umbrella Dashlets in DNAC (System 360)	The Umbrella dashlet shows the configuration status of Cisco Umbrella with Cisco DNA Center.	✓

Limitations

The following limitations apply:

- Umbrella will only be deployed to devices per specific instructions from the client. NTT will not create policies or deploy Umbrella to devices unless given specific instructions by client or representative of client.
- Umbrella will only be monitored in terms of DNAC-enabled and API-visible Events.

Cisco DNA Spaces

Cisco DNA Spaces Service Requests

Task	Description	Included
Configure DNA Spaces Integration with DNA Center	Registering DNA Spaces cluster with Cisco DNA Spaces; Assign Cisco DNA Spaces to Cisco DNA Center Sites. **Note:** The Cisco DNA Center and Cisco DNA Spaces integration is currently limited to only automatic map exports and synchronization for the location hierarchy. The integration does not support captive portal-based authentication features.	✓

Limitations

The following limitations apply:

- DNA spaces will only be configured per specific instructions from the client. NTT will not design or create policies/behaviour metrics/camera metrics, tags or asset locators or register devices unless given specific

instructions by client or representative of client. There are also limitations of the DNA Spaces integration with DNA Center as above.
- DNA Spaces will only be monitored in terms of DNAC-enabled and API-visible Events.

Cisco ThousandEyes

Cisco ThousandEyes can be installed to a subset of Cisco Devices (such as the Catalyst 9000 series with a minimum IOS XE version) via Cisco DNA Center. ThousandEyes is supported through Image deployment with the ThousandEyes Enterprise Agent - but configuration of ThousandEyes itself is not supported.

Cisco ThousandEyes Service Requests

Task	Description	Included
Deploy ThousandEyes-created Images - typically .TAR files (including the ThousandEyes Enterprise Agent) to Devices via DNA Center	This is using the default DNAC image management and deployment capabilities.	✓

Limitations

The following limitations apply:
- ThousandEyes will only be configured per specific instructions from the client. NTT will not design or create policies or register devices unless given specific instructions by client or representative of client.
- Docker Runtime options for ThousandEyes Docker/KVM images will be used as default.
- ThousandEyes Agents will **not** be monitored as part of this managed service.

Sensitivity Label: General