Managed Security Appliance Technology Service Description

Overview

This document provides information relating to the management and monitoring of Security appliances under the standard MCN offering. The monitoring, configuration, limitations, and available service requests are outlined hereunder.

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.

Technology Specific Operations

Monitors

The following technology specific monitors can be configured by default.

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Disk (if any)	Disk usage in %	✓	Graphs of the parameter measured over time.	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client if needed	300
Interfaces	Check of the device interfaces (virtual or physical)	✓	N/A	Engineering Teams will diagnose and try resolve the issue	300
IPSec VPN (Site-to-Site) tunnel	Monitors status and throughput metrics of static site to site IPSEC VPN tunnels	✓	N/A	Engineering Teams will diagnose and try resolve the issue	300
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 resolve the issue, and escalate to the Client if needed	180
HA Status(if any)	Check the status of High Availability	✓	N/A	Engineering Teams will diagnose and try resolve the issue	60

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 configurations are supported:

- Single security appliance i.e. a standalone security appliance (physical or virtual devices)

- Security appliances in high availability (HA) configuration (physical or virtual devices) which are on-premises i.e. Two security appliances of compatible models in an active/passive configuration, both connected at the same time (failure recovery can be manual).
- Virtual security appliances of compatible models in high availability mode with active/passive configuration. Failure recovery can be manual.
- Security appliance clustering i.e. two security appliances of compatible models in an active/active or active/passive 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.
- Security controller in High Availability mode.

The following environments are supported:

- Client on-premises data centre
- Colocation data centre
- Public Cloud (Azure/AWS/GCP) infrastructure.

Limitations

The following configurations are not supported:

- Virtual security appliances with active-active HA setup running in public cloud infrastructure.
- Security appliances are not supported unless paired with dedicated management console.
  - A security controller is recommended to manage the security devices. Where there is not a security controller available, a maximum of 15 On-prem standalone devices can be supported by NTT irrespective of whether the total number of standalone devices is comprised of physical security appliances, virtual security appliances or a combination thereof. Where the standalone devices are deployed for additional services, such as Security and SD-WAN and/or the security appliances are deployed in cloud environment, a controller is required irrespective of the number of security appliances.
- NTT ECL 2.0 integrated images for FortiGate are not supported.
- FortiGate security appliances with active-passive HA setup running in AWS Multi-AZ or Azure can only be configured with Source NAT using the main security appliance interface.
- FortiGate security appliances with active-passive HA setup running in AWS Multi-AZ or Azure can only be configured with Destination NAT using the "port forwarding" option on the "Virtual IP" configuration. One-to-one IP static NAT is not allowed.
- Dynamic VPN tunnels such as AutoVPN monitoring, SDWAN Virtual interfaces and Remote Access VPN tunnel monitoring are not supported.
- The tasks, features and services listed in this document are excluded from any underlying infrastructure hosting virtual Security Appliances.

Service Requests

A list of 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.