Enhanced Security Services - Web Filtering and Web Security Gateway

1 Overview of the Service

NTT manages policy-based internet filtering to restrict users from accessing unwanted websites as well as control over most cloud-based applications allowing for the restriction of uploading or posting to undesired services if specified as in scope in the SOW.

2 Client Responsibilities

(a) For firewall systems not managed or hosted by NTT, Client will ensure that Client firewalls support the traffic integration methods utilized by the Web Security Gateway.

(b) If Endpoint-Management-as-a-Service (EMaaS) is not included with the scope of this SOW, then it is Client's responsibility to deploy the software agent to the environment.

(c) Client shall create the applicable web access policy and provide the policy with guidance to NTT for technical implementation. Client shall test changes to URL filtering policy.

(d) Client shall, under guidance from NTT, select the applicable agent type(s) for the environment, i.e., GRE, IPSEC, Proxy Chaining, PAC file and Web Gateway vendor provided mobile application.

(e) Client warrants that it has obtained all consents necessary for the end user data to be collected and used on its behalf for the Web Security Gateway and that it has a legal basis for requesting such information (excluding consents from NTT employees and agents).

3 Service Specific Operations

Tasks	Description
Internet Security Gateway to Firewalled Locations	Provide Internet security controls and policy controls via the NTT standard web security gateway service.
Internet Security Gateway in Any Location	Provide the same security controls and policy controls regardless of where licensed users connect to the Internet. Requires the use of on system agent software.
Single Web Console for Client Access	Provide Client read access to web protection console.
User Based Reporting	With the use of local application on each endpoint, per user or per group reporting can be provided. Note: This Service is only available and in scope if agents are used.
URL Filtering	Block or limit access based on a user or a specific category up to a scoped limit specified in the SOW per month.
SIEM Integration	Send logs will to the SIEM for further automated correlation and long-term retention per the long-term retention section (if any) of the SOW.
Traffic Forwarding	Support GRE, IPSEC, Proxy Chaining, PAC file and vendor provided mobile application.
Cloud Application Control	Granular access to the most popular cloud-based applications in specific categories (Social Media, File Sharing, etc). Users can be allowed to view but not upload or post.

4 Supported Environments

(a) NTT managed client on-premises data center

(b) NTT managed private and public cloud

5 Out of Scope

Enhanced Security is not a standalone offer, and can only be included when standard security is in Scope in the SOW.