1 Networking Management - Web Application Firewall (WAF)

1.1 Overview of Service

This service provides configuration and management of a Web Application Firewall (WAF) offered explicitly selected in Scope for any of NTT's Managed Private and/or Public Cloud offerings.
A WAF helps protects web applications by filtering, monitoring, blocking malicious HTTP/S traffic and unauthorized data from leaving a web application. It does this by adhering to a set of policies that help determine what traffic is malicious and what traffic is safe. Just as a proxy server acts as an intermediary to protect the identity of a user, a WAF operates in similar fashion but in the reverse—called a reverse proxy—acting as an intermediary that protects the web application server from potentially malicious activity.

1.2 Client Responsibilities

(a) Provide list of applicable domains and/or URLs to be protected by this service

(b) Provide list of applications to protect

(c) Provide access to DNS registrars (either direct or via a named contact)

(d) Provide access to Authoritative DNS to configure CNAME setup (either direct or via a named contact)

(e) Testing of application specific functions such as file uploads, report generation, content, and any other additional tests required to validate functional operation of Domain/URLs protected by WAF

(f) Only applicable for Enterprise Plus WAF, contract for Managed Load Balancer/Traffic Manager Service for a dedicated virtual F5 BIG-IP VE appliance or Traffic Manager LTM and/or GTM cloud resource in any of NTT's Private or Public Cloud offerings.

(g) Client must maintain an active support agreement with the OEM and provide access to NTT

(h) Unless purchasing via NTT, Client must provide SSL certificates to be uploaded to the platform

1.3 Service Specific Operations

(a) Monitors

The following monitors are configured by default, if supported by the hardware and software:

Monitor	Description	Alert	Performance Info	Resolution
Error Rate	Origin Error Rate detected	Yes	N/A	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed
SSL Alert	SSL Certificate Error detected	Yes	N/A	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed
HTTP DDoS Attack	HTTP DDoS Attack detected	Yes	N/A	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed
Layer 4 Attack Alert	Layer 4 Attack detected	Yes	N/A	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed
Flow-based Monitoring	Volumetric Attack detected	Yes	N/A	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed
Access Service Token	Expiring Access Service Token detected	Yes	N/A	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed
Route Leak Detection	Route Leak Detection detected	Yes	N/A	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed
Secondary DNS Monitoring	Secondary DNS Primaries Failing Detected	Yes	N/A	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed

Alerts related to elements not under NTT management will be escalated to the Client.

(b) Service Requests

The fulfillment of the following types of requests are included:

Task	Description	Standard WAF without SIEM Integration	Enterprise WAF with SIEM Integration	Enterprise Plus WAF with SIEM and LTM/GTM Integration
Firewall Rules Management	Creation and troubleshoot Firewall Rules	Up to 10 per domain	Up to 25 per domain	Up to 50 per URL and/or Domain
Firewall Domain Rules Maintenance	Change/tune and deletion of Firewall Rules on a per Domain policy basis	✓	✓	✓
Firewall URL Rules Maintenance	Change/tune and deletion of Firewall Rules on a per URL policy basis	✗	✗	✓
Page Rules Management	Creation and troubleshoot Pages Rules	Up to 5 per domain	Up to 20 per domain	Up to 40 per URL and/or Domain
Page Domain Rules Maintenance	Change/tune and deletion of Page Rules on a per Domain policy basis	✓	✓	✓
Page URL Rules Maintenance	Change/tune and deletion of Page Rules on a per URL policy basis	✗	✗	✓
VIP to WAF Rules Management	Creation and troubleshoot VIP to WAF Rules	✗	✗	✓
VIP to WAF Rules Maintenance	Change/tune and deletion of VIP to WAF Rules	✗	✗	✓
WAF Remediation	WAF will be adjusted for items that can be remediated via WAF policy based upon security discoveries found with client provided Web Application Scanning reports, or when Web Application Scanning services have been contracted separately with NTT.	✗	✗	✓
Reporting	Upon request, provide monthly WAF report, with (30) days of analytics	✓	✓	✓
SSL Certificates	Provide SSL certificates via Universal SSL or certificate authority. Custom certificates require an advanced engagement.	✓	✓	✓

1.4 Supported Technologies

The following technologies are supported:

(a) Cloudflare SaaS for Standard and Enterprise WAF

(b) F5 BIG-IP VE appliance for Enterprise Plus WAF

The following configurations are supported:

(c) Internet accessible web application

(d) Dedicated F5 BIG-IP VE appliance in HA configuration for Enterprise Plus WAF

(e) Internal-only applications using F5 BIG-IP

1.5 Supported Environments

The following environments are supported:

(a) NTT Managed Private, contracted separately

(b) NTT Managed Public Cloud, contracted separately

1.6 Limitations

The following limitations apply:

(a) Direct access WAF administration console is not available.

(b) Changes within the configured application and application patching and versioning can result in nullification of WAF policy and customer perception/access.

(i) Recommended that customer teams coordinate with engineering for major updates.

(c) Web applications with more than 400Mbps of combined ingress and egress Internet bandwidth may require a customized WAF solution.

1.7 Tasks Included in the Standard Transition

As part of the Service, the following tasks are included if specifically identified as In Scope on the SOW:
Setup and configuration of:

(a) Application specific Firewall Rules, as defined in Service Requests

(b) Application specific Page Rules, as defined in Service Requests

(c) Protection against Generic attacks

(d) Protection against generic Network based attacks

(e) Protection against Network layer DOS attacks

(f) Protection against Application layer DoS attacks

(g) Protection against policy evasion attacks

(h) Protection against Known exploits

(i) Protection against Buffer overflows

(j) Protection Anti-Web defacement

(k) Protection against Known server and database vulnerability

(l) Protection against OWASP top 10 security risks

Additional Standard Transition tasks applicable only for Enterprise and Enterprise Plus WAF:

(m) Setup and configuration of WAF raw policy log reporting to NTT SIEM or Client provided and managed SIEM

Additional Standard Transition tasks applicable only for Enterprise Plus WAF:

(n) Setup and configuration of:

(i) Application Load balancing (VIP to WAF Rules)

(ii) Protection against outbound data theft

(iii) SSL offloading support

(iv) Prevent OS and web server Fingerprinting

(v) Protection against business logic attacks

1.8 Tasks Not Included in the Standard Transition

The following tasks are not included in the standard transition of *x technology:*

(a) Physical installation of the firewall(s)

(b) Any task requiring physical access.