Enhanced Security Services - Firewall Compliance

1 Overview of the Service

NTT will manage firewall optimization, cleanup, policy compliance and change tracking. NTT will collect data, log files and security policies to ensure network is in line with security policy design provided by NTT.

2 Client Responsibility

Client must select the supported compliance hardening configuration: PCI DSS, SOX, NSA, NERC, FISMA, or vendor recommended, and it must be specified in the SOW.

3 Service Specific Operations

Task	Description
Daily Import of logs from managed Firewalls	A report containing redundant and shadowed rules can be generated upon request.
Validate Policy Lifecycle	Upon request, up to once per year validation of Firewall Rules uses and Firewall Rules validation.
Review Firewall Changes	Upon request per month, a monthly report of all devices and their tracked changes.
Firewall Compliance Rating	Receive a monthly compliance rating PCI DSS, SOX, NSA, NERC, FISMA, or firewall vendor recommended.
Firewall Security Assessment	Monthly standardized report of attack vectors, rule and access hygiene from Firewall Security Assessment reports provided by the 3rd party assessment tool or delivered via NTT portal.

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.

Service Specific Terms and Conditions

This Service Description may require the agreement of third-party EULA or compliance with other terms. NTT reserves the right to require Client to agree to these terms and conditions before providing service.