Managed Advanced Security Technology Service Description

Overview

This document provides information relating to the management and monitoring of Advanced Security under the standard MCN offering.

This service is to provide advanced security management of Client's on-premises or colocation datacentre's security appliances. The service described herein is in addition to, and therefore complementary to, that described in the relevant MCN Service Description(s) for the on specific vendor technologies listed under Supported Vendors of this document. The Managed Advance Security Management offering will be delivered under the guidance of a Subject Matter Expert who is a specialist on the respective technology.

Client Responsibilities and Prerequisites

In addition to the pre-requisites documented in the MCN Statement of Work, the following technology specific pre-requisites are applicable.

- SIEM and SOC services are the Client's responsibility. At the Client's request, NTT may setup log forwarding to a third-party SIEM or log management service.
- The Client must share an updated Low-level Applications design with NTT Engineers to understand the traffic flow of infrastructure, that includes the application communication flow, application versions etc.
- Whenever required, the Client must facilitate meetings with the relevant application architects to enable NTT to understand the application traffic that passes through the security appliance.
- Client owns the security appliances security policies, application traffic flow policy definitions & approvals.
- Client IT personnel will retain technical design authority for security and share any data or additional information required with the SME.

Technology Component

SME Support

- A key aspect of the managed advanced security management offering is the provision of a subject matter expert (SME).
- The SME is an expert in the specific field of technology and product and provides additional support for the features described hereunder.
- SME will support their efforts by complementing their knowledge and collaborate closely with the client technical design authority to ensure that the best possible outcome is achieved.
- When clients have specific technical requirements described hereunder, SME play a crucial role in addressing these needs.
- Impact analysis can be performed on changes to security policies and recommendations shared with the client's IT security team for approval.
- SME is allocated from shared pool of resources based on number of configuration items.

Supported Vendors

For a listing of supported Security Appliance models and their respective sizing, consult the MCN Supported Technology documentation.

Supported Configurations

The Managed Advanced Security Management offering supports a range of features to enhance security of the client network.

These includes:

- Support of security zone protection policies, interface policies, management profiles etc.
- Support of layer 3/4 port-based access list & layer 7 app-based policies with security profiles.
- Support of identity-based policies and time-based policies.
- Support of high complex security rules.

- Support the following UTM profiles
  - Anti-Virus
  - Anti-Spyware
  - Sandboxing profiles
  - File filtering
  - IDS / IPS / Vulnerability profiles.
  - DNS Security
  - URL and content filtering profiles
- Support of DoS protection policies.
- Support of bandwidth (QoS) policies
- Support of SSL Decryption.
- Support of Destination NAT ,VIP, hair-pin NAT such complex NAT policies.
- Create, delete, modification of advanced S2S IPSec Tunnel with dynamic routes such as BGP.
- Support of advanced Remote access VPN policies – roaming profiles, split tunnel, multiple group policies, client posture check config etc with external identity integrations.
- Support of external / third-party identity federation and identity integrations and RBAC configurations.
- Support of system / third-party certificate generation, installation and configurations.
- Support of dynamic routing protocols- OSPF, BGP.
- Support of active/passive & active/active configurations
- Support of clustering, full mesh high availability configurations.
- Support of as-is security architecture, applications traffic flows are within scope.
- SME's can fine tune the device security policies on a best effort basis through the manual review of the logs. SME can collaborate with customer IT personnel to refine the security policies such as removal of unused rules, threat protection profiles and so on.

Limitations

The following limitations apply in the delivery of the offering:

- Design changes or re-architecture of the infrastructure is excluded.
- Design changes or re-architecture / rebuilding of the security appliance is excluded.
- The scope is limited to the listed supported technologies listed under Supported Vendors of this document.
- SME's will highlight the concerns and risks to the Client’s IT personnel on a timely basis, whereafter such accepted risks or challenges are out of scope.
- Design security policies of as-is security architecture, applications traffic flows are within scope. Designing or redesigning new applications security policies should be undertaken as a project.
- Converting Layer 3 / 4 security policies to Layer 7 application-based security polices with best effort basis where possible.
- Security policies rule optimizations such as closing of broad opened rules, removal of high complex security rules and duplicate rules are out of scope.
- End user system agent configuration, management, endpoint certificate installation, troubleshooting are out of scope.
- SDWAN Management is out of scope.

Service Requests

A list of service requests available for this technology can be found in the MCN Request Catalogue.