1 Networking Management - Basic Firewall

1.1 Overview of Service

This service provides remote configuration, monitoring and management of firewall (basic functionality) in the Client's on-premises, colocation data center or in public cloud.

1.2 Client Responsibilities

(a) The Client must be in possession of an active hardware service contract with NTT Uptime Support Services or the vendor of the firewall(s) under management

(b) The Client must delegate authority to the engineer to contact the firewall vendor directly

(c) Except in cases where the firewall is provided by NTT, any licenses required for management are Client responsibility

(d) Any software required to service or access the ethernet switches must be provided to NTT

(e) All access required for remote access and monitoring must be enabled by Client.

(f) Any action not specifically identified as in scope in this Service Description

(g) Any task requiring physical access

1.3 Service Specific Operations

(a) Monitors

The following monitors can be configured by default if available on the hardware:

Monitor	Description	Alerts	Performance Info	Resolution
Disk (if any)	Disk usage in %	Yes	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	Check of the device interfaces (virtual or physical)	Yes	N/A	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed
Sessions	Check the number of current/active sessions in the device	Yes	Graphs of the parameter measured over time	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	Yes	N/A	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed

(b) Service Requests

As part of the Service, the fulfillment of the following types of requests are included:

Task	Description
Creation and management of security zones	Creation, change and deletion of Security Zones configured in the device
Creation and management of VPNs	Creation, change and deletion of VPNs configured in the device, including the users in the VPNs; this does not include connection to the external peer to configure the remote end point, or the installation of any client on any Client computer
Management of access rules	Creation, change and deletion of access rules configured in the device that allow and deny traffic to/from the servers in the DMZs and other internal networks
Creation and management of NATs	Creation, change and deletion of NATs rules
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 optimizing disk space (if disk is present in the device)

1.4 Supported Technologies

The following firewalls are supported:

(a) Juniper SRX 1x0, SRX 2x0, SRX 300, SRX 550, SRX 650

(b) Palo Alto VM-300 VM-500 VM-700

(c) FortiGate D series: 800, 900, 1000, 1200, 1500, 2000

(d) FortiGate E series: 30, 50, 60, 80, 90, 100, 200, 300, 500

(e) FortiGate VM-series

The following configurations are supported:

(f) Single firewall: a standalone firewall

(g) HA firewall configurations (physical devices, FortiGate on Azure or AWS, Palo Alto on Azure or AWS): two firewalls of compatible models in an active/passive configuration, both connected at the same time (fail recovery can be manual)

(h) Firewall clustering: two firewalls of compatible models in an active/active or active/passive configuration and automatic switch over

(i) Load balancing cluster: a load balancer handles connections between 2 or more firewalls (no clustering at firewall level)

Supported VPN Configurations:

(j) FortiGate: IPsec LAN to LAN, IPsec Dial up, SSL Dial up

(k) Juniper: IPsec LAN to LAN

The following configurations are not supported:

(l) Virtual firewalls with active-active HA setup running in AWS or Azure

(m) Virtual firewalls functioning as perimeter firewall in a private cloud solution

1.5 Supported Environments

The following VPN configurations are supported:

(a) Client on-premises data center

(b) Colocation data center

(c) Public Cloud only as described in the Limitations section below.

1.6 Limitations

The following limitations apply:

(a) FortiGate firewalls with active-passive HA setup running in AWS Multi-AZ or Azure can only be configured with Source NAT using the main firewall interface

(b) FortiGate firewalls 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

(c) Firewall appliances in Public Cloud are subject to NTT review and approval in NTT's sole and absolute discretion. The specific version and type of Firewall must be specified in the SOW. End of life products are not supported.

1.7 Tasks Included in the Standard Transition

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

(a) Creation of security zones

(b) Creation of access rules and NATs, creation of default policies

(c) Creation and configuration of site-to-site IPsec VPNs

(d) Creation and configuration of client-to-site IPsec VPNs, including authentication (local users or external server); this does not include the connection to the external authentication server to perform any task

(e) Creation and configuration of client-to-site SSL VPNs, including authentication (local users or external server); this does not include the connection to the external authentication server to perform any task

(f) *In HA environments*: setup of HA services

(g) *In Cluster environments*: service clustering

The following tasks are optional and may incur a separate fee:

(h) Security policy definition: this is a consultancy task which must be contracted in addition to the Service

(i) Additional functions provided by the devices other than firewalling and VPN are not included in the Service but can be contracted additionally (Antivirus, AntiSpam, Web filtering, IDP, IDS, etc.)

1.8 Tasks Not Included in the Standard Transition

The following tasks are not included in the standard transition:

(a) Physical installation of the firewall(s) or any task requiring physical access

(b) Cabling of the device