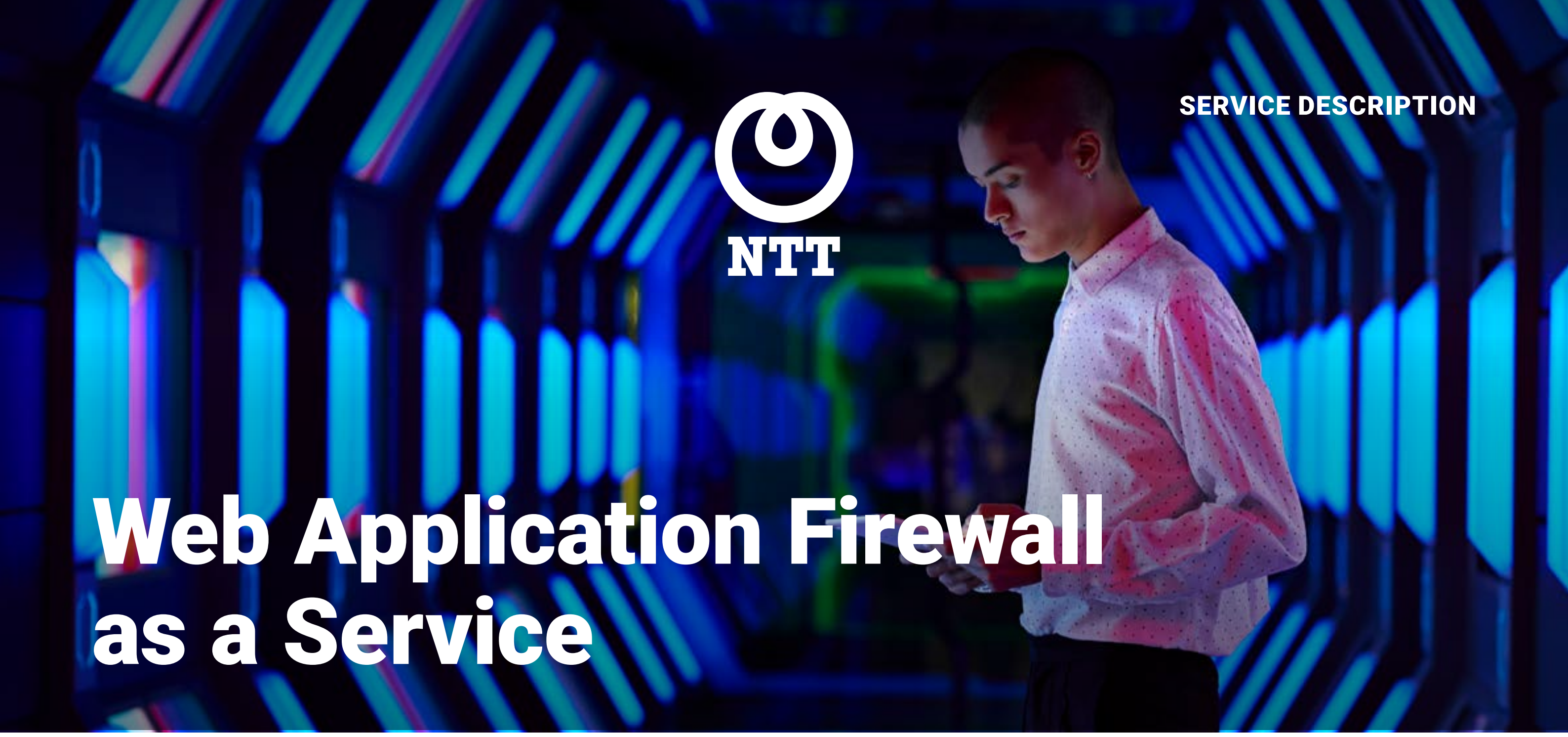

SERVICE DESCRIPTION

NTT

Web Application Firewall as a Service

Name	NTT Ltd. Service Description – Web Application Firewall as a Service
Owner	NTT Ltd.
Status	APPROVED
Classification	UNCLASSIFIED-EXTERNAL
Version	V1.21
Date	07 August 2019

Contents

Contents

1 Service Matrix

Managed Security Services are available in packages consisting of a core set of Service Modules, associated Service Elements and Options.

The following table reflects the service elements available in Web Application Firewall as a Service (WAF as a Service):

Section	Service Elements (WAF as a Service)	Standard	Enhanced
Core Service Elements			
3	• Hours of Operation (24x7) • Security Operations Centers (SOCs) • Client Portal • Language support • Management Options • Communication • Escalation Management • Health and Availability	✓	✓
4	Service Transition • Engagement Phase • Planning Phase • Staging Phase • Integration Phase • Go-Live Phase • Service Transition Deliverable Acceptance	✓	✓
Service Features			
5.1	Monitoring		
	• Security Analyst Interaction		✓
	• Client Notification	✓[1]	✓
	• Portal and Reporting	✓[2]	✓
	• Customization of Monitoring and Alerting Rules		✓
5.2	Web Application Security		
5.2.1	• Web Application Firewall	✓	✓
5.2.2	• WAF policies	✓	✓
5.2.3	• Security Policies	✓	✓
5.2.4	• SSL support	✓	✓
5.2.5	• Two factor authentication	✓	✓
5.3	DDoS protection for Infrastructure	✓	✓
5.4	Content Delivery Network (CDN)	✓	✓
Service Options			
6.1	DDoS protection: • Protection for websites • Protected IP • Edge IP • Protection for DNS • Infrastructure Monitoring	✓	✓
6.2	SIEM / Log Integration	✓	✓[3]
6.3	Attack Analytics	✓	✓
6.5	Load balancing and failover	✓	✓
6.6	Investigator – Enriched and aggregated Log Search		✓
6.7	Secure long-term log storage		✓
Service Delivery Management			
7.1	Incident Management	✓	✓
7.2	Service Request Fulfilment	✓	✓
7.3	Problem Management	✓	✓

2 Service Prerequisites

2.1 General Requirements

2.1.1 Service Selection

Client is responsible for selecting services and ensuring that the selected services meet their security requirements and operations.

2.1.2 Client Point of Contact

Client will assign a main Point of Contact (POC) to work with the NTT Ltd. Account Team to schedule all service-related activities and communications with the SOC as needed for installation and ongoing tuning and support.

- To prevent delays during Implementation, Client will ensure completion of the NTT Ltd. Client Security Services Detail (CSSD) form.
- Client POC will be available during all scheduled activities.
- Client is responsible for providing NTT Ltd. with all contact information updates pertaining to Incident, Service Request, and Security Incident escalation instructions.

2.1.3 Client Staff and Resources Requirements

Client will provide knowledgeable technical staff, and/or third-party resources, to assist with Service configuration and implementations, including:

- Configuring end-to-end connectivity of in-scope devices to WAF as a Service cloud infrastructure (via Public Internet)
- Working with third-party vendors for support or provide authorization for NTT Ltd. Account Team to contact third-party vendors on behalf of Client as appropriate
- Having an operational Domain Name Service (DNS) in place
- Using the Service via the provisioned portal(s) or such other means as directed by NTT Ltd. or its nominee
- Not reselling, renting, or leasing the Service to any third party without prior written consent from NTT Ltd.

[1] *Email only.*

[2] *Standard reporting only.*

[3] *Prerequisite with Enhanced.*

2.1.4 Third-Party Vendors

Client will work directly with third-party vendors hosting any in-scope devices/services to allow NTT Ltd. to perform services.

2.1.5 Maintenance, Support, and Licensing Agreements

Client is responsible for procuring all maintenance, support, and licensing agreements with third party vendors for all non-NTT Ltd. provided in-scope services for the term of the Client agreement, unless otherwise stated in the Purchase Order.

2.1.6 Software Modification

NTT Ltd. will not support altered, damaged, or modified software,
or software/service that is not an NTT Ltd.-supported version.

2.1.7 Third-Party Device/Service Failure

Client will work with third party vendors to rectify device/service failure for all non-NTT Ltd. provided devices/Services and
is responsible for all associated expenses.

2.1.8 Responsibility for Data Privacy, Regulatory, and Administrative Policies and Procedures

Except where otherwise provided for in applicable law, Client is responsible for all relevant complying with data privacy, regulatory, and administrative laws and policies and procedures related to monitoring user traffic and communications.

2.1.9 Internet Service Provider or Client Network Outages

NTT Ltd. is not responsible for resolving Client's Internet Service Provider (ISP) outages, or issues with Client's internal network infrastructure which is not under NTT Ltd. management.

2.1.10 Closure of Service Request, Incidents and Security Incidents

Client will work with NTT Ltd. to bring closure to each Service Request, Incident and Security Incident identified by the services presented in this Service Description and NTT Ltd. shall not be liable for any consequences of such delays.

2.1.11 Providing Required Information

Client's failure to provide any of the Service Requirement information on a timely basis can result in delays in Service Transition and Service Delivery by NTT Ltd..

2.2 Communication Requirements

2.2.1 NTT Ltd. Log Transfer Agent

WAF as a Service is a cloud-based service that doesn't require Client premises equipment.

NTT Ltd. uses secure API to fetch and process logs via the cloud based Log Transfer Agent (LTA).

NTT Ltd. is responsible for configuration, management, maintenance and enrolment of the client into the service.

The LTA collects service logs, events and reports for processing.

2.2.2 Connection to Client Network

Client must supply all the necessary network interfaces to connect the Client's own, third party and ISP networks to the WAF as a Service (via Public internet).

2.2.3 Connectivity and System Configuration

Traffic routing

The Service can only be provided if Internet traffic is routed through the required infrastructure.

Compliance

The client must be fully compliant with all Internet Corporation for Assigned Names and Numbers (ICANN) rules and regulations, and any applicable internet registrar procedures.

System configuration

The Web Application Firewall as a Service operates as a reverse proxy and can only be provided if the Web Sites to be protected are published (public DNS) and Internet traffic is routed through the required infrastructure.

Similarly, for Infrastructure DDoS protection, a public assigned BGP address space (ASN) is required.

The secured requests are passed on to the origin servers largely unaltered. In particular, the 'Host' header and the original transport protocol (HTTP or HTTPS) remain the same.

The client will need to make the following changes to utilize the Service:

- DNS changes to route traffic through the Service's network
- Firewall and ACL changes to only allow communication between the client's origin server and the Service's IP addresses. This will ensure the only path to the origin server is via the protected service (e.g. not bypassed)

Note: Client is responsible to manage the devices and configurations, where the device is not an NTT Ltd. managed device.

3 Core Service Elements

3.1 Hours of Operation

WAF as a Service is delivered through the NTT Ltd. Operations Centers (SOCs), which operate 24 hours a day, 7 days a week.

3.2 Security Operations Centers (SOCs)

NTT Ltd. will deliver the WAF as a Service from its SOCs. NTT Ltd. may
at its sole discretion deliver services from any of its SOCs, and Client data may be held in any of the SOC and NTT Ltd. Infrastructures unless there is prior agreement and approval between NTT Ltd. and the Client.

The Client will be provided with the contact details of relevant SOCs through the Service Transition process.

3.3 Client Portal

For the WAF as a Service offering, Clients have access to the following web-portals:

- The NTT Ltd. Portal
- The WAF as a Service Portal

In the Standard Management (default) set up, all user lists and rights are owned and managed by NTT Ltd. for all portals.

3.3.1 NTT Ltd. Portal

NTT Ltd. Portal is a globally available web-based application, which allows Clients to interact with, manage, and monitor the MSS.

3.3.2 WAF as a Service Portal

A globally available web-based application provides specific management, reporting and role-based access for the Service configuration and features including:

- Traffic
- Security
- Performance
- Real-time statistics

This portal is only available for WAF as a Service Clients.

NTT Ltd. configures the WAF as a Service portal for the Client with all relevant service information.

An account is created for the nominated service administrator verified by the Client.

Clients can be assigned administrative or reviewer entitlements based on their management service deployment.

In a Standard Management (default) set up, the Client will be assigned a reviewer role (Read-Only).

In a Co-Management set up, the Client can be assigned specific permissions to configure and manage the policy of the Service through the Portal.

In a Co-Management set up, specific conditions apply.
For further information refer to Co-Management (3.5.2.)

3.4 Language support

The WAF as a Service is provided in English language only, unless there is prior agreement and approval between NTT Ltd. and the Client.

Note: the WAF as a Service Portal is available in English.

3.5 Management Options

NTT Ltd. offers two types of management for the Service configurations:

- Standard Management (default)
- Co-Management
- The management type of the Service is selected by the Client in the Planning phase.

3.5.1 Standard Management (default)

NTT Ltd. maintains all configuration items in the Service.

The Client can be provided with up to three (3) read-only accounts to access configurations within scope.

If the Client expects more (>3) read only accounts, NTT Ltd. will create a read-only account via MACD consumption.

NTT Ltd. will create one administrator account for the client and will securely store the credentials and password. In the event of an emergency where NTT Ltd. is unable to make a Change or access the configurations/management infrastructure, the Client nominated service administrator will be provided with the credentials and password.

Each time the Client uses the administrative account, NTT Ltd. will reset the account with a new password.

3.5.2 Co-Management

Available on request at no cost, NTT Ltd. and the Client and/or its nominated third party and/or an NTT Ltd. Group Operating Company have access to the in-scope configurations with the ability to make updates and configuration changes.

In a Co-Management set up, Client can be assigned a role and may configure and manage the WAF as a Service Portal policies, configuration, view data and statistics.

Client will not be granted access to any configuration item that is not already included in the record of entitlement / contracted scope.

In Co-Management Client is responsible for maintaining user accounts and rights for in the portal. For more information about portal, refer to the NTT Ltd. Portal section 3.3.1 in this document.

Note: The Management option must be selected during 'Planning' phase. Clients cannot change this selection after the service 'Staging' phase is complete.

The Client acknowledges only appropriately-trained and skilled WAF engineers will be granted administrative account rights to perform changes in a Co-Managed environment.

In a Co-Managed scenario, specific conditions and responsibilities apply as outlined below:

1. Co-management is only available as an option when the client has an appropriately-trained and skilled WAF engineer
2. WAF configuration and policy changes can only be made by the specific client's engineer, outlined within the CSSD or added by raising a service request via the NTT Ltd. Portal
3. In order for NTT Ltd. to provide effective support the Client shall:
   a. Notify NTT Ltd. in advance of changes being made to include scheduling and scope of changes being made to avoid 'lost transaction' or collision of change work
   b. Record all changes to be made via a Request for Change within the NTT Ltd. Portal
   c. If applicable and upon completion, the Client shall provide a report/status update from their internal Change Management process to ensure NTT Ltd. is aware of all the changes occurring to the configurations

Clients accept any exception that may arise due to deviation from, or circumventing the processes described may result in an unstable configuration(s) and service. Accordingly, Clients release NTT Ltd. from any liability resulting from outages, misconfigurations, exposures, loss of business, or other negative impacts directly related to changes implemented directly by Clients.

3.6 Communication

3.6.1 Email

For security and data privacy reasons, email notifications from NTT Ltd. will only contain minimal information to notify Clients about creation of, or updates to, Incidents, Service Requests, Changes and Problems. Such emails from NTT Ltd. shall not contain any sensitive information apart from the appropriate ticket reference number (and where possible not to disclose any private information a short description of the ticket).

Clients may send emails relating to new or existing Incidents, Service Requests, Request for Changes and Problems to NTT Ltd.. In the case where no reference number is provided as formatted by NTT Ltd., NTT Ltd. shall create a new Incident, Service Request or Request for Change with a short description based on the subject line provided.

When a Client is replying to an email with an existing reference number (as provided by NTT Ltd. and unchanged by the Client), the message body text shall be copied (upon receipt) to the timeline of the relevant Incident, Service Request or Request for Change and shall be marked as updated by the customer and waiting on NTT Ltd.'s further input. For security reasons, if Clients wish to send sensitive information to NTT Ltd. or provide approval workflow pertaining to an existing or new incident or request, they must do so using the secure NTT Ltd. Portal.

Note: WAF as a Service - Standard, email notifications of events from the service will include real-time email notification details of threats. These settings can be modified (turned off) in notification settings of the WAF as a Service portal. Refer to section 5.2.1 for further details.

File attachments

Diagrams, images, PDFs, executables and any other attachments must not be attached to any Incident, Service Request or Request for Change via email. Where file attachments are necessary, the Client must log in to the NTT Ltd. Portal and attach the file securely through their web browser connected to the NTT Ltd. Portal.

3.6.2 Telephone

NTT Ltd. SOC staff may contact Clients and Clients may contact NTT Ltd. SOCs by telephone. In both cases an authentication shall be completed to verify Client identity.

3.6.3 NTT Ltd. Portal

Unless otherwise stated and agreed, all other communications originating from NTT Ltd. SOCs shall be secure and follow security best practices via the NTT Ltd. Portal.

3.6.4 ITSM (Service Management) Tool

NTT Ltd.'s ITSM manages all Incidents, Service Requests, Change Request, and Problems following ITIL wherever appropriate. Access is provided to appropriate NTT Ltd. staff.

3.6.5 Engineering

NTT Ltd. MSS Infrastructure

NTT Ltd. utilizes a regional based infrastructure with security built in by design. The infrastructure is highly resilient and secured using best practice methodologies tools and techniques.
It is fully managed by NTT Ltd. Global Services staff and monitored using our platform (Global Managed Security Services Platform).

3.7 Escalation Management

NTT Ltd. utilizes well-defined processes, procedures, and responsibility assignments for Client escalations. To escalate a configuration Incident, Request for Change or Service Request, the Client may telephone or email the service desk (quoting the reference number).

NTT Ltd. may downgrade an escalated Security Incident, Incident, Change Request or Service Request if it is being managed to a scheduled timeframe, or resolution has been provided to the Client and is in the process of being tested.

If the Client initiated the escalation, NTT Ltd. will obtain the Client's approval prior to downgrading an escalated Security Incident, Incident, Change Request or Service Request.

Clients may request their Incident, Service Request or Problem be escalated to a higher priority at any time provided that they give sufficient justification. Upon review, the SOC manager shall be responsible for agreeing any urgent change.

3.8 Health and Availability Monitoring

The SOC monitors the overall Health and Availability of the Service.

The Client will be notified and kept up to date of issues with overall health and availability via the Incident ticket available on the NTT Ltd. Portal.

Client responsibilities include Health and Availability of their Internet connection, web application sites, third-party hosting environments and SaaS applications.

***Note**: NTT Ltd. is not responsible for Health and Availability of Imperva's Application Delivery Cloud (Incapsula) , Network DDoS.*

NTT Ltd. informs the Client about any planned and scheduled maintenance or probable outage of the Service via Incident ticket available on the NTT Ltd. Portal. During these periods, no OLA applies.

Refer to the Operational Level Agreement for more information.

4 Service Transition

Service Transition is executed in five phases, these are:

1. Engagement
2. Planning
3. Staging
4. Integration
5. Go-Live

The five phases and activities and procedures within them, ensure a consistent approach to management and completion of the transition and a framework for governance and communication. During the first four phases of the Service Transition period there will be no alerts, incidents, or cases generated for customer review and triage.

4.1 Engagement Phase

To initiate the Service Transition, the Account Manager will submit a Purchase Order (PO) along with the Pricing Information from the approved quotation, a High-Level Design document, and the Client Security Services Detail (CSSD) to NTT Ltd.

- Purchase Order (PO)
- Pricing Information
- Client Security Services Detail (CSSD)
- High Level Solution Design

NTT Ltd. reviews the provided documentation and confirms that all the requirements for commencement of the transition have been met.

A Kick-off meeting is held to communicate the Transition Process, the project tasks, roles and responsibilities and introduce the key stakeholders.

The Engagement Phase is expected to take 12 business days and can be accelerated if the Client provides completed and accurate documentation when submitting the Transition Service Request. For WAF as a Service, the following aspects of the design should be reflected in the High Level Design document.

- Connectivity (e.g. Internet connection(s))
- Web Site (URLs) requiring protection, business function provided by web sites, location of sites
- DNS architecture for public facing sites requiring protection
- Denial of service for Web and or Infrastructure protection details
- Other Metrics as required for the scope (SSL inspection, network bandwidth to sites, white list, black list, etc.)
- Special requirements (results from Penetration audits, custom rules, alerts)

Failure to provide this level of detail at the start could delay the transition of the service to an active state.

4.1.1 Engagement Phase Activities

The key activities during the Engagement Phase are as follows:

- Receive the Service Transition Request and PO and respond within three business days
- Review provided documentation within six business days
- Provide feedback and confirm content is complete and aligned to the Service Order
- Assign a Service Transition team including allocation of an NTT Ltd. Client Service Manager (CSM)
- Create the Draft Service Transition Project Plan, including timeline and constraints within 10 business days
- Arrange a Kick-off meeting within 12 business days (if documentation is complete and confirmed)

NTT Ltd. Service Transition

- NTT Ltd. Portal account(s) configurations
- WAF as a Service Portal account(s) configuration

4.1.2 Engagement Phase Deliverables

The deliverables provided during the Engagement Phase are as follows:

- Purchase Order Approval
- Kick-off meeting (face to face or call)
- Draft Service Transition Project Plan, including timeline, standard risks and issues
- Client credentials for NTT Ltd. Portal
- Client credentials for WAF as a Service Portal
- Client Entitlement in NTT Ltd. ITSM

4.2 Planning Phase

The Service Transition Planning Phase validates the provided documentation and locks down the transition plan, scope, and timeline. The Planning Phase is expected to take six business days.

4.2.1 Planning Phase Activities

The key activities during the Planning Phase are as follows:

- Agree on final architecture, scope and service levels
- Low level design produced and documented
- Client Approval of Final Service Transition Plan
- Confirm Services Delivery Model, including Incident Management and Steady State Governance

4.2.2 Planning Phase Deliverables

The Final Service Transition Plan (including timeline, risks, and issues) is provided as a deliverable during the Planning Phase.

4.3 Staging Phase

The Service Transition Staging Phase establishes the primary service elements for NTT Ltd. to provide the service. The Staging Phase is expected to take up to 12 business days.

4.3.1 Staging Activities

The Final Service Transition Plan (including timeline, risks, and issues) is provided as a deliverable during the Planning Phase.

NTT Ltd. Tech Ops

- Log Transport Agents (LTAs) set up and configuration
- MSS infrastructure and WAF as a Service cloud infrastructure integration
- SOC infrastructure preparation

NTT Ltd. Service Transition

- WAF as a Service initial configuration, tenant setup.

Note: Activation of Web sites during transition stage includes up to 20 domains. Further sites may be added via MACD (refer to Section 14 Usage table) once the Service Transition Deliverable Acceptance has been completed.

Client

- Configuration of Client infrastructure to support connectivity and authentication
- DNS configuration updates
- SSL certificates
- Client accounts in NTT Ltd. portal
- For infrastructure protection, additional tasks as directed by SOC (e.g. BGP configuration) – may take up to 14 days based on standard configuration.

Client/Professional Service

- Define/Design the WAF as a Service policy for all selected service elements including:
  - If not already provided, specifying policies to be blocked/allowed/alert only
  - Creation of white / black lists: specific URLs, Good Bots, etc.

Note: Client is responsible for performing and signing off User Acceptance Test (UAT) for the WAF as a Service initial policy prior to 'Go live'.

NTT Ltd. SOC

- WAF as a Service Policy Configuration

4.3.2 Staging Deliverables

The deliverables provided during the Staging Phase are as follows:

- Client connectivity
- Client authentication
- Client Policies are verified
- Test results

4.4 Integration Phase

The Service Transition Integration Phase completes the required technical service elements for NTT Ltd. to provide the service. It includes configuration of Monitoring (Enhanced Service Level only), advanced features for log collection and policy/device management, and final Portal and ITSM integration.

Additionally, during the Integration Phase, the NTT Ltd. Client Service Manager (CSM) conducts the Welcome meeting and Portal training with the Client.

The Integration Phase is expected to take 10 business days.

Following the Welcome meeting, the CSM becomes the Client's interface into the NTT Ltd. services.

4.4.1 Integration Activities

The key activities during the Integration Phase are as follows:

- Final validation of connectivity/log flow towards the SOC
- Final validation of the WAF as a Service readiness
- Log(s) and service testing and final verification (Enhanced Service Level)
- CMDB instantiation (where appropriate) for Contracts, Entitlements, Assets and CI's
- Test ticket creation and validation to NTT Ltd. ITSM via phone, email and NTT Ltd. Portal by Client
- Final validation of reachability to Client POC and Client's accounts access to the Portals
- Quality assurance review and activation of the service(s)
- Risk and Issue documentation
- MSS SOC Welcome meeting or call with Client (NTT Ltd. decision)
- NTT Ltd. Portal training meeting or call with Client (NTT Ltd. decision)
- WAF as a Service Portal training meeting or call with Client (NTT Ltd. decision)
- Confirm Service Activation Date (in phases, if required), Billing Date, and OLA start date

4.4.2 Integration Deliverables

The deliverables provided during the Integration Phase are as follows:

- Client Welcome meeting and Portal training
- Service Activation Date
- Confirmation of WAF as a Service Readiness
- Client review and acceptance of the Risk and Issue Register

4.5 Go-Live Phase

The Service Transition Go-Live confirms that the service is live and closes the Service Transition Project. The Go-Live Phase is expected to take six business days.

4.5.1 Go-Live Activities

The key activities during the Go-Live Phase are as follows:

- Operational Check List review by SOC
- Conduct Service Transition Plan closure review meeting or call with Client (NTT Ltd. decision)
- Review all remaining open action items including lessons and risks/issues to be considered for Steady State (going forward)
- Receive Client Service Transition Plan closeout final approval

4.5.2 Go-Live Deliverables

The deliverables provided during the Go-Live Phase are as follows:

- Risks/Issues Register (if any)
- Commencement of service and Billing
- Lessons learnt (if any)

4.6 Service Transition Deliverable Acceptance

The Service Transition is considered complete on the Service Activation Date and after any Go-Live deliverables is provided. The deliverables are considered as being accepted at the completion of next phase. The Client will close the Service Transition by agreeing to the closure of the parent ticket in the Service Management tool.

5 Service Features

The following features are available in the service:

- Monitoring
- Web Application Firewall
- WAF policies
- Security Policies
- SSL support
- Two factor authentication
- DDoS protection for Infrastructure
- Content Delivery Network (CDN)

5.1 Monitoring

Two levels of monitoring can be selected based on the contract service level.

- **Standard** service is designed for organizations with standardized compliance requirements across a core set of security technologies.
- **Enhanced** service is designed for organizations with custom compliance requirements across a broad set of security technologies.

5.1.1 Standard

The Standard service is best suited to clients who do not require customization of events or correlation from other NTT Ltd. Services. The events that are generated are not processed by NTT Ltd..

Security Analyst Interaction

The service utilizes automated detection for high confidence Security Incidents, no further Security Analyst verification is performed.

Client Notification

Clients are notified directly from the cloud service via the e-mail address defined in the CSSD.

Clients may select from the following categories for automated real-time email notification:

- Website threats
- Load balancing alerts
- Infrastructure Protection status

Nominated client administrator(s) can choose to receive via email a weekly report of summary activity in HTML or download as PDF.

Portal and Reporting

- Clients will have access to the WAF as a Service portal that includes access to 90 days of Events (All)
- Clients will have the ability to generate a PCI report or define a schedule to email (weekly, monthly, quarterly)
- Clients will have access to the NTT Ltd. Portal for Service Management purposes.

Note: No events or security reports from the Standard service will be presented in the NTT Ltd. Portal.

5.1.2 Enhanced

The Enhanced service is best suited to clients who require customization of alerts or correlation from other NTT Ltd. Services. The events that are generated from the cloud service are further processed by the MSS.

The service uses customized rules and an anomaly-based security detection and compliance profile to identify and can report on the following categories of Security Incidents:

- **Compliance** - Events that indicate a deviation from a pre-defined baseline of a regulatory body's definition of compliance controls.
- **Security Best Practices** - Events that indicate a deviation from a pre-defined baseline of NTT Ltd.'s definition of security best practices.
- **Business Policy Compliance** - Events that indicate a deviation from a pre-defined baseline of an organization's custom business policy compliance requirements.

To ensure service quality, NTT Ltd. will continuously make detection tuning decisions based on the validity and relevance of service generated Events and Security Incidents. WAF as a Service - Enhanced includes the following:

- Use of the NTT Ltd. Standard Rule sets defined for WAF as a Service.
- Up to fifteen (15) Standard or Compound Rules can be developed and implemented annually.
- Additional Standard or Compound Rules can be purchased via the Move Add Change Delete (MACD) process at a rate of 6 MACDs per rule.
- Development of new Analyzers can be purchased via the MACD process at a rate to be determined based upon the level of effort associated with the development of the Analyzer.

Security Analyst Interaction

Enhanced service level utilizes automated detection for high confidence Security Incidents, with Security Analyst verification for custom high severity business use cases.

Client Notification

Security Incident Reports are created by Security Analysts in the Enhanced service level.

Clients are notified based on Client's selection of NTT Ltd. supported notification options, including e-mail and phone calls. Additionally, cases may be viewed on the NTT Ltd. portal (ITSM).

Portal and Reporting

Clients will have access to the NTT Ltd. web portal that includes access to 90 days of Events and Security Incidents processed by the MSS. Clients will have access to monitoring and compliance reporting in the NTT Ltd. Portal.

Clients will have access to portal and reporting features in section 5.1.1. Development of custom reports is not included as part of the service.

5.2 Web application security

The Service provides PCI-DSS certified, cloud-based web application security, through the implementation of Web Application Firewall (WAF).The WAF will be used to secure key assets against known and emerging threats. The Service detection and mitigation capabilities covers web application and infrastructure attacks, including advanced bot attacks, web defacing, brute force attacks, sophisticated injections, and cross-site-scripting (XSS) site scraping.

This service feature is priced on number of web sites (domain / URLs) and total network bandwidth (for all sites).

5.2.1 Web Application Firewall (WAF)

The WAF protects the client against the most critical web application security risks, such as SQL injection, cross-site scripting, illegal resource access, remote file inclusion and other OWASP top 10 threats. Security experts behind the Service ensure optimum protection against newly discovered vulnerabilities to prevent disruption to the client's applications and improve website performance.

This service element implements an enterprise-grade and PCI DSS-certified WAF.

Once this feature is selected, other service elements, as shown below are included and customizable.

5.2.2 WAF policies

WAF rules are deployed to protect web applications against advanced threats. Customized security rules can also be implemented to allow tighter enforcement of organizational security policy. These customizations can be based on many parameters including, browser details, IP Addresses, header information, web page details, cookies and more.

The actions that can be taken on these requests include alerting, blocking (user, IP Address, request) or ignoring a request, session or specific IP Address indefinitely or for a specific period of time. The Service can also identify human interactions by providing a CAPTCHA mechanism.

Threats

The service identifies and categorizes threats into the following:

- Backdoor Protection
- Remote File Inclusion
- SQL Injection
- Cross Site Scripting
- Illegal Resource Access
- DDoS

Based on the policy configured, each threat type may be handled differently, e.g. Alert only or Block IP Address. These settings can be applied on site basis. Exceptions / whitelists can also be applied where required.

Custom Rules

Rules in the service allow clients to implement custom policies aligned to business requirements. Rules are applied at the web application site level and can be created perform the following for security specific or application delivery use cases:

- Prevent bots from accessing a site's registration form
- Restrict access to a specific part of an application based on IP address
- Limit the rate of requests to a website
- Manipulate traffic routes and redirects
- Control a request's URL structure, headers and cook

Rule actions for security include: block, alert, require additional authentication (CAPTCHA, JavaScript and Cookie).

Rule actions for application delivery include: redirect URL, rewrite or forward traffic.

Rules created will appear in event logs when triggered and revision control allows rollback of previous versions.

5.2.3 Security Policies

Bot mitigation

Bot mitigation blocks known bad or suspicious bot activity such as comment spam, scraping and vulnerability scanning, while making sure that legitimate bots such as Google, Facebook can freely access the client's website. In addition to the improved security, blocking malicious bots also improves website performance as they account for up to 50% of all website traffic.

This service element provides several options for handling bad and suspected bots. The client can choose to receive an alert, block the bot, or challenge it with a CAPTCHA test to ensure that the visitor is human. Bad bots can be blocked at both the bot signature (user agent) and IP address levels.

White and Black Lists

The service supports both Black and White lists. Black lists are categorized by:

- Geolocation (Countries)
- URLs
- IP addresses / subnets / ranges
- Exceptions to the Black lists can also be added.

White list is based on either single or multiple IP Address, IP ranges or subnets.

5.2.4 SSL support

SSL support allows the Service to become the intermediate for all HTTP over SSL traffic targeted to the client's web applications. By allowing the Service to be an intermediate, HTTP over SSL traffic can be inspected and security applied to the encrypted traffic heading towards the client's web applications.

The Service is compliant with PCI-DSS and uses industry security techniques for secure key handling.

Custom certificates

Custom certificates allows the client's web site to use the client's own SSL certificate while having SSL traffic inspected.

Note: NTT Ltd. does not manage the certificate (e.g. monitor for expiry, manage public-private key, revoking certificates etc.).

5.2.5 Two factor authentication

The 'Login Protect' feature provides a two-factor authentication overlay solution for any website or application that requires strong authentication mechanism. Login Protect does not require plugin install, code changes or integration with a third party authentication product. Login Protect provides seamless integration and can be introduced as an additional authentication prompt to enforce strong authentication and appropriate access.

For example, access to sensitive pages, site administration, partner access, access to unpublished content, etc.

The service option supports the following authentication methods:

- Email
- Text message (SMS)
- Google Authenticator mobile application

This service element provides the client with five (5) Login Protect accounts.

Additional Login Protect accounts can be provided at an additional charge and configured using MACD service units.

5.3 DDoS protection for Infrastructure

DDoS protection for infrastructure helps to protect key infrastructure components across entire subnet ranges or individual IP addresses. All incoming network traffic to the protected IP subnets is inspected and filtered in real-time. Malicious traffic is blocked, where only legitimate traffic is forwarded to the enterprise network via GRE tunneling.

If subnets are being protected, the Service acts as the service provider and advertises all protected IP ranges to the internet. All traffic from the internet will be re-routed through the Service's scrubbing centers, using BGP announcements.

This feature (priced) is available as '**Always on**' or '**On-demand**', the number of tunnels (connections), the total amount of clean bandwidth required.

Infrastructure protection services require a full C-class prefix and border gateway protocol (BGP) routing capability.

Infrastructure protection plans include up to 32 C-class prefixes and 8 connections (GRE tunnel, Equinix cloud Exchange, Cross Connect, or Internet Exchange).

Clients whom require Infrastructure DDoS and do not own a full public Class C can utilize IP Protection. Refer to section 6.1.4

Note: This feature can be included without any WAF features.

5.4 Content Delivery Network (CDN)

CDN consists of a network of data centers located across the globe that delivers full site acceleration. The service elements in CDN are included as part of web application security service elements. On average, users will experience 50% acceleration in web site browsing experience. The origin web servers will also benefit from a reduction in web bandwidth consumption between 40% and 70%. This is achieved through a combination of application-aware traffic analysis, dynamic profiling and intelligent caching technologies. The Service's CDN maximizes cacheable content while ensuring that the most frequently accessed resources are served from memory.

Caching and policies

CDN caching policies are fully customizable to provide the client with granular control over its users' web experience. The following pre-defined caching modes are available:

- Disable caching: no caching is performed; all content is forwarded from the origin web server.
- Static only: only content that has been marked as static (using standard HTTP headers) will be cached.
- Static and dynamic: the Service applies a learning algorithm, which dynamically profiles the site and identifies what content should be cached.
- Aggressive: all site content is cached. A time period (in minutes, hours, days or weeks) can be set to determine how often the cache is refreshed.

Content optimization

Content optimization uses many content and networking optimization techniques to accelerate the web site browsing experience and minimize bandwidth utilization. These techniques include content 'minification', 'on-the-fly' file compression, image compression, session reuse optimization and TCP optimization and connection pre-pooling.

This feature is included with the service at no charge when purchasing Web Application Security.

6 Service Options

The following (priced) options can be added to the service as required with prerequisite features (section 5.2, 5.3).

6.1 Distributed Denial of Service (DDoS) protection

6.1.1 DDoS protection for websites

DDoS protection for websites provides security for large and sophisticated DDoS attacks against key websites on network, protocol and application levels (layers 3, 4 and 7). This service element is built to handle volume-based attacks, such as SYN flood and domain name server (DNS) amplifications. This service element mitigates sophisticated application layer attacks by implementing advanced and progressive challenge mechanisms.

The DDoS protection mechanism can be set to Automatic where threats are transparently mitigated based on predefined thresholds. Alternatively, this configuration can be set to on, where all DDoS rules are enabled, or off (disabled). Whitelists can also be set.

Advanced settings also permit customization of thresholds, challenge for unknown clients.

When included, the service provides an unlimited amount of protection and based on the amount of clean bandwidth required for the web sites protected.

6.1.2 DDoS protection for DNS

This service element safeguards domain name servers (DNS) from DDoS attacks and is deployed as an always-on service which automatically identifies and blocks attacks seeking to target DNS servers. This feature also accelerates DNS responses. This service feature forwards legitimate DNS requests to the client's original name servers, ensuring that existing processes for managing name servers remain unaltered.

Clients receive protection for up to 10 DNS zones with their Web DDoS. Protection for additional zones may be added at an additional cost.

6.1.3 Infrastructure Monitoring (On Demand Infrastructure Protection)

The Infrastructure Monitoring service is available as an option with On-Demand deployment of Infrastructure DDoS protection. With this option the service automatically detects DDoS attacks and facilitate activation of the service by providing the client with notification. The service achieves this by monitoring the origin network edge routers and firewalls, providing packet level visibility for both clients and operations team.

The Monitoring service supports Netflow (v5,9,10) and sFlow.

6.1.4 Single IP Protection

If individual IP address are being protected (Edge IP), the Service provides an always-enabled protected IP address for any backend services. These are ideal for services hosted in cloud infrastructure, email, FTP or other non-web or non-DNS services where the Client does not possess a public routable Class C network range.

Edge IP (Protected IP over TCP/IP)

Edge IP can be used in place of a Dedicated Network for the use case of DDoS protection for TCP services where non-HTTP traffic needs to be passed to the origin server with no WAF inspections. E.g. proprietary protocols.

Edge IP provides Layer 3/5 volumetric DDoS for TCP whereby the origin server is resolved to a CNAME and an Anycast IP address is assigned. At least one of the identified IPs must respond to ICMP to show status as UP.

Note: This service can be added to 'Always on' Infrastructure Protection (DDoS Protection for Networks) plan or a Web DDoS Protection (DDoS Protection for Websites) plan.

IP Protection (Protected IP over GRE)

Also deployed as an always on type of service, a GRE tunnel is established between the client network and Imperva network. To provide IP level protection, Incapsula 'leases' an IP address out of its own range to the client and acts as the client's ISP (although the client is still required to get additional IP addresses from an ISP to which clean traffic is routed).

The GRE tunnel can be connected to different types of equipment on the client's side, depending on the specific topology of the client's network. Such devices may include routers, firewalls, load balancers and Linux servers (physical, virtual, and cloud instances).

6.2 SIEM / Log Integration

This Client managed service element securely transmits logs from the service via a number of supported formats (CEL, LEEF, W3C) and supported SIEM vendors.

Detailed security logs are collected and sent in near real-time to the Client device to permit long term data retention, detailed investigations and leverage internal use cases that may be developed as part of an on-premises SIEM solution.

Logs that are collected include:

- Security logs, which provide a detailed alert for each suspicious event detected by the service. All logs include site and account ID references.
- Access logs, specify every request and response sent between the client's web server and the service. This is all the traffic that would have been sent between end users and the client's origin server, including traffic served from the service's cache.

A number of tools are provided for clients such as API integration, log encryption and predefined SIEM packages for leading OEM's.

The Client is responsible for all configuration of their SIEM. NTT Ltd. will make Logs available in the supported formats.

This priced option may be added to WAF as a Service – Standard (packaged with WAF as a Service – Enhanced).

6.3 Attack Analytics

Attack Analytics is a tool to help speed up the security investigation of WAF alerts. It provides a comprehensive view of attacks and attackers targeting your resources. The Attack Analytics service aggregates and analyzes your account's security alerts, identifies common characteristics, and groups them into meaningful security incidents.

Attack Analytics takes events from both the On-Premises WAF (formerly SecureSphere) and the Cloud WAF (formerly Incapsula – this service) and analyzes them to identify related events.

Note: Attack Analytics, includes SIEM / Log integration.

6.4 Dedicated Network

A dedicated network provides the client with a unique static IP address for a website. Once a dedicated network is allocated, it is never shared among other clients. This provides additional control over your TLS certificates.

Typical reasons to use a dedicated network include:

Using a dedicated network is recommended to support the following use cases:

- Non-HTTP traffic needs to be passed to the origin server with no WAF inspection (e.g., proprietary protocols).
- HTTP/S traffic needs to bypass WAF inspection and tunnel directly to a specific origin server (impacting all domains sharing the IP).
- Non-SNI clients, such as APIs, need to be served with a custom SAN certificate for multiple customer domains.

- Non-SNI clients need to be served with a custom cipher-list or TLS versions.
- Only your domains are allowed to appear on the Imperva-generated SAN certificate list, such that no other brands or competitors will share the same certificate.

6.5 Load balancing and failover

The load balancing and failover service elements provide Layer 7 load balancing and failover from the cloud to support the client's application and server availability deployed in data centers and cross-data centers. This feature is particularly useful for applications and servers deployed in a hybrid cloud or multi-cloud environment.

Load balancer allows clients to manipulate traffic by using application delivery rules.

This priced option is only available when selecting Web application security feature.

6.5.1 Single data center load balancing

Single data center load balancing supports a wide variety of load balancing and traffic distribution methods to maximize performance and distribute the load across a number of servers within the same data center. This supports maximizing application performance and reducing server load.

Sophisticated traffic distribution algorithms are available with or without a 'persistence override' option. Real-time server health and performance checks are used to rapidly detect outages and eliminate downtime. In the event of web server failure, the Service stops routing traffic to the failed server. As soon as the web server resumes operation, traffic will be re-forwarded to the server.

6.5.2 Global Server Load Balancing (GSLB)

GSLB supports automatic failover, selection between multiple sites to enable high availability, ensure consistent performance in multiple geographies, and accelerate disaster recovery. Leveraging a global CDN, GSLB is offered through performance-based (i.e. user is assigned to data center with the best connection time), and geography-based mechanisms (i.e. user is assigned to data center according to his geographic location).

6.6 Investigator – Enriched and Aggregated Log Search

WAF as a Service Clients have the option to include NTT Ltd. Investigator log search capabilities. Investigator provides the Client access to an interface to perform historical log searches.

This priced option is only available with *5.1.2 Enhanced.*

6.7 Secure Long-Term Log Storage

WAF as a Service Clients have the option to purchase secure long-term log storage and of logs.

By default the service will only store events for up to 90 days.

This priced option is only available with *5.1.2 Enhanced.*

7 Service Delivery Management

7.1 Incident Management

Incident Management focuses on responding to any unplanned interruption to service and operation to minimize any impact to business operations and ensure service quality and availability.

7.1.1 Incident Generation

Incidents may be generated by the SOC or Client raising an Incident related ticket via the NTT Ltd. Portal or telephone call via the service desk.

For Incident tickets raised via the NTT Ltd. Portal, with a provided Impact and Urgency, the SOC team will validate the ticket and reserves the right to modify the Impact and Urgency as deemed necessary.

For Incidents raised via a telephone call to the SOC, the SOC will create an Incident ticket on behalf of the Client with the relevant Impact and Urgency.

7.1.2 Incident Diagnosis

Incidents are managed based on the priority of the Incident ticket raised on the NTT Ltd. Portal. Priorities are calculated based on Impact and Urgency of an Incident ticket, leading to a specific priority. Priorities are defined as Major, High, Moderate and Low as outlined in the table below.

Incident Diagnosis		Urgency/Impact		
		1 Work blocked	2 Work degraded	3 Work not affected
Scope	1 Organization wide	Major=P1	Major=P1	High=P2
	2 Multiple Departments	Major=P1	High=P2	Moderate=P3
	3 Single Department	High=P2	Moderate=P3	Low=P4
	4 Individual	Moderate=P3	Low=P4	Low=P4

The SOC will triage the Incident to assess the priority. Incidents will be assigned to the appropriate SOC engineer who will investigate and analyses further to identify a correction plan to resolve the Incident. Clients are notified of updates to an Incident via the NTT Ltd. Portal and any restoration plan to resolve.

7.1.3 Incident Resolution

The SOC will work to resolve incidents and move to a 'resolved' state to allow customers to confirm resolution. Incidents will then remain in a resolved state until:

- Client confirms resolution and the incident will be moved to a 'Closed' state
- Client confirms incident is not resolved, the ticket will be moved back to a 'In Progress' state
- Client does not respond, and the incident will be auto closed after 3 days

NTT Ltd. will keep Clients updated on any Incident resolution plans via the NTT Ltd. Portal. Resolution targets are outlined in the NTT Ltd. Operating Level Agreements – Managed Security Services.

7.1.4 Incident Reporting

Clients are notified of all Incidents via a notification email which contains very minimal information for security purposes, with the full Incident details only available via the NTT Ltd. Portal.

7.2 Service Request Fulfilment

Service Request Fulfilment focuses on request for information, advice, a change or access.

7.2.1 Service Request Management

Service requests are managed through ITIL process and raised via the NTT Ltd. Portal. Attainment of various key performance metrics are tracked, monitored and reported within NTT Ltd. on a monthly basis.

Request for Information

Clients may request information through the NTT Ltd. Portal about the performance or other aspects of in-scope items/services where applicable. NTT Ltd. shall deduct the commensurate number of MACD credits (if applicable) and provide the information in the Service Request.

Service Request Reporting

All Incidents, Service Requests, Problems or Changes are recorded in the ITSM system and reported back through the NTT Ltd. Portal.

Project Oriented Requests

NTT Ltd. will charge, and the Client agrees to pay, the then-current applicable hourly rates for work associated with PORs. If any Change performed by the Client results in adverse effects and requires remediation work be performed by NTT Ltd. to restore the software/configuration item to proper working service, the Client agrees to pay NTT Ltd. the then-current Engineering hourly rate to return the 'in-scope' device to normal operating run-state.

7.2.2 Move, Add, Change, Delete (MACD) Fulfilment

Service Requests are administered through a Move, Add, Change, Delete (MACD) service unit model and are requested via the NTT Ltd. Portal.

MACD unit usage is tracked by NTT Ltd. and is included within any scheduled service reviews to ensure the client account is operating in line with MACD availability. Should MACD unit balance drop below a certain threshold the client will be notified for purchase of additional MACD service units, however will still be entitled to raise any changes as required.

MACD service units are bundled offerings with the option to purchase additional MACD units. MACDs are deducted in the execution of any service requests pertaining to Request for Changes of configuration items with the Client's approval. The number of MACD service units deducted per service request is based on a predefined list of standard tasks that NTT Ltd. has derived assessing level of complexity to route accordingly to an appropriate SOC engineer.

Where the usage of MACD service units for a service request exceeds 6 hours of effort or for non-standard tasks, NTT Ltd. may charge additional MACD service units or propose a Project Orientated Request (POR) to perform the work on a time and materials basis.

Non-Standard Tasks utilizing MACD Service Units

In the unlikely event that there is not a pre-existing menu item for a Client request, NTT Ltd. considers this a Non-Standard task.

NTT Ltd. will review Non-Standard tasks requested by the Client to determine if:

- What the apparent risk is associated with performing the task
- What impact the change is likely to have
- NTT Ltd. has the appropriate skills to action or implement the task
- Whether the Non-Standard task should become a standard task (based on demand/repeatability)

NTT Ltd. will assess the Non-Standard task to determine the correct
number of MACDs. NTT Ltd. will provide the Client with the number of MACD service units the task will incur for approval to proceed. Once approved by the Client, NTT Ltd. will execute the Service Request for a Non-Standard pre-approved task. No service levels agreement will apply to the execution of a Non-Standard pre-approved task.

7.2.3 Change Management

At a Client's request, NTT Ltd. will implement a request for change to the Service in accordance to an associated MACD task or Non-Standard task outlined in section 14 Appendix A – WAF as a Service Policy Management MACD.

Client sourced requests

Requests for Change must be submitted by valid Client contacts using the Request for Change ticket type within the NTT Ltd. Portal.

NTT Ltd.-Sourced Requests

NTT Ltd. may submit a Request for Change when a Change is necessary to resolve a Problem or Incident.

Change Reporting

All Changes must be reported and tracked via the NTT Ltd. Portal, this includes Co-Managed scenarios.

The party making a Change is required to open an applicable Request for Change in the NTT Ltd. Portal prior to implementation
to ensure coordination between both parties.

Request for Change

All requests for change types follow the NTT Ltd. Change Management process and require approval by NTT Ltd. NTT Ltd. classify each Request for Change as Simple or Complex which corresponds to the number of Service Units utilized by each task. There are 4 (four) types of request for change outlined below.

Normal Change

Normal changes follow a prescriptive process which requires approval (from both NTT Ltd. and Client respectively) before being implemented. Neither Client nor NTT Ltd. is authorized to apply Changes on behalf of the other without documented consent from appropriately authorized individuals (documented within a Change Approver Group on the NTT Ltd. Portal) from both parties via a request for change resident in the NTT Ltd. Portal.

Standard Change

A standard change type ticket is a pre-authorized change that is low risk, relatively frequent and follows a specified procedure. NTT Ltd. is authorized by the Client to apply changes without authorization from the Client when a standard change ticket is raised via the NTT Ltd. Portal, though an NTT Ltd. internal approval process is still valid.

Emergency Changes

An emergency change is considered a request for change that must be implemented as soon as possible, for example to resolve an Incident or implement a security patch. NTT Ltd. will work with the Client during the Change Management process.

Cancelling a Request for Change

The Client may cancel a Service Request up to 2 hours before any scheduled changes being committed to the Service configuration. In which case any MACD credit that would have been deducted shall be cancelled.

If the Client would like to reverse a Change that has already been implemented, the Client must submit a new Service Request for Change via the NTT Ltd. Portal. In which case the commensurate MACD credits shall be deducted for both the original change and any subsequent reversal requested.

Change Implementation

The party making the Change must complete and document the following tasks associated with each Change:

- Ensure that all changes are documented so that the previous change can be identified and reverted back as no rollback feature is available in WAF as a Service.
- Implement and test the change (as far as is possible – testing responsibility is also shared with the Client) to confirm whether the change was successful or not.
- Update NTT Ltd.'s Service Request ticket indicating whether the Change was successful or not.

It is imperative each Change is fully documented via a Service Request in the NTT Ltd. Portal to ensure NTT Ltd. can quickly troubleshoot if/when unanticipated negative consequences arise.

Exceptions

The Client agrees that any exceptions that may arise due to deviation from or circumventing the processes described herein may result in unstable and/or unsecured configuration item(s) and/or non-compliant configuration(s) and accordingly, the Client releases NTT Ltd. from any liability resulting in outages, misconfigurations, exposures, loss of business, or other negative impacts directly related to any Change made by the Client.

The Client agrees any work performed by NTT Ltd. to troubleshoot issues directly attributable to a Client Change is billable at the current NTT Ltd. Security Engineer's hourly rate.

Client Responsibilities

The Client agrees only appropriately-trained and skilled Web Application Firewall engineers will perform Changes in a Co-Managed environment.

The Client agrees that NTT Ltd. reserves the right to bill for incremental troubleshooting work NTT Ltd. performs as a result of:

- Client introduced service impact or outage.
- Client performing work that violates OEM support agreements or leads to in-scope configuration items negatively effecting Client production environment

Change Impact Analysis

As part of the Change design process, NTT Ltd. conducts a Change Impact Analysis process applies to all Requests for Change (pre- and/or post-implementation) (except changes made by the Client under Co-Management). NTT Ltd. reviews Incidents, service requests and documentation regarding Requests for Change in the event of a Co-Managed service and may seek clarification.

NTT Ltd. will conduct a Change Impact Analysis prior to implementation of any Request for Change – including request for change, Patch and Version Management, or PORs to ensure:

- Any change is consistent with security best practices and does not compromise the Clients network, service or that of NTT Ltd.
- Any change is relevant to Client's environment
- Any change can be implemented within the requested timeframe

NTT Ltd. considers the Change Impact Analysis complete and the implementation period will begin, when Client has addressed all issues raised during the analysis (if applicable), and the engineer acknowledges receipt of a valid Request for Change via the NTT Ltd. Portal.

7.3 Problem Management

7.3.1 Problem Identification and Recording

NTT Ltd. follows ITIL best practices for Problem identification and recording. Problem identification is performed in a number of ways and will typically result in a Problem Ticket in the NTT Ltd. ITSM tool and NTT Ltd. Portal. Typically, Problems are derived from a number of factors such as:

- Repeated Incidents of same or similar nature within single Client or across multiple Clients
- Compound problems caused by multiple Incidents of different nature within single Client
- Notification of problem from Vendor
- Lack of timely patch from Vendor to address security vulnerability
- Trend analysis

7.3.2 Problem Reporting

All Problems are recorded in the ITSM system and reported back through the NTT Ltd. Portal.

7.3.3 Solution Identification and recording

Once a problem is identified and recorded, a suggested plan or where appropriate a number of suggested options for resolution will be recorded in the problem ticket.

7.3.4 Solution Implementation

The Client and NTT Ltd. shall discuss and agree on the best or most appropriate solution and implement as a controlled change or series of changes in line with the standard change process.

8 Terminologies and Definitions

Terminologies and Definitions for Threat Detection services are presented in the 'NTT Ltd. - Terminology and Shared Services Reference' document that accompanies this Service Description.

9 Operational Level Agreement

Operating Level Agreements (OLAs) for WAF as a Service are presented in the 'Operating Level Agreements – Managed Security Services' document that accompanies this Service Description.

10 Changes in Service

10.1 Regulatory Change Requirements

If regulatory changes (e.g., changes by a regulatory agency, legislative body, or court of competent jurisdiction) require NTT Ltd. to modify the Services described herein, NTT Ltd. will modify the Services and this Service Description accordingly without diminishing the features, functionality or performance. In the event a modification in response to regulatory changes results in a diminishment of features, functionality or performance, Client agrees in good faith to work with NTT Ltd. to amend this Service Description accordingly and execute any additional agreement which may be reasonable requested by NTT Ltd. to document such amendment.

10.2 Method of Service Delivery

NTT Ltd. reserves the right to make changes to the service, provided these changes do not have a material adverse impact on functionality or performance.

10.3 Unanticipated Network Volume

NTT Ltd. will provide advanced notice if the Client exceeds the maximum volume of data allowance for the Subscription Services specified in the applicable Order. Client agrees in good faith to work with NTT Ltd. to amend the scope of work accordingly. If the Client does not upgrade to the next Subscription Service plan level through submission of an additional Order, overage fees may apply.

The overage fees are calculated by 95th percentile of the Subscription Service bandwidth purchased. If exceeded, the Client can either upgrade contract to next plan or pay overages of USD 400/10Mbps per month in US Dollars.

10.4 Changes in MACD

NTT Ltd. has the right to modify/change MACD lists and associated service unit.

11 Service Exclusions

Unless otherwise stated in Purchase Orders, the services described in this document do not include the following:

- Client staff training unrelated to NTT Ltd. services (NTT Ltd. provides training on the NTT Ltd. Portal and the different functions that Client may use within the portal).
- Software or hardware maintenance (unless otherwise stated).
- Software licensing (unless otherwise stated).
- Software or hardware upgrades (unless otherwise stated).
- Internet link issues troubleshooting.
- On-site forensic services.
- Security policy or procedure establishment.
- Firewall rule set design, validation and troubleshooting.
- Client device / software configuration changes
- Remediation of a Security Incident or attack on a Client's network, server or application.

12 Controlling Terms

In the event of any conflict between the terms of this Service Description and the terms of the Client agreements, then terms of this Service Description shall control.

13 Additional conditions

13.1 Intellectual Property Infringement Claim

Notwithstanding any provision to the contrary in the Agreement, this clause applies to any third party Infringement Claim that the Service as delivered infringes the intellectual property rights of that third party.

'**Infringement Claim**' means a claim by a third party that the Service when used as authorized in the Agreement and as provided by NTT Ltd.:

- Infringes a patent registered in the US, the UK or Australia (each a '**Registered Patent Country**');
- Breaches the third party's copyright; or
- Misappropriates the third party's trade secrets.

a) NTT Ltd. will defend the Client against an **Infringement Claim** and indemnify the Client against all costs and expenses incurred by the Client as awarded by a court of competent jurisdiction arising directly out of the Infringement Claim, and damages awarded against the Client by a court of competent jurisdiction or agreed in settlement by NTT Ltd. in respect of the Infringement Claim ('Losses'), provided the Client:

- Promptly notifies NTT Ltd. of all threatened actions, claim and proceedings of an Infringement Claim;
- Grants NTT Ltd. sole control over the defence and settlement thereof; and
- Gives NTT Ltd. reasonable assistance in response to NTT Ltd.'s requests for assistance.

Client agrees NTT Ltd. has no obligation to defend or indemnify Client for any claim that the Service infringes a patent registered in a country other than a Registered Patent Country.

The obligations in clause **a)** do not apply to Services or parts of the Services (i) that are modified by any entity other than NTT Ltd. or its authorized agents after delivery by NTT Ltd., (ii) that are combined with other services, processes or materials, where the alleged infringement would have been avoided without such use, (iii) where Client continues any alleged infringing activity after being notified of the alleged infringement, (iv) where Client has not used modifications made available to it by NTT Ltd. that would have avoided the alleged infringement, or (iv) where Client's use of the Service is not strictly in accordance with the Agreement.

If NTT Ltd. believes a Service may become subject to an Infringement Claim, NTT Ltd. may at its discretion, either (i) modify the alleged infringing Service to be non-infringing provided the modified Service has substantially the same or better functionality, (ii) obtain for Client a license to continue using the Service, or (iii) terminate the Agreement and all Orders and refund to Client the prorated, unused portion of the fees paid in advance.

THIS CLAUSE SETS FORTH NTT Ltd.'S SOLE OBLIGATION AND CLIENT'S SOLE AND EXCLUSIVE REMEDY FOR ANY CLAIM FOR INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

14 Appendix A – WAF as a Service Policy Management MACD

Task	MACD	Comment	Justification (Notes)
WAF as a Service			
Onboarding	10	WAF Protection Single Website onboarding	2 hours for preparation/communication and 0.5 hour for implementation
Onboarding	16	WAF Protection multiple Websites onboarding (Up to 3 Websites)	2.5 hours for preparation/communication, 0.5 hour for implementation for each site
Onboarding	8	Log Integration for Website	1 hour for preparation/communication, 0.5 hour for implementation, 0.5 hour for testing
Onboarding	15	Log Integration for Multiple Websites (up to 3 sites)	1 hour for preparation/communication, 0.5 hour for implementation for each site, 1 hour for testing
Reporting	3	Ad hoc Report Generation from Portal	0.5 hour for preparation/communication, 0.25 hour for implementation
Website Setting	7	Renew/Upload custom SSL certificate for single Website	1 hour for preparation/communication, 0.5 hour for implementation
Website Setting	9	Renew/Upload custom SSL certificate for multiple Websites (up to 3 sites)	1.5 hour for preparation/communication, 0.25 hour for implementation for each site
Website Setting	3	Change Website setting	0.5 hour for preparation/communication, 0.25 hour for implementation
Website Setting	5	Change multiple Websites setting (Up to 3 sites)	0.5 hour for preparation/communication, 0.25 hour for implementation for each site
Account Setting	3	Change Client account setting on Incapsula	0.5 hour for preparation/communication, 0.25 hour for implementation
Account Setting	3	Create, Remove or Update account user	0.5 hour for preparation/communication, 0.25 hour for implementation
Account Setting	11	Create Error page/Login Protect page	2 hours for preparation/communication, 0.25 hour for implementation, 0.5 hour for testing
Account Setting	2	Change Log Level	0.25 hour for preparation/communication, 0.25 hour for implementation
WAF tuning	3	Change Security Setting, including Add or update IP/URL/Bot/country to whitelist/ blacklist	0.5 hour for preparation/communication, 0.25 hour for implementation for each site
WAF tuning	5	Change Security Setting for multiple Websites, including Add or update IP/URL/Bot/country to whitelist/blacklist (up to 3 sites)	0.5 hour for preparation/communication, 0.25 hour for implementation for each site
WAF tuning	2	Manage WAF setting, including create or update whitelist/blacklist	0.25 hour for preparation/communication, 0.25 hour for implementation
WAF tuning	9	Create or update Rule	1 hour for preparation/communication, 0.25 hour for implementation, 1 hour for testing
WAF tuning	11	Create or update Rule for multiple Websites (up to 3 sites)	1 hour for preparation/communication, 0.25 hour for implementation for each site, 1 hour for testing
API	3	API management, including generate API Key and permission management	0.5 hour for preparation/communication, 0.25 hour for implementation

NTT

Together we do great things