Managed Zscaler Technology Service Description

Overview

This document provides information relating to the management and monitoring of Zscaler under the standard MCN offering. The monitoring, configuration, limitations, and available service requests are outlined hereunder.

The scope of the Managed Zscaler technology is as follows:

- Secure Internet and SaaS Access (ZIA)
  - Zscaler Internet Access (ZIA) is for connecting users to public applications on the internet.
- Secure Private Access (ZPA)
  - ZPA is for connecting users to an enterprise's internal applications.
- Digital Experience monitoring (ZDX)
  - Zscaler digital Experience (ZDX) Service provides the digital experiences analytics from the licensed end users agents.

Client Responsibilities and Pre-requisites

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

- Administrative access to the Zscaler Cloud based portal is required to manage the described devices, software's and support tickets.
- The Client must delegate authority to NTT engineers to manage Simple Network Management Protocol (SNMP), API, Syslog, https, SSH such Management communication between NTT & Cloud vendor portal as part of the service.
- End user devices and SSE clients must be managed by the Client with their own MDM.
- The Proxy PAC deployment to all the end users must be managed by the Client through their own MDM.
- Identity management must be Client managed either directly or vendor approved third party and must authorize NTT Engineers to contact the responsible party for integrations.
- The Client must arrange the necessary third-party account details for purpose of integration such as CASB API, SaaS Application monitoring etc.
- Any other vendor technologies integration requirements must be authorized and approved by the Client as part of the service.
- An IPsec/GRE capable device must be provisioned by the Client at each branch and corporate network where connectivity to the Zscaler Cloud is intended.
- The Client must adhere that Zscaler SSE is a Cloud Delivered, Shared Service Model. The vendor may change the administration and operating model from time to time. In such cases it must be mutually agreed between NTT, Zscaler and the Client and a decision taken accordingly.
- The Hypervisor, Virtual Machines, Storage, OS systems and licenses required to install any software components for the purpose of integration to SSE must be provisioned by the Client. Example - AD connector, Zscaler Client Connector, Branch Connector etc. if required.
- It is the responsibility of the Client to upgrade SSE Agents, Cloud Identity Engines or any other agents. NTT will only provide notification to the Client when update and/or a new version is available.
- Client IT personnel will remain the technical design authority for network and security and share any data or additional information required with NTT Engineers.
- The Client must select the list of SSE Clients that should have ZDX functions enabled.

Technology Specific Operations

Monitors

The following technology specific monitors can be configured by default.

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
ZIA Core Cloud service	Monitors Zscaler internet access ZTE Core Cloud health status	✓	N/A	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware maintenance provider as required	180
ZIA Data Centers	Monitors ZIA tunnel terminated individual Datacenters health status	✓	N/A	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware maintenance provider as required	180
ZPA Core Cloud service	Monitors Zscaler Private access ZTE Core Cloud health status	✓	N/A	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware maintenance provider as required	180
ZPA Data Centers	Monitors ZPA individual Datacenters health status	✓	N/A	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware maintenance provider as required	180
App Connector Device Health	Monitor the device health and performance metrics (CPU, Memory, disk usage)	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware maintenance provider as required	180
App Connector Interface health status	Monitor the interface status, data throughput.	✓	Graphs for the parameter measured over time	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client or hardware maintenance provider as required	180

Configuration Management

Zscaler is a full SaaS offering, therefore device configuration backups are inherent to the solution and are executed automatically with the built-in toolsets to the Zscaler Cloud. All Zscaler configuration backups are stored in the Zscaler Cloud itself as part of Management Orchestration

Firmware Maintenance

Firmware maintenance for the Zscaler solution is an automated process and is included within the Zscaler. Firmware schedules and frequencies are determined and managed by the Zscaler vendor. For further details in this regard refer to the vendor’s relevant documentation.

Supported configurations.

The following features and services are supported under the MCN offering.

General supported configurations

Platform specific administrative functions such as the configuration of authentication, authorization, and accounting (as applicable per design).

Management of ZIA security policies, Advance threat protection, Malware protection content filtering policies, URL filtering policies, Anti-virus, sandbox etc. standard internet gateway supported configurations.

Management of ZIA authenticated, unauthenticated secure web traffic and non-web traffic, machine tunnel, Source IP Anchoring.

Management of ZPA administration for On-Prem, Public cloud hosted applications.

Management of Zscaler Client connector portal and agent settings.

Management of Zscaler Digital experience management.

Traffic forwarding

Various traffic forwarding mechanisms are supported to forward traffic from the Enterprise to Zscaler Cloud.

The following traffic steering methods are supported for Zscaler internet access.

- Zscaler Client Connector
- Zscaler Client Connector over GRE
- IPsec tunnel
- Proxy Auto-Configuration (PAC)
- Zscaler Cloud Connector

The following traffic steering methods are supported for Zscaler Private access.

- Zscaler Client connector.
- Zscaler App Connector.
- Zscaler supported browser access.

The following traffic steering methods are supported for Zscaler Digital Experience.

- Zscaler Client connector.

Authentication

Authentication enables Zscaler to identify traffic that it receives so it can enforce configured department, group, user policies, and provide user and department logging and reporting. The service supports Security Assertion Markup Language (SAML 2.0), SCIM, Secure Lightweight Directory Access Protocol (LDAP) including Active Directory, Zscaler Authentication bridge.

If ZPA is utilized, the client must utilize a SAML 2.0 compliant identity provider (IdP) for authentication of users to access client applications.

Logging

Configuration of NSS Server in ZIA portal, Web & Firewall feeds, Cloud NSS feeds.

Zscaler Internet Access

NTT supports the configuration and policy management of following ZIA features based on the underpinning Zscaler edition it includes the following standard features:

- Cloud-delivered secure web gateway.
  ZIA provides a cloud delivered SWG for complete visibility and control over user's web access while enforcing security policies that protect the users from the latest threats.
  - Advance threat and Content Filtering
    - Content filtering policies protects the Client's organization from inappropriate or harmful content.
    - Inline Anti-virus & Anti-spyware
    - Signature-based anti-malware protection that detects and blocks all known viruses, spyware, and other kinds of malware.
  - Cloud Application Visibility & Control
    - This capability manages user access to cloud applications, such as Webmail, streaming media, or social networking.
    - Context-aware security policies that are based on the application's user identity, group, and location.

- Bandwidth Control
  - Protect key apps and limit recreational apps by location or time of day.
- Data Loss Prevention (DLP)
  - Protect users across devices and networks to ensure data security, data privacy and regulatory requirements are met.
- SSL inspection
  - Full inline threat inspection of all SSL traffic with granular policy.
- Cloud Browser Isolation.
  - Isolate the users from harmful content on the internet.
  - Native Zscaler CBI are supported.

- Cloud Advanced firewall

  Based on the underpinning Zscaler edition, ZIA provides a cloud-delivered next generation firewall that has the following standard features:
  - Cloud firewall filters non-web internet traffic.
  - Intrusion Prevention System (IPS) control and protect your traffic from intrusion over all ports and protocols using signature-based detection.
  - Domain Name System (DNS) security and control
- Cloud Sandbox
  - Sandbox provides an additional layer of security against zero-day threats and Advanced Persistent Threats (APTs)
  - Sandbox security widgets and reports available in Zscaler cloud portal.
- Cloud Access Security Broker (CASB Inline and OOB).
  - Zscaler SaaS Security API provides visibility and security for sanctioned SaaS applications and authorize sanctioned SaaS applications with Zscaler by adding them as tenants.
  - Protect the SaaS & Cloud Applications data by applying appropriate DLP dictionaries, engines, Indexed data match and Exact data Match.

Zscaler Private Access

NTT supports the configuration and policy management of following ZPA features based on the underpinning Zscaler edition it includes the following standard features:

- Application Discovery
  - Applications can be explicitly defined or ZPA can discover applications as they are requested by users. The discovered applications can be defined into application segments for policy control.
- Device Posture Enforcement
  - ZPA takes into consideration compliance or posture of a user's device, prior to providing access to applications. A user can be blocked from accessing application if the user's device is deemed non-compliant.
- Realtime View
  - ZPA provides visibility into a user's activity, such as user status and application access.
- Policy Enforcement
  - ZPA can allow or block requests to an application based on the rules specified within an Access Policy.
- Application Segmentation
  - Application segmentation provides granular access control by User or User group for a specific grouping of defined applications. Based on the underpinning ZPA edition, a specific number of application segments is permitted.

Zscaler Digital Experience

- Zscaler Client connector monitor business critical SaaS Applications and Datacenter using synthetic probes to detect real-time user experience.
- ZDX function on ZCC supported as per vendor release.
- ZCC Collects the real-time data (i.e., CPU usage, memory usage, Network IO, Disk IO, Wi-Fi signal strength, etc.) and forward the data to Zscaler Cloud.

- Excusive insights reports and digital experience analytics aggregated at organization, location, and application levels and data available in the Zscaler cloud management portal for review and reporting.

Supported Environments

- Zscaler managed POP's across the globe are supported.
- Zscaler internet Access and Private application access integration with Client on-premises data center, Colocation data center, Public Cloud infrastructure are supported.

Limitations

The following limitations apply:

- ZCC Agents or any other agent's deployment is the responsibility of the client, and that NTT will only provide notification/recommendation to a client that there is an update and/or new version available.
- Zscaler Cloud Identity configuration is supported, Service excluded third-party Identity management such as Azure Active directory, any type of identity services, and identify agent management are out of scope.
- Any changes in Vendor committed SLA's.
- Zscaler Workload Segmentation, Zscaler Posture control, Zscaler Cloud protection such as Cloud Security Posture Management (CSPM), Cloud Infrastructure Entitlement Management (CIEM), Security and Compliance, Infrastructure-as-Code (IaC) Security, Vulnerability Management, deception, Risk360, etc. services are out of scope.
- Zscaler service does not include procurement of internet or WAN circuits, or software or hardware / virtual devices. These services are available from NTT under a separate Statement of Work.
- All the supported features and standard supports are subject to license availability.
- Re-design from AS-IS architecture to new target state architecture is out of scope.
- NTT will not design or create policies or register devices unless given specific instructions by client or representative of client.
- NTT will not provide end-user support but assist to Client Support teams to resolve any end-user faults that are or suspected to be attributed to the network.
- NSS, LSS Service Management and its related integration are out of scope. These services are available from NTT under a separate Statement of Work.
- Threat Intelligence, Forensic analysis, External Dynamic list, and IOC blocking is out of scope.
- Design changes or re-architecture of service, Designing the security policies, UTM policies, re-structure of security policies etc. are out of scope.
- Zscaler Private edges and Virtual Service edges are not supported.
- The tasks, features and services listed in this document are excluded from any underlying infrastructure hosting virtual Zscaler appliances.

Service Requests

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

Technology Transition Tasks

No technology specific transition tasks are required. A description of the standard transition tasks included for the service offering is documented in the MCN Statement of Work

Note:

Any tasks not explicitly described under the Technology Transition tasks are implicitly excluded from transition.