1 Networking Management - Advanced Firewall

1.1 Overview of Service

This service provides configuration, monitoring and management of firewalls (advanced functionality) remotely in the Client's data center, colocation facility or in public cloud. The functionality described herein is in addition to the “basic” services described in the *Managed Basic Firewall* services description.

1.2 Client Responsibilities

(a) 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) Client must delegate authority to NTT’s engineers to contact the firewall vendor directly.

(c) Except in cases where the device is provided by NTT, license management is client responsibility.

(d) Except in cases where Client has contracted with NTT to provide Managed Detection and Response, or for which Standard Security is in-scope as part of Managed Public or Private Cloud (MSP or NTT Anywhere), SIEM and SOC services are Client responsibility. At Client request, NTT may setup log forwarding to a third-party SIEM or log management service.

(e) After management is initiated, there may be many false positives. Client is required to review the logs to ensure that policies do not result in an unmanageable number of false positives.

(f) Design of a security policy or definition of changes to an existing policy is Client responsibility.

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

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

(i) Any task requiring physical access.

1.3 Service Specific Operations

(a) Monitors

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

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 solve the issue
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 solve the issue

(b) Service Requests

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

Task	Description	Baseline or UTM
Creation and management of profiles and filter features specific to Palo Alto	Creation, change or deletion of application filters for enabling the app-ID feature Creation, change or deletion of profiles for enabling the content-ID policy-based features like antivirus, anti-spyware and vulnerability protection (IPS); and Creation, change or deletion of profiles for enabling the URL filtering and file blocking policy-based features.	UTM
Bandwidth management	Creation, addition or deletion of Bandwidth Management, Quality of Service or shaping rules	UTM
Management of Time Policies	Creation, addition, changes and deletion of Work Hours, After Hours, or Weekend Hours schedules	UTM
Management of SSL certificates and settings	Addition, removal and modification of SSL certificates associated with the device and services	UTM

Management of network generic services	Changes in the NTP, DHCP, DNS and Dynamic DNS settings	UTM
Relaying of network generic services	Configuration of NTP, DHCP and DNS settings for these to be resolved by external services	Baseline
Management of AD/LDAP settings	Changes in the end-users auth mechanisms to external AD's and LDAP services	UTM
Configuration of DDoS service	Detection of DDoS attacks is based on the devices capability and employs a mix of methods to cover the varying nature of attacks. Some of the important methods employed are: · Misuse Anomaly – Setting thresholds for potentially malicious traffic (TCP SYN, IP Frag, DNS malformed, etc) · Profiled Anomaly – Identifying malicious traffic that exceeds normal patterns (e.g., http flood attacks, DNS/NTP amplification attacks) · Fingerprint Anomaly – Identifying known sources of bad traffic and attack signatures	UTM
Management of DDoS service	Changes in flood protection, DDoS parameters and other mitigation features as available in the device	UTM
Creation and management of 2 Factor Authentication settings	With new Tokens, registration of the tokens, association with users Revoke activities and association of tokens to users Creation, change or deletion of the policies associated to users and tokens Renewal of tokens Deletion of tokens	UTM
Management of load balancing	Creation, addition or deletion of load balancing rules and dynamic gateways	UTM
Creation and management of antivirus component	Creation, change or deletion of the pattern updates and automatic pattern updates Creation, change or deletion of Antivirus custom objects and features profiles Creation, change or deletion of Antivirus policies to security policies Creation, change or deletion of file scanning and application protocol scanning (HTTP, FTP, SMTP, POP3 and IMAP) Creation, change or deletion of whitelists and/or blacklists Creation, change or deletion of Client Anti-Virus settings Creation, change or deletion of notifications (to the Client admins); and Management of third-party antivirus engines (if present and bought by the Client)	UTM
Creation and management of Anti-spam component	Creation, change or deletion of the pattern updates and automatic pattern updates Creation, change or deletion of whitelists and/or blacklists Creation, change or deletion of notifications; and Management of third-party anti-spam engines (if present and bought by the Client)	UTM
Creation and management of IDP/IDS	Management of ID signature updates Creation, change or deletion of IDP/IDS attack objects and object groups Creation, change or deletion of IDP/IDS policies, policy templates, policy rules, ID rules, rule bases, rule object and rule actions Creation, change or deletion of custom attack objects (attack properties, protocol, ports, services, test conditions, etc)	UTM

	Creation, change or deletion of IDP/IDS applications and application sets Creation, change or deletion of IDP/IDS application identification Creation, change or deletion of IDP/IDS class of service actions; and Creation, change or deletion of IDP/IDS monitoring and IDP notifications (to the Client admins)	
Creation and management of WAF	Addition, removal and modification of Action Sets and associated policies and jobs Configuration of error pages and error page groups Configuration of system definition settings DPI SSL and SSL firewall control settings; and Application Control settings;	UTM
Creation and management of web filtering/Web Proxy	Management of Safe Search features Management of advanced filtering features Creation, change or deletion of web filter profiles Management of web filtering override features Management of users for web filtering profiles Management of web filtering for SSL traffic; and Management of Web Proxy forwarding.	UTM
Forward logs to an external SIEM service	Changes in the settings to forward logs to an external SIEM and SOC solution, destination, ports and or information being sent. • only applicable when Client has not contracted with NTT for SIEM and SOC services such as NTT MDR or embedded Standard Security services included with Managed Public and Managed Private Cloud	Baseline
Forward logs to a managed log management service	Changes in the settings to forward logs to an associated (and managed) log management system such as Panorama, FortiAnalyzer or others • only applicable when Client has not contracted with NTT for SIEM and SOC services such as NTT MDR or embedded Standard Security services included with Managed Public and Managed Private Cloud	Baseline

Those tasks labeled “Baseline” can be provided on all devices. Those tasks labelled “UTM” are subject to license and vendor support limitations.

(c) Other Capabilities

The following UTM features can be configured provided if the device is correctly licensed (some of the features require additional licensing or ongoing maintenance costs) and the vendor supports these functions:

(i) Configuration of Web filtering and/or Web Proxy
(ii) Configuration of Gateway Antivirus
(iii) Configuration of Client Antivirus
(iv) Configuration of AntiSpam and/or RBL filters for SMTP
(v) Configuration of Reputation, Geo-IP and Botnet filtering
(vi) Configuration of Anti-Spyware
(vii) Configuration of Web Application Firewall and/or Application Control
(viii) Configuration of Load balancing
(ix) Configuration of time scheduling for operation
(x) Configuration of DDoS and/or Flood protection mechanisms
(xi) Configuration of Bandwidth management and QoS
(xii) Configuration of DNS
(xiii) Configuration of DHCP
(xiv) Configuration of end user access to external auth AD/LDAP systems
(xv) Configuration of IPS/IDS
(xvi) Configuration of Multi-Factor Authentication; and

(xvii) Configuration of Content Filtering.

(xviii) Contact the NTT with the exact device description (model, serial number, etc.) for verification of management features.

1.4 Supported Technologies

The following firewalls are supported:

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

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

(c) FortiGate VM Series

(d) Palo Alto PA and VM series

The following configurations are supported:

(e) Single firewall: a standalone firewall

(f) 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)

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

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

(i) 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 functioning as perimeter firewall in a private cloud solution

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

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

(a) Firewalls require an active Internet connection, to allow the appliance to download the latest policy updates

(b) 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

(c) 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

(d) 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 Client Requests Not Included:

IDS, WAF and other advanced security features are configured specifically for the application(s) being protected. The Client, therefore, must provide the intelligence used to determine appropriate security policies. The scope of the managed IDS, WAF and advanced security features will be **limited to** applying changes based on Service Requests which are identified based on SIEM or other log management tools used by the Client. Likewise, Client must advise NTT of the reasons why applications are blocked, or not blocked, if generating false positives. A log review for unidentified errors or false positives is not included and is the responsibility of the Client. While NTT will make all attempts to reduce the number of false positives, it may not be held responsible for authentic users being denied access to the Client's application.

1.8 Tasks Included in the Standard Transition

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

(a) For all devices:

(i) Initial licenses and contracted subscriptions configuration

(ii) Install SSL keys/certificates associated to protected sites for the advanced services that need them

(iii) Configuration of error pages and error page groups

(iv) Creation of Work Hours, After Hours, or Weekend Hours schedules. *After hours and Weekend hours must be specified as in-scope in the SOW.

(v) Configuration of DNS, DHCP, Dynamic DNS and other network generic services if contracted
(vi) Configuration of load balancing rules if contracted
(vii) Configuration of Web filtering, Content Filtering and/or WebProxy forwarding if contracted
(viii) Configuration of Intrusion Detection Services if contracted
(ix) Configuration of WAF and/or Application Control settings if contracted
(x) Configuration of Advanced Firewall settings and flood protection (depending on vendor) if contracted
(xi) Configuration of Bandwidth Management and Quality of Service if contracted
(xii) Configuration of AntiSpam settings if contracted
(xiii) Configuration of end user access and connection to external auth systems (AD, LDAP) if contracted
(xiv) Configuration of Client Anti-Virus if contracted
(xv) Configuration of Gateway Antivirus if contracted
(xvi) Configuration of Intrusion Prevention Service if contracted
(xvii) Configuration of Anti-Spyware if contracted
(xviii) Configuration of Anti-Spam and/or RBL Filters for SMTP if contracted
(xix) Configuration of MultiFactorAuthentication and tokens if contracted
(xx) Configuration of Reputation and/or Geo-IP and Botnet filters if contracted
(xxi) Configuration of AppFlow, log relaying and other log management mechanisms if contracted

(b) For Palo Alto devices:
(i) Integration with LDAP/AD for enabling the User-ID feature
(ii) Configuration of Application Filters for enabling the App-ID feature
(iii) Configuration of Profiles for enabling the Content-ID policy- based features like Antivirus, Antispyware and Vulnerability Protection (IPS)
(iv) Configuration of Profiles for enabling the URL Filtering and File Blocking policy-based features

(c) The following tasks are optional and may incur a separate fee:
(i) Definition of security policies: This is a consultancy task that must be contracted separately
(ii) Analysis of Client's applications, consultancy, audits and advisory services are not included in the setup fee
(iii) Hardware, Software and/or support

1.9 False Positives

As a general rule, the following approach is used to transition IDS, WAF, Application Profiling or Advanced Firewall devices into management:

(a) The installation includes the configuration of all policies defined by the Client
(b) During the time immediately following installation, many false positives are expected; during this time the security policies should be less restrictive
(c) Additional rules are then added incrementally to strengthen the security policy
(d) This process will eliminate false positives and is intended to provide a more secure environment for the Client's applications; and
(e) Once stabilized, no further changes are required until new versions of the Client's applications are released and deployed, at which point the process is repeated.

Due to the expected results described above, it is important Client discuss with NTT how to adapt the Advanced Firewall policy to the Client's applications. In the event of issues once a policy has been activated, NTT is only responsible for the deactivation of the policy or (if possible) or to change the policy from "Block" to "Alert", "Log", or similar options specific to the technology. 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.

1.10 Tasks Not Included in the Standard Transition

The following tasks are not included in the standard transition:

(a) Physical installation of the firewall(s)
(b) Any task requiring physical access.
(c) Licenses, software, use rights or support agreements.