



Service Specification

FORTINET SD WAN Managed Service



Contents

Table of Contents

Managed Service Overview.....	3
Definitions	4
Service Overview	4
Service Hours	5
Responsibilities	5
Service / Change Request Management	7
Standard change types	8
Service Request Points Entitlement Overview.....	9
Service Reporting.....	10
Customer Responsibilities	10
Exclusions.....	10
Dependencies	11

Managed Service Overview

This Managed Service consists of the following set of high-level capabilities that can be used to build a full end to end SD-WAN managed service.

Standard Run Services:

Proactive Monitoring – This provides monitoring that is required to provide the customer with a proactively managed service. It incorporates the 2nd and 3rd line desks who are used to solve any incident management issues that cannot be solved at the 1st line desk.

Performance Reporting – this relates to levels of network performance reporting and application performance reporting which are available to all customers.

Service Reporting – A monthly service report will be provided to customers.

Capacity Management – provides reports and commentary on the customer's network capacity.

Availability Management – provides reports and commentary on the availability of the customer's network.

The following services are optional but recommended to enhance your service experience:

Service Management – a service manager will work on behalf of the customer and will provide a review of the customer's service and performance reporting.

Service Desk – this provides the customer with a 1st line service desk as contact for any customer incident management.

Supply and provision of the circuit underlay using either DIA Ethernet circuits or Subscriber Broadband services.

Break fix Maintenance – this relates to SD-WAN appliances and SCC provided CPE devices where applicable and provides several maintenance care level options.

Hardware Asset Management – A comprehensive Hardware Asset Management Service covering 4 areas:

- Transition Phase – Data Validation & Load
- Asset Inventory Management
- Reporting
- Monthly Audit

As part of the Hardware Asset Management Managed offering SCC shall provide an administrative Asset Management operating model for Network Devices in the scope of SCC management with additional reporting and Auditing to provide increased levels of governance and control.

Change Management – this provides the customer with the ability to raise a Service Request for a set of pre-defined noncontract affecting configuration changes.

Optional Deployment Services

Packaged Deployment Services - provides a project managed installation service including a range of project management levels to choose from, as well as a commissioning and installation service.

Professional Services – provides either a pre-defined packaged service or can be bought as a one-off or on a call-off or day-rate consultancy charge.

Site IMAC– this provides the customer with the ability to invoke a contractual change (such as delivery of a new site).

These services are all available under a single contract and a single bill across all the technical solutions to which the set of Managed Services apply.

Definitions

The following expressions will have the following meanings unless inconsistent with the context:

SD-WAN	Software Defined – Wide Area Network
WAN	Wide Area Network
DIA	Direct Internet Access
MPLS	Multiprotocol Label Switching A routing technique that directs data from one node to the next based on short path labels
Broadband	A wide bandwidth data transmission method which uses a wide range of frequencies and Internet traffic types, used in fast internet connections
Underlay	The transport layer that the SD-WAN utilises. This includes MPLS, Internet (DIA), Subscriber Broadband and 4G mobile data.
SSE	Secure Service Edge

Service Overview

A Software-defined Wide Area Network (SD-WAN) is a virtual WAN architecture that works through a centralised platform, detaching the management of the network from the hardware itself which allows customers to leverage any combination of underlying transport services – including DIA, MPLS, LTE and Broadband Internet services, to securely connect users to applications. SD-WAN enables a secure local Internet breakout of IaaS and SaaS application traffic from a user's location providing the highest levels of management and performance while protecting the customer's network from security threats. The SD-WAN service uses a centralised control function, to securely and intelligently direct traffic across the circuit underlay. The management infrastructure can either be hosted in SCC's own Data Centres or the Customers own hosting environment or a Public Cloud.

The SCC SD-WAN Managed Service offers a set of standardised support services across the range of FortiGate networking appliances. These services utilise the capabilities of Forti manager software providing the centralised provisioning capabilities into a customers managed SD-WAN, centralised policy deployment, firmware and feature upgrades, network visibility and pro-active remote troubleshooting to deployments of any size, also centralised logging capabilities using a powerful log

management, analytics, and reporting platform using a single console to manage, automate, orchestrate, and respond. SCC's Fortinet certified managed service resources will operate this environment.

The standard technologies covered under this Service are as follows:

- Managed SD-WAN (Fortinet Fortigate Firewalls, FortiGuard Support Bundle, includes UTM license and 24x7 FortiCare and Unified Threat Protection)

Service Hours

24 x 7 x 365

Responsibilities

The following table defines the responsibilities of SCC within the scope of this Service. Please note certain Customer Responsibilities identified within this Service description may be superseded either in part or entirely by SCC as part of other SCC Services that the Customer has contracted for under this Agreement.

Feature	SCC Activities
SD-WAN Support & Administration	SCC will Identify and resolve Incidents relating to the pre-agreed scope of SD WAN Managed infrastructure as detailed in the Technical Specification.
	SCC will implement firmware upgrades for all the managed Fortigate appliances and management platform where required for Incident Resolution.
	For service impacting faults that are identified as a P1 by the SCC Operations team, perform out of hours resolution.
	Where SCC determine it is appropriate as part of Incident Resolution apply any appropriate firmware upgrades or configuration restores for Service restoration.
	If a critical error cannot be resolved by SCC using the normal support tools and processes, the problem may require escalation to Fortinet. SCC will manage the escalation and resulting outcome.
Underlay circuit support	SCC will monitor the WAN interface of the Fortigate Equipment for availability. In the event of any changes of state to the interface an alert will be generated and investigated.
	SCC will investigate and triage alerts reporting an issue with an Underlay circuit used by the managed SD-WAN
	Log an incident with the third-party circuit provider to investigate and resolve. Regularly check with the third-party circuit provider the resolution status of the incident.
Event and Alert	Proactive device monitoring of the Fortigate hardware under the scope of this Service via the SCC Fortimanager platform.

Management	Notify the Customer when allocated capacity is approaching limits and there is a risk of service performance degradation.
	Take action to investigate and remediate a reported degradation of SD WAN performance beyond agreed Customer thresholds.
	Make proactive recommendations to prevent possible service degradation of the SD-WAN performance beyond agreed Customer thresholds.
	Action changes to monitoring thresholds or alerts raised as a Service Request.
Capacity and Availability Reporting	If implemented, ensure the customer's read only access to the Forti manager dashboard access is maintained.
	As part of the Service reporting provide availability, performance, uptime, and capacity reporting for the SD WAN Managed infrastructure as detailed in the Technical Specification.
	Provide a high-level overview of total traffic across all devices monitored and managed as part of the SD WAN Service as detailed in the Technical Specification over an agreed period.
	A Customer has access to run their own capacity and availability reports.
License management	Report quarterly on the licensing status of the SD WAN and compliance within the management portal. Where Fortigate licenses are included as part of the Service Charges, SCC will maintain license compliance for the term of the Order. When the Customer is responsible for the procurement of Fortigate licenses SCC will report license term end dates to the Customer 60 days before they expire.
SD-WAN & traffic shaping	SCC will manage Customer requested updates or changes to the SD WAN infrastructure in scope of the managed service. This includes and is limited to the following features: • SD WAN policies • Traffic shaping rules • Flow preferences • IP circuit SLA's • WAN traffic load balancing • Advanced routing • Security policies Where applicable updates will be applied on a per application basis.
UTM Security Features	SCC will manage Customer requested updates or changes to the Security functionality in scope of the managed service. This includes and is limited to the following available features under the Fortigate UTM license: • Enterprise Firewall • application control • advanced persistent threat protection, Web and content filtering • IP reputation • integrated WLAN controller • Web and Content Filter • DNS Filter • Application Control • Intrusion Prevention • Application Signatures

	• IPS Signatures • WebRatings and override • Web Profile overrides
Device software update	If required SCC will perform mandatory device upgrades to ensure system security, stability, mitigating vulnerabilities and compatibility with the SCC monitoring and management platforms. A bi-annual assessment is performed of the software and firmware version to ensure full system stability is maintained of the managed Fortinet SD-WAN appliances, SCC may recommend that the latest stable Operating System or feature updates be applied to all managed Fortigate devices specified in the Technical Specification. The recommended updates for each bi-annual assessment will be applied on no more than three separate dates / times of the Customer's choosing over a three-week period. These updates will be managed by SCC in accordance with the Customers Change management processes. Supported Equipment that fails after an upgrade will be resolved in accordance with the terms of the Equipment Maintenance Service.
Active Directory	For those Customers with integration configured between their on-premises Active Directory and the SCC SD-WAN management platform for the purpose of supporting Administration user authentication to the management platform, SCC will support the trouble shooting of Active Directory authentication issue in relation to those accounts only.
Fortimanager software Updates	If required SCC will perform mandatory software upgrades to ensure system stability, security and compatibility with the SCC monitoring and management platforms. A bi-annual assessment is performed on the FortiManager software version to ensure full system security and stability is maintained; SCC may recommend that the latest stable firmware upgrades be applied to the Fortimanager Appliance specified in the Technical Specification. Any update will have to be compatible with the firmware release running on the SD-WAN Firewall appliances. The update will be managed by SCC in accordance with the Customers Change management processes.
Fortianalyser software Updates	If required SCC will perform mandatory software upgrades to ensure system stability, security and compatibility with the SCC monitoring and management platforms.
Configuration Change Requests	All policy and template configuration changes to SD WAN service may be requested through the Service Desk. Design changes or changes that require architectural assistance are required to be raised as projects due to risk and effort and will be subject to additional Charges.

Service / Change Request Management

Detail on how to make requests is provided in your Operations Manual.

Requests specific to this Service, include, but are not limited to the following, and should be logged as a Service Request through the SCC Service Desk:

- Additional reporting, and
- All Service Request Catalogue items.

If you require any changes or additions to any of the above, your requests will be reviewed by us and confirmed with you. Following agreement by both Parties, we will implement all configuration changes agreed upon with you via the Change Request procedure. If the changes required are deemed to be significant changes to the Service or require a professional services engagement due to your bespoke or detailed requirements, additional Charges will be discussed with you before any change is implemented and applied at our prevailing rates or as otherwise agreed with you in your applicable Service Request.

Within the SCC Vision Services Hub Portal, you can view:

- 24/7 any requests you raise and their detail.
- the list of possible Service Requests (“Service Request Catalogue”); and
- Your available and consumed Service Request Points.

Standard change types

Category	Service Request	Points
General	Add/remove device or term licenses.	1
	Add/remove read only Administrator accounts.	1
Monitoring and reporting	Add/remove/modify alerts	1
	Change alert destination email address or resolver group	1
	Add a new bespoke report to the standard monthly reporting pack	3
	Add/remove a device from the SCC monitoring service.	1
	Perform a SD-WAN service device discovery.	3
Security – Firewall	Add/remove/modify the enablement and/or denial of relevant UTM features	3
	Add/remove/modify Firewall rules for applications through layer 3,4 and 7	3
	Add/remove/modify geo-IP based firewall rules (enabling source country rules)	3
	Add/remove/modify port forwarding rules	3
	Add/remove/modify 1:1 NAT forwarding rules	3
Security - Appliance Features	Addressing and VLANs	3
	Add/remove/modify traffic shaping	3
	DHCP	5
	Firewall policies	1
	Add an additional site SD-WAN VPN	5
	Configure Site to Site VPNs	5
	Additional configuration to the SD-WAN hubs	5
	Add/change Threat Protection rule	5

	Make a single change to Access Control	3
Security – content and security filtering*	Add/remove/modify content filtering (add and amend blocked website categories)	1
	Add/remove/modify URL whitelisting	1
	Add/remove/modify URL blacklisting	1
	Add/remove/modify HTTPS filtering	1
	Add/remove/modify assignment of device or user to an existing group policy	1
	Add/remove/modify security filtering	3
	Add/remove/modify Advanced Malware Protection	3

* The following indicative features are subject to change following changes to firmware upgrades and are accurate as of the published date of this service description

Complex Design changes that require architectural assistance or changes which fall outside the scope of Service Description will be raised as projects due to risk and effort required to implement. These requests will be assessed and if implemented will be charged in addition to the charges for this Service.

- Complex design changes include but are not limited to:
- Redesign of the SD-WAN service network architecture
- Adding a new hub site and configuring routing policies
- Integrating of the SD-WAN Service with a new Public Cloud site
- Integration of the SD-WAN Service with a new Data centre

Less complex changes, small works requests will be assessed and if implemented will be charged in addition to the charges for this Service.

- Installing a new site on to the SD-WAN
- Decommission an SD-WAN site.

Service Request Points Entitlement Overview

A Customer accrues Service Request points based on their total managed services spend, excluding Public Cloud and one-off charges.

For every £1000 of spend this entitles the customer to 5 points per month of Service Request spend.

New points are allocated from the service commencement date and reset every 30 days thereafter until the end of the contract term. If any of the monthly points entitlement is not used during each 30-day cycle, the remain balanced is wiped and will not be carried over.

In the event that the monthly balance of Service Request points is fully consumed, and the Customer requires further changes to be made before the next 30 day allocation of points an On-Demand change will have to be raised which is charged at the prevailing hourly rate published on the SCC Services Portal, Vision.

Service Reporting

SCC will provide any reporting included as part of the Service within 2 weeks of the end of the relevant reporting period, where this falls on a non-Working Day then the required reports will be provided by the next Working Day.

Report Type	Frequency
Monitoring Reports	Monthly
Capacity & Availability Reports	Monthly / Ad hoc

Customer Responsibilities

- The Customer is responsible for ensuring End Users raise Service Requests and Incidents to SCC's Service desk in accordance with the processes detailed in that Service Description
- Participation in change control process as required due to any actions arising as result of Event & Alert Management.
- A default threshold of 70% of capacity will be put in place unless specific measures, alerts and corresponding remedial actions are advised and provided by the Customer.
- Where changes to monitoring thresholds or alerts are required raise these through the Service Desk as a Service Request.
- Where the Service Underlay is not supplied by SCC, the Customer is required to provide details of where the Customer end of each circuit terminated (including postcode).
- Where the Service Underlay is not supplied by SCC, the Customer is responsible for configuring their end of each circuit and associated equipment forming the Underlay.
- Raise all changes to reports via the SCC Service Desk.
- Agree a schedule for service unavailability (maintenance windows) to allow critical maintenance to take place.
- Ensure the SD WAN Network device hosting locations and environment must meet the recommendations of the vendor for any remote locations not under SCC's control.
- Maintain and support the cabling infrastructure for any remote locations not under SCC's control.

Exclusions

- Support, Integration or Management of a Customer's Active Directory unless taken as part of another Service.
- Provision and Management of any Underlay, leased lines, network connectivity required for this Service to operate unless provided by SCC as part of another service.
- Remediation activities by SCC, required because of degradation or failure of the Equipment or Hardware by parties other than SCC are excluded and shall be subject to additional Charges from SCC.
- Provision of Hardware required to operate this service.

- Installation of Major feature releases of firmware or operating systems upgrades are deemed as a project activity and chargeable. For example: Version 10 to 11.
- The design and implementation of new or additional features, additional capacity, configuration of new devices will chargeable project activity
- SCC will not be responsible for any changes that the vendor makes to available features and the associated charges that may occur when these are enabled.
- The following security features are not included as part of the managed service:
 - Anti-virus
 - SSL/SSH Inspection
 - Video Filter
 - File Filter

Dependencies

- Incident Management, Major Incident, Problem, Change Management and Hardware Maintenance services (unless Customer provided and managed), Governance (SDM), DCS Critical Desk if no other SCC Service Desk is part of the customer service wrap.
- A physical Underlay is required either Customer provided service provision or an SCC Underlay service.

