Managed Palo Alto Prisma SASE Technology Service Description

Overview

This document provides information relating to the management and monitoring of Palo Alto Prisma SASE (Prisma Access and Prisma SDWAN) under the standard MCN offering. The monitoring, configuration, limitations, and available service requests are outlined hereunder.

The Scope of Managed Palo Alto Prisma Secure Access Service Edge as follows.

- Prisma Access SSE (Security Service Edge)
  - Palo Alto Cloud Management portal (STRATA Cloud Manager)
  - Palo Alto Cloud POPs (Data plane that inspecting actual traffic).
- Prisma SDWAN
  - Cloud Orchestrator and Controller (STRATA Cloud Manager)
  - Physical Edge device(s)
  - Virtual Edge instance(s)
  - Prisma SD-WAN Cloud Blades

The following sections clarify the Prisma Access technology descriptions.

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.

- Administrative access to the Palo Alto Cloud based portal is required to manage the described devices and software's and support tickets.
- The Client must be managing the end user devices and SASE clients with your own MDM.
- The Client must be managing the Identify management either directly or vendor approved third party and authorize NTT Engineers to contact them for integrations.
- The Client must ensure there is not conflict of IP address and Providing IP address pools for the service infrastructure, the branch locations, and/or your mobile users.
- The Client must adhere that Prisma Access is Cloud Delivered Shared Service Model, Vendor may change the administration and operating model from time to time, in such cases it must be mutually aligned between NTT, Palo Alto, Customer and take the decision accordingly.
- The Client must arrange the Hypervisor & VM's, Storage, OS systems and license to install any software components for the purpose of integration to Prisma Access. Example - AD connector, ZTNA Connector etc. if required.
- Global Protect Agent and the Cloud Identity Engine or any other agents updating is the responsibility of the client, and that NTT will only provide notification to a client that there is an update and/or new version available.
- The Client must choose the list of SASE Clients that should have ADEM Agents installed.
- The Client must share the list of critical applications that should be enabled in part ADEM Synthetic monitoring.

Technology Specific Operations

Prisma Access Monitors

The following technology specific monitors can be configured by default:

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
External Alerts Current	Shows the alert count by severity	✓	Graphs for Critical, High, Medium Severity alerts count	Engineering Teams will diagnose and follow process to investigate and inform / escalate to the Client if needed.	1200
Current Alerts Generated	Shows all currently generated alerts	✓	Graphs for Critical, High, Medium Severity alerts details	Engineering Teams will diagnose and follow process to investigate and inform / escalate to the Client if needed. / escalate to the Client if needed.	1200
Global Protect Mobile User Edge location Status	Shows the status of the mobile users managed for a specific Prisma Access location.	✓	Graphs for Mobile user's service edge location status - up/down.	Engineering Teams will diagnose and follow process to investigate and inform / escalate to the Client if needed.	60
Remote Network Edge location Status	Shows the status of the remote networks managed by a specific Prisma Access location	✓	Graphs for Remote Network service edge location status - up/down.	Engineering Teams will diagnose and follow process to investigate and inform / escalate to the Client if needed.	60
Remote Network Bandwidth Consumption	Shows remote network bandwidth consumption for a specified Prisma Access location	✓	Graphs for Tunnel interface Bandwidth status	Engineering Teams will diagnose and follow process to investigate and inform / escalate to the Client if needed.	300
Service Connection Bandwidth Consumption	View the service connection bandwidth consumption managed by a specific Prisma Access location	✓	Graphs for Tunnel interface Bandwidth status	Engineering Teams will diagnose and follow process to investigate and inform / escalate to the Client if needed.	300
Service Connection Status	View the number of users connected in real time to Prisma Access View the number of RN connected to Service Connection	✓	Graphs for Tunnel status - up/down Total no.of RN and Mobile users.	Engineering Teams will diagnose and follow process to investigate and inform / escalate to the Client if needed.	300
Explicit Proxy Mobile Users Status	View the status of the explicit proxy mobile users managed for a specific Prisma Access location	✓	Graphs for Explicit proxy service status - up/down.	Engineering Teams will diagnose and follow process to investigate and inform / escalate to the Client if needed.	300
Tunnel list	Query the state of a tunnel	✓	Graphs for Tunnel status - up/down	Engineering Teams will diagnose and try to solve the issue and escalate to the Client if needed.	300
Service Connection Bandwidth Consumption Over Time	Shows service connection bandwidth consumption for the past 24 hours	✓	Graphs for Tunnel interface Bandwidth status	Engineering Teams will diagnose and follow process to investigate and inform / escalate to the Client if needed.	300

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
Service Connection Site List	Shows the service connections status and metrics	✓	Graphs for Service Connection status - up/down.	Engineering Teams will diagnose and follow process to investigate and inform / escalate to the Client if needed.	300
Remote Network Bandwidth Consumption Over Time	Shows the ingress, egress, average, and peak bandwidth consumption over time	✓	Graphs for Tunnel interface Bandwidth status	Engineering Teams will diagnose and follow process to investigate and inform / escalate to the Client if needed.	300
Remote Network Bandwidth Allocated	Shows the remote network bandwidth allocated per compute location	✓	Graphs for Aggregate Bandwidth Mbps.	Engineering Teams will diagnose and follow process to investigate and inform / escalate to the Client if needed.	300
Remote Network Site List	Shows a total remote network site list of your remote networks' status and metrics for the last 30 days	✓	Graphs for Remote Network service edge location status - up/down.	Engineering Teams will diagnose and follow process to investigate and inform / escalate to the Client if needed.	300
Connected User Count	Shows the number of Mobile Users connected in real time.	✓	Graphs for Mobile users count	Engineering Teams will diagnose and follow process to investigate and inform / escalate to the Client if needed.	300
List license utilization	Shows an aggregated list of all licenses utilized.	✓	Graphs for license status	Engineering Teams will diagnose and inform to the Client if needed.	300
ADEM Synthetic Monitoring	Synthetic tests to baseline network quality and application monitoring from SASE Agents. ADEM Agent collects web performance metrics such as HTTP(s) transactions to a specific application, including application availability, DNS lookup, TCP Connect, SSL connect, HTTP latency, Time-to-First-Byte, Data Transfer rate and Time-to-Last-Byte.	✓	Graphs for Web performance status	Engineering Teams will diagnose and follow process to investigate and inform / escalate to the Client if needed.	N/A

Configuration Management

Prisma Access 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 Prisma Access Cloud. All Prisma Access configuration backups are stored in the Palo Alto Cloud itself as part of Management Orchestration.

Firmware Maintenance

Firmware maintenance for the Prisma Access solution is an automated process and is included within the Prisma Access Solution. Firmware schedules and frequencies are determined and managed by the Palo Alto vendor. For further details in this regard refer to the vendor's relevant documentation.

Supported configurations

Palo Alto's Prisma Access delivers networking and security capabilities required in today's enterprise networks through an architecture designed for all types of traffic, applications, and users. Prisma Access uses a common cloud-based infrastructure to deliver multiple network security services thereby eliminating many sources of complexity normally associated with the deployment of point products. Prisma Access Services comprises of

- Network as a Service Layer or supported network features.
- Security as a Service Layer or supported security features.

All the features listed below sections are supported in part of MCN Prisma SASE service-specific operations, configurations.

Network as a Service Layer

Prisma Access provides consistent, secure access to all applications whether they are located in the cloud, in a data Centre or on the internet. The Network as a Service capabilities of Palo Alto Prisma Access offers:

- Networking for Mobile Users
  - Using Palo Alto's Global Protect application allows organizations to connect mobile users thereby providing user-based always-on, pre-logon always-on, and on-demand connectivity.
  - Prisma Access also supports split tunnelling for an always-on optimal security connection and can be based on access route and application type including associated risk and bandwidth utilization thereof.
  - Explicit Proxy allows clients to choose proxy mode where the client (browser) is configured to use a proxy server. This option is an alternative way for mobile users to connect to Prisma Access and secure their internet and SaaS application traffic (HTTP/HTTPS). PAC files are supported for browser configuration.
  - Explicit Proxy is supported in several locations and are listed at https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/secure-mobile-users-with-prisma-access/explicit-proxy/explicit-proxy-locations.
  - Clientless VPN enables secure remote access to enterprise applications from SSL-enabled web browsers eliminating the need to install the Global Protect software on endpoints. This form of connectivity is useful for facilitating partner or contractor access to applications BYOD endpoints.
- Networking for Remote Networks
  - Connect branch offices to Prisma Access over a standard IPSEC tunnel using a common IPsec-compatible device that implements IPSEC to industry standards and is RFC compliant are implement, such as an existing branch router, SD-WAN edge device, Palo Alto Networks NG Firewall or third-party firewall and includes Cloud blades managed tunnel connectivity from Prisma SD-WAN, which enables managed SASE connectivity.
  - Inter branch routing support through Border Gateway Protocol (BGP) or static routes.
  - Equal-cost multi-path (ECMP) routing is also supported and provides faster performance and improved redundancy across multiple links.
- Service Connections
  - Service connection is standard IPSEC tunnel terminated in Corporate Access Node (CAN), enables both mobile and branch users to access resources on the network that may be located in data center's and regional headquarters.
  - It also enables intercommunication between mobile users and branch (remote) networks with Net Internet connect license.
  - Service Connections must be planned before being implemented.
  - Each Service Connection typically provides approximately 1 Gbps of throughput but this is dependent on traffic types, latency and packet loss (between the service connection and the destination), any Service Provider performance limitations and terminating equipment limitations.

- Bandwidth Management
  - Increase bandwidth by restricting bandwidth-intensive applications through application whitelisting and blocking policies using Palo Alto's App-ID technology.
  - Prisma Access quality of service (QoS) policies provides the capability to priorities and shape traffic traversing the network.
- Logging (Cortex Data Lake)
  - Automated, centralized, cloud-scalable log storage. Log retention will be based storage volume.
  - Centralized management and reporting via the cloud-based Cortex Data Lake.
  - Log forwarding to Syslog servers and security information and event management (SIEM) systems.
- ZTNA Connector
  - Private application access in overlapped networks, ZTNA Connector simplifies app access in overlapped networks by allowing you to connect to apps using FQDN, port, and protocol, without you having to configure IP routing.
  - Easy Data Center to Cloud Migration, ZTNA Connector can accelerate the process of providing cloud-delivered app access.
  - Easy Private application access in Business Partner Networks without building Service connections.

Security as a Service Layer

Prisma Access also includes comprehensive security capabilities in a consolidated, service edge. These capabilities include:

- Cloud Secure Web Gateway (SWG)
  - Cloud secure web gateway (SWG) functionality for remote users across all web traffic protocols and applications in hybrid environments.
  - Advanced URL and content filtering for users based on dynamic group monitoring, allowing the implementation of granular behavior's-based policies.
  - The integrated proxying capability gives users maximum flexibility for how they connect to the Prisma Access service.
  - C2 (command-and-control) callback and DNS tunnelling attacks can be prevented through advanced DNS security.
- Firewall as a Service (FWaaS)
  - Using Palo Alto Next-Generation Firewall (NGFW) functionality provides firewall-as-a-service (FWaaS) capabilities and includes inbound and outbound protection, native user authentication, access control, and Layer 3–7 single-pass inspection to secure branch offices against any threats.
- DNS Security
  - The DNS Security service combats threats in DNS traffic through a combination of predictive analytics, machine learning, and automation allowing organizations to block known malicious domains, predict new malicious domains, and stop DNS tunnelling.
  - Automatically prevents C2 callback and tunnelling to malicious domains identified with real-time analysis and global threat intelligence.
  - C2 Protection stops malicious outbound communications stemming from malware infections by passively analyzing DNS queries and identifies the unique patterns of botnets and prevents secondary downloads and data from leaving the organization.
- SSL Decryption
  - Inspects and applies the policy to TLS/SSL-encrypted traffic, both inbound and outbound, including traffic that uses HTTP/2. For privacy and regulatory compliance, decryption can be enabled or disabled flexibly based on URL, source, destination, user, user-group and port.
  - Prisma Access has the capability to "self-scale" SSL Decryption based on the network load thereby ensuring that configured performance SLA's are honored.
- Advanced Threat Prevention
  - Prisma Access threat prevention combines the proven technologies inherent in Palo Alto Networks platforms, together with global sources of threat intelligence and automation, to stop known and unknown attacks.
- Zero Trust Network Access (ZTNA)
  - Authenticates and provides user application connectivity based on granular role-based access control (RBAC)

- Single pane of glass policy creation and enforcement.
- Both agent-based and agentless connection methods are supported regardless of the user's location.
- Single-pass traffic inspection for malware, data loss, and malicious behavior is performed after users connect.

- Data Loss Prevention (DLP)
  - DLP policies allow organizations to categories data and establish policies that prevent data loss. Prisma Access combines integration with DLP controls that are API-driven through Prisma SaaS, and in-line driven through Prisma Access.
- IoT Security
  - Prisma Access includes powerful IoT (Internet of things) security capabilities to help protect against IoT threats without needing deployment of additional sensors or appliances.
  - Combines machine learning with Palo Alto's App-ID technology and crowdsourced telemetry to profile all devices for discovery, risk assessment, vulnerability analysis, anomaly detection, and trust-based policy recommendations thereby preventing known and unknown IoT, IoMT and OT threats.
- Machine Learning powered security
  - Inline machine learning is used to prevent unknown, zero-day attacks in real time. Additionally, machine learning is utilized to analyze vast amounts of telemetry data to make automated security policy recommendations thereby improving security much more quickly.
- Next-Gen Cloud Access Security Broker (CASB)
  - Prisma Access natively provides inline visibility and control of software-as-a-service (SaaS) applications.
  - API-based security and contextual controls can be introduced for sanctioned SaaS applications through Prisma SaaS and is implemented in an integrated manner and applied throughout all cloud application policies.
- Cloud Identity Engine
  - Comprises of two components, namely Directory Sync and Cloud Authentication Service.
  - Directory Sync provides user information and Cloud Authentication Service authenticates users and when both components are deployed, provides a comprehensive identity solution.
  - Cloud Authentication Service uses a cloud-based service to provide user authentication using SAML 2.0-based Identity Providers (IdPs) and simplifies user authentication across the network.
  - The Cloud based solution provides the capability to reallocate authentication resources between the firewall, Panorama and the Cloud.
- ADEM (Advance Digital Experience Management)
  - Performance trends for Mobile users for the selected applications on selected mobile users. Performance visibility of those ADEM user's endpoints to the target applications to identify the network errors.
  - Synthetic application monitoring from Mobile user and Prisma SDWAN Devices to SaaS Applications via Prisma Access Cloud.

Management Orchestration

- Prisma Access Cloud Management
  - Streamlined Prisma Access configuration management with seamless onboarding, continuous assessment of security posture and digital experience monitoring.
  - Reporting through a unified experience delivered from the cloud.

Supported Features

- The Managed Prisma access SASE Service includes platform specific administrative functions such as the configuration of authentication, authorization, and accounting (as applicable per design), Creating, managing security policies, and controlling features such as syslog, SNMP etc are standard supported configurations.
- Prisma Cloud infrastructure setup.
- Remote Networks (RN) and Remote Network Service Process Node (RN-SPN) related configurations.
- Service connection (SC) and Corporate Access Node (CAN) related configurations.
- Global Protect Mobile user and Mobile Users Service Process Node (MU-SPN) related configurations.
- Standard traffic routing from Mobile users to SC and RN to SC.
- Advance Routing - Mobile Users to Remote network routing if Net Interconnect license in place.
- Advance Routing that includes the BGP and ECMP configurations.

- User-ID deployments and User info redistribution configurations in the Management orchestration.
- Cortex Data Lake log management configuration and reporting.

Limitations

- Managed Palo Alto Prisma Secure Access Service Edge (SASE) Service does not include procurement of internet or WAN circuits. These services are available from NTT under a separate Statement of Work.
- Any changes in Vendor committed SLA's.
- Cloud-based management option is preferred over Panorama management, So Service is supported with Cloud based management rather Panorama Management. Panorama Management suggested to use for NGFW.
- Palo Alto Prisma Access Cloud delivered features are supported. Service exclude from the Prisma Cloud Services such as CSPM, CNAPP, CWP,CIEM etc.
- All the supported features and standard supports are subject to license availability.
- Completely Re-design from AS-IS architecture to new target state architecture is out of scope from this service description.
- SASE Agents - GP, ADEM, Identity, TS Agent such any client management is out of scope.
- ADEM will only be configured per specific instructions from the client. 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 will provide assistance to Client Support teams to resolve any end-user faults that are or suspected to be attributed to the network.
- A CSP (customer support portal) account with an app administrator or higher role assigned to configure ADEM.
- Prisma Access and Prisma SD-WAN apps must be available and linked with each other on the HUB interface under the CSP account.
- Global Protect Agent and the Cloud Identity Engine or any other agents updating is the responsibility of the client, and that NTT will only provide notification to a client that there is an update and/or new version available.
- The tasks, features and services listed in this document are excluded from any underlying infrastructure hosting virtual Prisma Access appliances.

Prisma Access Service Requests

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

Technology Transition Tasks for Prisma Access

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.

Prisma SD-WAN Overview

Palo Alto Prisma SD-WAN service with Instant-On Network (ION) models of hardware and software devices enable the integration of a diverse set of wide-area network (WAN) connection types to improve application performance and visibility, enhance security and compliance, and reduce the overall cost and complexity wide area networks.

Client Responsibilities and Prerequisites

- Administrative access to the Palo Alto Cloud based portal is required to manage the described devices and software's and support tickets.
- The Client must be managing the Identify management either directly or vendor approved third party and authorize NTT Engineers to contact them for integrations.

Technology Specific Operations

Prisma SD-WAN Monitors

The following technology specific monitoring can be configured by default.

Monitor	Description	Alerts	Performance Info	Resolution	Poll Interval (sec)
DNS	Checks to see if the collector is able to resolve the IP address to the applied host.	✓	N/A	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client if needed.	120
Interface Status	Check interface's status	✓	Graphs of Interface Status up /down	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client if needed	60
Interface Usage	Check interface's bandwidth usage	✓	Graphs for the parameter measured over time	N/A	120
Synthetic Monitoring	Provides visibility into real traffic utilization between Prisma SD-WAN remote sites and the applications, for traffic traversing the Prisma Access infrastructure.	✓	Network quality metrics such as latency, jitter, and loss.	Engineering Teams will diagnose and try to resolve the issue, and escalate to the Client if needed	300

Configuration Management

Prisma SDWAN 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 Prisma SDWAN Cloud. All Prisma SDWAN configuration backups are stored in the Palo Alto Cloud itself as part of Management Orchestration.

Firmware Maintenance

There are no specific requirements or demands for the technology. Firmware maintenance is administered in accordance with the standard MCN processes. Refer to the MCN Common Network Management Service Description for further information.

Supported configurations.

The following Palo Alto Prisma SD-WAN configurations are supported.

- Cloud Orchestrator and Controller (STRATA Cloud Manager)
- Physical Edge device(s)
- Virtual Edge instance(s)
- Prisma SD-WAN Cloud Blades

Not all these elements may be required in every deployment. The features required and or deployed in the network determines the requirement for the various elements. The following section describes each of these elements:

- Cloud Orchestrator and Controller (STRATA Cloud Manager)
  - This service leverages the Multi-Tenant Prisma SD-WAN cloud management portal also called as STRATA Cloud Manager, which is utilized for device policy management, real-time monitoring, and remote diagnostics. All aspects of configuration, management, and monitoring of Prisma SD-WAN ION hardware and software devices are performed on this portal thereby eliminating individual device configuration each location.
- Physical Edge device(s)
  - These are the Instant-On Network (ION)devices installed at the Client's premises and enables integration of a diverse set of wide-area network (WAN) connection types. It also improves application

performance and visibility, enhances security and compliance, and reduces the overall cost and complexity of the WAN.
It provides SD-WAN and WAN optimization based on the purchased subscription model. These devices support multiple modes of operation, based on the deployment scenario, namely:

- Analytics Mode
- In analytics mode, the Prisma SD-WAN solution provides end-to-end visibility and analytics of applications and networks, operating independently of the full suite of Prisma SD-WAN capabilities. ION devices are deployed at the WAN edge and automatically begin examining application data on the network to identify the application and measure several key performance indicators of each session. These statistics are stored securely in the Prisma SD-WAN cloud management portal, which can be used to configure ION devices, define applications and sites, and monitor end-to-end application performance and availability.
- Control Mode
- Control mode builds on the visibility and analytics foundation of analytics mode by allowing the ION devices to intelligently take action based on performance, compliance and security policies. Routing functions, including path selection, prioritization, and security, can be integrated into the ION device to reduce the amount of hardware and operational expense associated with each remote office.

- Virtual Edge instances
  - Prisma SD-WAN Virtual ION is installed on a virtual machine that is either provided locally or by the Client's Cloud Service Provider. The virtual appliance has the same capabilities as the physical devices as described in the preceding paragraph.
- Prisma SD-WAN Cloud Blades
  - The Cloud Blades platform enables API-based integration of the branch CPE (Client Premise Equipment). It provides a centralized platform for programming and an application-flow engine at the CPE, access to Prisma SD-WAN telemetry, and secure authenticated API access Prisma SD-WAN CPE and systems. As a result, businesses can easily enable the cloud-delivered branch and simplify management and operations.

Limitations

- Palo Alto NGFW PAN SD-WAN is not supported.
- The tasks, features and services listed in this document are excluded from any underlying infrastructure hosting virtual Prisma Access appliances.

Prisma SD-WAN Service Requests

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

Technology Transition Tasks for Prisma SD-WAN

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.