Managed Fortinet Edge Technology Service Description

Overview

This document provides information relating to the management and monitoring of Fortinet Edge technology under the standard MCN offering. The monitoring, configuration, limitations, and available standard service requests are outlined hereunder. The MCN Fortinet Edge offering includes:

- Fortinet Security devices including
  - Fortigate E-series and F-series hardware appliances.
  - Fortigate virtual appliances
  - Fortigate appliances on Public Cloud (AWS, Azure, Google)
- FortiManager
- FortiAnalyzer
- FortiSwitch Ethernet Switches
- FortiAP
- FortiAuthenticator
- FortiSD-WAN
- FortiExtender
- FortiWeb

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

Client Responsibilities and Pre-requisites

There are no technology specific pre-requisites required, however, a description of the standard pre-requisites for the offering are documented in the MCN Statement of Work.

Fortinet Security Appliances

Technology Specific Operations

Fortinet Specific Monitors

The following technology specific monitors can be configured by default.

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Hardware Health	Monitors FortiGate appliance sensor readings and alarm status	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware maintenance provider as required	180
SSL VPN Stats	Monitors SSL VPN statistics by VDOM	✗	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client as required.	180
WAN Links	Monitors FortiGate WAN link load balancing link state and performance including throughput, loss, latency, jitter	✗	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client as required.	120

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Link Monitor	Monitors the VDOM interface link health and performance	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware maintenance provider as required	180
IPSEC VPN Stats	Monitors status and throughput metrics of individual IPSEC VPN tunnels	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware maintenance provider as required	180
Interfaces	Monitors the FortiGate device interfaces status and performance metrics including SD-WAN interfaces.	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client as required.	120
High Availability	Monitors FortiGate appliance high availability, including status, peer performance metrics	✓	N/A	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client as required.	60
VDOM Monitoring	Monitor the FortiGate VDOM State & utilization	✗	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client as required.	120
Session	Monitor the active sessions	✗	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client as required.	120
FortiGuard Update	Monitor the FortiGuard update statistics	✗	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client as required.	300
Fortigate License	Monitor the license status	✓	N/A	Engineering team notify to customer/SDM.	180

Configuration Management

Device configuration backups are included in the standard offering and are described in more detail in the MCN Managed Configuration Backup Service Description

Firmware Maintenance

There are no specific requirements for firmware maintenance of the technology. Firmware maintenance is administered in accordance with the standard MCN processes. Refer to the MCN Common Network Management Service Description for further information.

Supported Configurations

The following Fortinet FortiGate Security devices are supported.

- Fortigate hardware security appliances.
- Fortigate virtual security appliances deployed in on-prem or Public Cloud (AWS, Azure, Google)
- Single security appliance: A standalone security appliance or a set of standalone security appliances (managed independently from each other), running a minimum of FortiOS 6.4 or above.

- Resilient security appliances: Two or more security appliances of compatible models in an HA configuration. This could be either active / passive or active / active configuration, running a minimum of FortiOS 6.4 or above.
- Virtual security appliances of compatible models in high availability mode with active/passive configuration. Failure recovery can be manual.
- Clustered appliance: Two security appliances of compatible models in clustering configuration with automatic switch over.
- Load balanced cluster whereby a load balancer handles connections between two or more security appliances that are not clustered at the security appliance level.
- Single security controller running in standalone mode or two security controllers in high availability (active/passive) configuration.
- security appliances, deployed in the client's on-premises data center and Public Cloud (Azure/AWS/GCP) infrastructure, that are to be managed must be accessible over an IPsec tunnel, allowing management protocols such as SSH, SNMP etc.

Limitations

- Cloud management solutions such as Forti-Cloud or equivalent SaaS based management solutions are not supported.
- The managed Fortinet Edge Infrastructure Service does not include procurement of internet or WAN circuits, or Fortinet Software or hardware / virtual devices. These services are available from NTT under a separate Statement of Work.
- The tasks, features and services listed in this document are excluded from any underlying infrastructure hosting virtual {Technology} appliances.
- FortiSD-WAN features on the virtual security appliances deployed in public cloud infrastructure.

Standard Service Requests

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

Technology Transition Tasks

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

FortiManager

Technology Specific Operations

FortiManager Specific Monitors

The following technology specific monitors can be configured by default.

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Disk Status	FortiManager appliance disk including RAID status	✓	N/A	Engineering Teams will diagnose and try to resolve the issue, contacting the hardware maintenance provider as required.	180
IP Sessions (Connection Status)	FortiManager IP sessions	✗	Graphs for the parameter measured over time	N/A	60

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
FortiManager High Availability (HA), including HA peers	Monitors FortiManager High Availability status, and availability of HA devices that form part of the cluster.	✓	N/A	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client or hardware maintenance provider as required.	180
Global Statistics	FortiManager global performance statistics	x	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue.	120
FortiManager Administrative Domains	Monitors individual FortiManager Administrative domain states	x	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue., contacting the hardware maintenance provider as required.	180
Database Status	Monitors status of the FortiManager database	x	N/A	Engineering Teams will diagnose and try to resolve the issue, contacting the hardware maintenance provider as required.	180
HTTP / HTTPS Service Status	Monitors the status of the HTTP(S) status.	x	Graphs response time for HTTP(s) port connection.	Engineering Teams will diagnose and try to resolve the issue, contacting the hardware maintenance provider as required.	60
SSL Status	Monitors SSL status for errors	x	N/A	Engineering Teams will diagnose and try to resolve the issue, contacting the hardware maintenance provider as required	

Configuration Management

Device configuration backups are included in the standard offering and are described in more detail in the MCN Managed Configuration Backup Service Description

Firmware Maintenance

There are no specific requirements for firmware maintenance of the technology. Firmware maintenance is administered in accordance with the standard MCN processes. Refer to the MCN Common Network Management Service Description for further information.

Supported Configurations

- A FortiManager physical or virtual appliance running on infrastructure provided by the Client (either on-premises, private cloud, or public cloud infrastructure).
- Fortinet Edge Infrastructure physical and virtual devices are managed via a FortiManager.
- FortiManager providing centralized functions like config templates, policies and objects configuration, high availability configurations are supported.
- FortiManager and FortiAnalyzer associated environments.

Limitations

- Availability SLA's will be excluded for environments that have a single (standalone) FortiManager deployed.
- Where multiple FortiManagers are deployed and these have not been configured for high availability, clustered or load-balanced i.e. are operating as multiple standalone FortiManagers managing specific Fortinet Edge devices in the environment, availability SLA's will be excluded. NTT will seek to remediate the environment to provide FortiManager redundancy, at an additional cost.

- The tasks, features and services listed in this document are excluded from any underlying infrastructure hosting virtual {Technology} appliances.
- Cloud solutions such as FortiCloud or equivalent SaaS based management solutions are not supported.

Standard Service Requests

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

Technology Transition Tasks

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

FortiAnalyzer

Technology Specific Operations

FortiAnalyzer Specific Monitors

The following technology specific monitors can be configured by default.

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Disk Status	Appliance disk status	✓	N/A	Engineering Teams will diagnose and try to resolve the issue, contacting the hardware maintenance provider as required.	180
High Availability (HA)	Monitors High Availability status, and availability of HA devices that form part of the cluster.	✓	N/A	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client or hardware maintenance provider as required.	180
Global Statistics	Global performance statistics	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue.	120
Interfaces	Monitors the interfaces status.	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue and escalate to the Client as required.	120

Configuration Management

Device configuration backups are included in the standard offering and are described in more detail in the MCN Managed Configuration Backup Service Description.

Firmware Maintenance

There are no specific requirements for firmware maintenance of the technology. Firmware maintenance is administered in accordance with the standard MCN processes. Refer to the MCN Common Network Management Service Description for further information.

Supported Configurations

- FortiAnalyzer physical or virtual appliance(s) running on infrastructure provided by the Client (either on-premises, private cloud, or public cloud infrastructure).
- Fortinet Edge infrastructure physical and virtual devices managed via a FortiManager and interconnected with FortiAnalyzer.
- FortiAnalyzer deployed in Analyzer and collector mode is supported.

- Log view and log quota management are supported.

Limitations

- Security operations, FortSIEM/SOC and FortiSOAR, playbook automations are not supported.
- The tasks, features and services listed in this document are excluded from any underlying infrastructure hosting virtual {Technology} appliances.

Standard Service Requests

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

Technology Transition Tasks

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

FortiSwitch

Technology Specific Operations

FortiSwitch Specific Monitors

The following technology specific monitors can be configured by default.

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
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	180
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	120
Device Health	Device health and performance metrics (CPU, Memory, disk 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	120

Configuration Management

Device configuration backups are included in the standard offering and are described in more detail in the MCN Managed Configuration Backup Service Description

Firmware Maintenance

There are no specific requirements for firmware maintenance of the technology. Firmware maintenance is administered in accordance with the standard MCN processes. Refer to the MCN Common Network Management Service Description for further information.

Supported Configurations

- Single switch. A standalone switch or a set of standalone switches (managed independently from each other), running a minimum of FortiOS 6.4 or above.

Limitations

- The tasks, features and services listed in this document are excluded from any underlying infrastructure hosting virtual {Technology} appliances.

Standard Service Requests

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

Technology Transition Tasks

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

Forti Wireless Controller and AP

Technology Specific Operations

FortiAP Specific Monitors

The following technology specific monitors can be configured by default.

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Interfaces	Check port's throughput, packet transmission and errors	✗	Graphs of the parameter measured over time	N/A	180
Device Health	FortiWLC device health and performance metrics including CPU, memory, and disk 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	180
AP Performance Stats	Performance metrics for AP's connected to the specific WLC	✗	Graphs of the parameter measured over time	N/A	180
AP Operating Status	Device health for AP's connected to the specific WLC	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to solve the issue, and escalate to the Client if needed	300

Configuration Management

Device configuration backups are included in the standard offering and are described in more detail in the MCN Managed Configuration Backup Service Description

Firmware Maintenance

There are no specific requirements for firmware maintenance of the technology. Firmware maintenance is administered in accordance with the standard MCN processes. Refer to the MCN Common Network Management Service Description for further information.

Supported Configurations

- Wireless controller in the FortiGate security appliance
- All FortiAP Access Points (AP's)

Limitations

- FortiWLC Controllers are not supported
- The tasks, features and services listed in this document are excluded from any underlying infrastructure hosting virtual {Technology} appliances.

Standard Service Requests

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

Technology Transition Tasks

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

FortiAuthenticator

Technology Specific Operations

FortiAuthenticator Specific Monitors

The following technology specific monitors can be configured by default.

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Authentication	Authentication service monitoring	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the vendor or client as required	60
High Availability	Monitors high availability, including status, peer count	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the vendor or client as required	60
DNS Health	Collector DNS resolution status	✗	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the vendor or client as required	180
HTTP / HTTPS Service Status	Monitors the status of the HTTP(S) status.	✗	Graphs response time for HTTP(s) port connection.	Engineering Teams will diagnose and try to resolve the issue, and escalate to the vendor or client as required	60
Interface utilization	Monitors the interfaces status and performance metrics including SD-WAN interfaces.	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the vendor or client as required	120
System level IP status	Monitor the system TCP/UDP sessions and errors info.	✗	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the vendor or client as required	300

Configuration Management

Device configuration backups are included in the standard offering and are described in more detail in the MCN Managed Configuration Backup Service Description.

Firmware Maintenance

There are no specific requirements for firmware maintenance of the technology. Firmware maintenance is administered in accordance with the standard MCN processes. Refer to the MCN Common Network Management Service Description for further information.

Supported Configurations

- single appliance or a set of standalone authenticator appliances (managed independently from each other).
- Two or more appliances of compatible models in an HA configuration.

- Single appliance deployed in the client's on-premises data center or Public Cloud (Azure/AWS/GCP) infrastructure, that are to be managed must be accessible over an IPsec tunnel, allowing management protocols such as SSH, SNMP etc.

Limitations

- Cloud solutions such as FortiCloud or equivalent SaaS based solutions are not supported.
- The tasks, features and services listed in this document are excluded from any underlying infrastructure hosting virtual {Technology} appliances.

Standard Service Requests

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

Technology Transition Tasks

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

FortiSD-WAN

Technology Specific Operations

FortiSD-WAN Specific Monitors

The following technology specific monitors can be configured by default.

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Interface utilization	Monitors the SD-WAN member interfaces inbound and outbound bandwidth utilization	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the vendor or client as required	120
Interface statistics	Monitor the SD-WAN interface status, packet loss, discards.	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the vendor or client as required	120
Jitter	Average jitter on the specified SD-WAN link	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the vendor or client as required	120
Latency	Average latency on the specified SD-WAN link	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the vendor or client as required	120
Packet loss	Average packet loss on the specified SD-WAN link	✓	Graphs of the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the vendor or client as required	120
GRE tunnel	Monitor the GRE tunnel state, Jitter, Latency and delay of tunnel probe	✓	N/A	Engineering Teams will diagnose and try to resolve the issue, and escalate to the vendor or client as required	900

Configuration Management

Device configuration backups are included in the standard offering and are described in more detail in the MCN Managed Configuration Backup Service Description

Firmware Maintenance

There are no specific requirements for firmware maintenance of the technology. Firmware maintenance is administered in accordance with the standard MCN processes. Refer to the MCN Common Network Management Service Description for further information.

Supported Configurations

- Fortinet Secure SD-WAN feature enabled on FortiGate Security appliances.
- FortiGate hardware or virtual security appliances deployed in on-premises infrastructure.
- Fortinet Secure SD-WAN feature enabled on FortiGate security appliances managed by FortiManager.

Limitations

FortiGate Network virtual appliances (NVAs) deployed in Azure vWAN hub.

Standard Service Requests

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

Technology Transition Tasks

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

FortiExtender

Technology Specific Operations

FortiExtender Specific Monitors

The following technology specific monitors can be configured by default.

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
operational status	Monitors the operational status of FortExtender	✓	NA	Engineering Teams will diagnose and try to resolve the issue, and escalate to the vendor or client as required	300

Configuration Management

Device configuration backups are included in the standard offering and are described in more detail in the MCN Managed Configuration Backup Service Description

Firmware Maintenance

There are no specific requirements for firmware maintenance of the technology. Firmware maintenance is administered in accordance with the standard MCN processes. Refer to the MCN Common Network Management Service Description for further information.

Supported Configurations

- Standalone management of FortiWeb
- Fortigate WAN Extension using FortExtender.
- FortiExtender Out-of-Band Management (OBM).

Limitations

Cloud management solutions such as FortiCloud or equivalent SaaS based management solutions are not supported.

Internet or WAN circuits management is out of scope.

Standard Service Requests

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

Technology Transition Tasks

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

FortiWeb

Technology Specific Operations

FortiWeb Specific Monitors

The following technology specific monitors can be configured by default.

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
operational status	Monitors the operational status of FortWeb	✓	NA	Engineering Teams will diagnose and try to resolve the issue, and escalate to the vendor or client as required	300

Configuration Management

Device configuration backups are included in the standard offering and are described in more detail in the MCN Managed Configuration Backup Service Description

Firmware Maintenance

There are no specific requirements for firmware maintenance of the technology. Firmware maintenance is administered in accordance with the standard MCN processes. Refer to the MCN Common Network Management Service Description for further information.

Supported Configurations

- Standalone management of FortiExtender.
- FortiWeb hardware or virtual security appliances deployed in on-premises infrastructure.

  Appliance deployed in the client’s on-premises data center or Public Cloud (Azure/AWS/GCP) infrastructure, that are to be managed must be accessible over an IPsec tunnel, allowing management protocols such as SSH, SNMP etc.

Limitations

Cloud management solutions such as FortiwebCloud or equivalent SaaS based management solutions are not supported.

Internet or WAN circuits management is out of scope.

Standard Service Requests

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

Technology Transition Tasks

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