SERVICE DESCRIPTION

QuickStart Service for NGFW: PA-400 Series

1. Introduction

This service description document ("Service Description") outlines the Palo Alto Networks QuickStart Service for NGFW: PA-400 Series offering ("Services").

By placing a purchase order ("Purchase Order" or "PO") for the Services, the customer ("Customer") is purchasing Palo Alto Networks QuickStart Service for NGFW: PA-400 Series and agrees to the terms in this Service Description. The term of the Services shall commence upon purchase order acceptance by Palo Alto Networks and shall continue for, and must be used within, a period of six (6) months.

Palo Alto Networks will provide Services on the Customer's existing security infrastructure to Palo Alto Networks hardware and software offerings (collectively "Products") described in the Deliverables section of this Service Description.

1.1. United States and Canadian Public Sector Customers

United States and Canadian Public Sector Customers, which term shall include but may not necessarily be limited to the federal governments, state and local governments, education (both K-12 and higher education), and other quasi-governmental entities in the United States and Canada (collectively "Public Sector Customers") shall purchase the Services in this Service Description through a Palo Alto Networks authorized partner only and not directly from Palo Alto Networks. Any Services performed by Palo Alto Networks through this Service Description will be in support of the partner prime contractor's contractual obligations. This Service Description shall in no way create a contractual obligation between Palo Alto Networks or its subsidiaries and any Public Sector Customers or government end user. For purposes of Public Sector Customers only, the following sections will not apply: Section 5 (Travel Expenses for On-Site Work), Section 8 (Fees and Payment), and Section 9 (Terms and Conditions). The term of the Services for Public Sector Customers shall commence upon purchase order acceptance by Palo Alto Networks and shall continue for, and must be used within, the Public Sector Customer's contracted period of performance as defined in the applicable partner prime contract. Further, any references to payment of travel expenses due to cancellation shall not apply. To the extent that any term or condition of this Service Description contradicts any applicable rule, law or regulation, such rule, law or regulation shall take precedence over that term or condition.

2. Scope of Services

The Services include project management, planning, configuration, production deployment event support, documentation, and knowledge transfer. The specific deliverables ("Deliverables") included in the Services are defined in Section 3.

The objective of the Services, to be agreed upon at project kick off, is to provide the Customer with the expertise to either:

- Remotely upgrade an existing Palo Alto Networks NGFW to a new Palo Alto Networks NGFW ***or***
- Remotely deploy a new Palo Alto Networks NGFW in a net new environment (greenfield) or migrate from an existing non-Palo Alto Networks firewall identified in Section 2.1.1

2.1. Service Parameters

2.1.1. General

Parameter	Description
Target PA-Series NGFW(s)	The target system must be one (1) of: PA-400 Series
Legacy firewalls supported for Migration use case	The legacy firewall must be one of the vendors specifically identified at: https://live.paloaltonetworks.com/t5/expedition-articles/expedition-supported-3rd-party-vendor-matrix/ta-p/336922#. The list of identified vendors may be updated from time to time by Palo Alto Networks. All other legacy firewall vendors will be considered greenfield for this service.
Type of rules migrated	Layer 3/4 Security and NAT rules, migration of any other rule type is **not** supported
Legacy firewall configuration	The legacy firewall must be a physical or virtual device configured as a single or Active/Passive HA pair - multiple virtual systems/contexts are **not** supported
FIPS Mode	Deployment of NGFW in FIPS mode is **not** supported
IPSec VPN migration/creation	IPSec VPN configuration/migration is **not** supported - add-on service available
Threat configuration	Use existing Security Profile(s) if available, otherwise the Day 1 configuration available via Customer Support Portal (CSP) will be used
URL Filtering configuration	Use existing URL profile(s) if available, otherwise URL Filtering configuration is **not** supported - add-on service available
Subscription configuration	Other Subscription configuration is **not** supported - add-on service available
Advanced PAN-OS capability configuration	Advanced PAN-OS capability (App-ID, User-ID, SSL Decryption) configuration is **not** supported - add-on service available

2.1.2. Upgrade

Parameter	In Scope	Description
Number of upgrade events	1	Perform an upgrade from an existing Palo Alto Networks NGFW to a new Palo Alto Networks NGFW - one (1) NGFW as defined in Section 2.1.1 in one (1) cutover event

Number of NGFWs to upgrade	1	One (1) single or Active/Passive HA pair of existing Palo Alto Networks NGFWs
PAN-OS versions to upgrade	1	Generally available version of PAN-OS - PAN-OS 10.1 or newer is **required** for PA-400 Series
Configuration changes	Yes	Only as required to support the upgrade, no other new configuration is in scope
Panorama integration	Yes	Transition of Panorama management from the existing to the new NGFW

2.1.3. Deploy

Parameter	In Scope	Description
Number of deployments* * Choice of one (1)	1*	Perform a new Palo Alto Networks NGFW deployment as greenfield - one (1) PA-400 Series NGFW in one (1) cutover event
		Perform a new Palo Alto Networks NGFW deployment as migration from legacy firewall - one (1) PA-400 Series NGFW in one (1) cutover event
Number of source firewalls	1	One (1) source legacy firewall
Number of NGFWs	1	A single or Active/Passive HA pair of NGFWs
Number of Virtual Systems (vsys)	1	Single vsys deployment
NGFW deployment mode	1	NGFW can be in vwire, Layer 2, or Layer 3 mode
Number of Virtual Routers (VRs)	2	Up to two (2) VRs for static/supported dynamic routing protocol - if applicable
Number of Security/NAT rules to migrate or create * Choice of one (1) of these options, not all	50*	For legacy firewall rules migration from legacy firewall vendors identified in the link provided in Section 2.1.1 migrate up to fifty (50) Security/NAT rules - add-on service available for additional rules
	20*	For legacy firewall rules from legacy firewall vendors **not** identified in the link provided in Section 2.1.1 or a greenfield firewall deployment, create up to twenty (20) new Security/NAT rules
Security/NAT rule review sessions	1	Maximum number of sessions to be scheduled in blocks of two (2) hours, two (2) hours total, to review rules either created or migrated
Multi-factor Authentication	Yes	For NGFW administrative management with supported MFA protocol/system
Panorama integration	Yes	To an existing Panorama system, a new Panorama deployment or upgrade is not in scope
Log Forwarding	Yes	Send to an existing Panorama/Log Collector and up to two (2) Syslog destinations - custom log format creation is not in scope
Monitoring and Alerting	Yes	Integration with up to two (2) each of the following existing systems: SNMP Poller/ Trap destinations for monitoring, and SMTP gateways for alerts

2.2. Planning

Palo Alto Networks will, with Customer's participation, conduct planning activities and a project kick-off call. The project kick-off will include review of the project requirements (upgrade or new deployment), discuss milestone timelines, identify the Customer's project team members and follow-up action items.

Palo Alto Networks will provide a predefined Project Plan, as defined in Section 3, and perform one (1) review with the Customer team for the addition of customer specific requirements/feedback. The final Project Plan will be mutually agreed to prior to moving to the next phase of the project.

2.3. Discover

Upgrade

Palo Alto Networks will review with Customer the requirements to upgrade the NGFW system and/or PAN-OS software. This will be used to capture the mutually agreed technical requirements (the "Requirements") for the upgrade of the target to the new NGFW.

Deploy

Palo Alto Networks will review with Customer the Customer-provided architecture and design documentation as well as the legacy firewall configuration as required. This will be used to capture the mutually agreed Requirements for implementation of the new NGFW.

Palo Alto Networks will provide a predefined Technical Requirements Document ("TRD"), as defined in Section 3, and perform one (1) review with the Customer team for the addition of customer specific requirements. The final TRD will be mutually agreed to prior to moving to the next phase of the project.

2.4. Configure and Review

Upgrade

Palo Alto Networks will work with the Customer to perform a test upgrade of the hardware and/or PAN-OS software to confirm the upgrade process.

Palo Alto Networks will review Release Notes and other available information to identify known issues that may impact the hardware and/or PAN-OS software upgrade. This review will be performed based on the current NGFW configuration and documented known issues to finalize the version of PAN-OS to be deployed.

Deploy

Palo Alto Networks will work with the Customer to configure the targeted Palo Alto Networks device based on the mutually agreed upon Requirements. This will include the creation of new or migration of legacy firewall Security/NAT rules as defined in Section 2.1.3.

Palo Alto Networks will review the configuration and provide the number of rule review sessions as defined in Section 2.1.3, for either a legacy firewall migration or a greenfield deployment use case, with the Customer team prior to the production deployment event to validate the accuracy of the NGFW configuration. This time must be scheduled in advance and in a single session of two (2) hours in length.

If the number of migrated Security/NAT rules from the legacy firewall exceeds the service parameter, as defined in Section 2.1.3, Palo Alto Networks will provide guidance on and collaborate with the Customer to prioritize which migrated rules will be reviewed.

***Note:** The Customer is responsible for the review of any remaining rules and providing written confirmation to the Palo Alto Networks team prior to scheduling the cutover event or working with Palo Alto Networks to procure additional services to complete that task.

Palo Alto Networks will provide a predefined Deployment Playbook and Validation Plan, as defined in Section 3, and perform one (1) review with the Customer team for the addition of customer specific requirements and feedback. The final Deployment Validation Plan will be mutually agreed to prior to moving to the next phase of the project.

2.5. Production Deployment

Palo Alto Networks will assist the Customer in performing one (1) production deployment event, of up to eight (8) hours, scheduled during or after business hours. The purpose of this will be to introduce the Palo Alto Networks NGFW into the Customer environment.

Post introduction, the traffic flows will be redirected to the newly introduced Palo Alto Networks NGFW and the legacy system removed from the network. This will include assistance with verification of functionality and troubleshooting any production issues during Customer application testing. If required, the Consultant will assist the Customer and the Palo Alto Networks Technical Assistance Center (“TAC”) to raise cases as needed.

2.6. Knowledge Transfer

Palo Alto Networks consultant will provide up to four (4) hours of knowledge transfer. This time must be scheduled post-production deployment, in advance, and in sessions two (2) hours in length at a minimum.

2.7. Documentation

Palo Alto Networks will provide a predefined As-Built Configuration, as defined in Section 3, and perform one (1) review with the Customer team for the addition of customer specific feedback.

2.8. Service Specific Customer Obligations, Assumptions and Exclusions

Customer Obligations

Prior to the delivery of the Services, Customer will ensure that:

- All purchased Palo Alto Networks Products (not demo or evaluation) are in a state of readiness for configuration (racked, stacked, powered, cooled, and cabled).
- All Palo Alto Networks Products are registered on the Palo Alto Networks support site.
- All Palo Alto Networks licenses and activation codes are available to be utilized.

Assumptions

The following assumptions will apply to the Services:

- All implementation activity will follow Customer's change control processes, as coordinated by Customer's SPOC.
    - Ensure legacy firewall configurations to be migrated can be frozen (no network or policy changes) no less than ten (10) business days prior to the production deployment.
    - Identify critical applications, develop their own deployment and/or application test plans, and facilitate appropriate testers/support personnel for the production deployment event.
- PAN-OS software release recommendation will be based upon generally available hardware and software features as defined in the Requirements.
- If required, upgrade existing Panorama Management system(s) to a version of software compatible with the NGFW software
- Existing Security Profiles, or "Day 1" Security Profiles, will be used as applicable.
- Existing URL Filtering profiles will be used as applicable.
- Palo Alto Networks will work with the Customer to integrate into the existing networking environment within the limitations of the Product. Any changes to non-Palo Alto Networks systems in this environment are the responsibility of the Customer.
- If dynamic routing tables are in use in the legacy network, the migrated configuration will be based on point-in-time routing data that may not be fully accurate at the time of implementation.

Exclusions

This Service Description is based upon, and is subject to, the following exclusions:

- Security architecture or design services and/or documentation.
- Legacy Security policy conversion for more than one (1) legacy firewall or virtual system/context.
- Creation of new Security/NAT rules for more than one (1) Palo Alto Networks NGFW/virtual system.

- "Consolidation" migrations. Palo Alto Networks will not migrate rules, or networks, from multiple source legacy firewalls to consolidate to a single Palo Alto Networks NGFW.
- "Partial" or "Split" migrations. Palo Alto Networks will not migrate a subset of rules, or networks, on any defined firewalls to be split across multiple Palo Alto Networks NGFWs/virtual systems.
- "Iterative" migrations, that is, Palo Alto Networks will not perform additional iterative migrations beyond the first one for any given legacy configuration.
    - Customer will track/document all changes on the existing configuration from the time the initial configuration is provided to Palo Alto Networks until the production cutover event.
    - Palo Alto Networks will incorporate these changes during the Customer change freeze period prior to the production cutover event based on Customer provided documentation.
- Review of all migrated rules if the number of migrated rules exceeds the parameters defined in Section 2.1.3.
- Redeployment of Palo Alto Networks products due to hardware sizing of the original purchase.
- Upgrade or deployment of Panorama Management system(s).
- Configuration of new Security or URL Filtering profiles.
- Development of Customer specific Application Test Plan.
- Development of Customer specific Deployment Plan for non-Palo Alto Networks activities.

The Palo Alto Networks part number covered by this Service Description is:

SKU	Description
PAN-CONSULT-NGFW-QS-PA4XX	QuickStart Service for NGFW, PA-400 Series - includes one (1) cutover

3. Deliverables

The following Deliverables will be provided in accordance with the Services:

PROJECT DELIVERABLES	
Project Deliverable	**Deliverable Criteria**
Project Plan	• Capture project management requirements ○ Milestones ○ Task/activities ○ Owners ○ Timeline

Technical Requirements Document (“TRD”)	Upgrade ● Capture system/PAN-OS upgrade requirements ○ Existing/new hardware systems ○ Existing/proposed PAN-OS versions ○ New system configuration changes to support upgrade - if required ● Capture upgrade verification requirements ○ Configuration upgrade validation ○ Hardware upgrade validation ● Establish timeline for the Customer to provide required information Deployment ● Capture foundational configuration requirements ○ High Availability (if required) ○ Network integration (interface and routing configuration) ○ Security Zones (as required to support the policy development activities) ○ Administrative authentication ○ Log Forwarding, Monitoring and Alerting ○ Security Profile Group (Day 1 configuration) ○ PAN-OS/content version update (if required) ● Capture Panorama integration requirements ○ Device Group - identify if using existing or new to be created ○ Template Stack - identify if using existing or new to be created ○ Templates - identify if using existing or up to three (3) new to be created ● Capture NAT/Security rules requirements ○ New rules development ■ Review Security/NAT rule functionality ■ Establish new Security/NAT rule documentation process ○ Legacy firewall migration ■ Review Security/NAT rule functionality ■ Review legacy firewall migration process ■ Identify legacy firewall system, OS version, and files required for migration ● Establish timeline for the Customer to provide required information
Deployment Playbook* - based on TRD * Customer to develop their own deployment plan	● Capture production deployment requirements ○ Production change event timing ○ Production change event success and roll-back criteria ○ Palo Alto Networks steps for deployment and roll-back
Deployment Validation Plan* - based on TRD * Customer to develop their own application specific test plan	● Capture production deployment testing requirements ○ Baseline network reachability/traffic flow to/from NGFW ○ NGFW High Availability failover/failback - if required ○ Verification of other configured functionality per TRD ● Identification of critical applications/flows - as provided by the Customer ○ Key Customer testing/support resources for critical applications/flows
As-Built Configuration Document	● Document the “as implemented” configuration of the deployed NGFW(s)

4. Project Resources and Designated Place of Work

Palo Alto Networks will assign project resources with the appropriate skills to deliver the Services and agreed upon Deliverables including, but not limited to, a project manager to serve as a single point of contact for the administration and management of the Deliverables. Palo Alto Networks resources may be subject to change at any time throughout the project, and Customer will be notified by Palo Alto Networks as soon as practicable of any such changes.

5. Travel Expenses for On-Site Work

The Services will be performed remotely. Travel and Expenses ("T&E") are not included in the price of the Services. Any travel by Palo Alto Networks will be mutually agreed upon before the travel occurs. Fees for travel-related costs are purchased and billed separately.

6. Scheduling

Palo Alto Networks resources work a normal work day of eight (8) hours and will adhere to the Customer's local business hours. In addition, Palo Alto Networks resources will adhere to the local Palo Alto Networks office holiday schedule. Any Services performed after normal business hours and on weekends must be approved in advance by Palo Alto Networks management.

Cancellation of a working session without a minimum of two (2) business days advance notice may cause: (i) delay in the performance of the Services; and (ii) risk the completion of the Services within the term of this Service Description. In the event of a delay due to a late cancellation, Customer may be required to purchase additional Services to complete the project. Any delays due to Customer's late cancellation shall be at no fault of Palo Alto Networks.

7. General Customer Obligations, Assumptions and Exclusions

Palo Alto Networks obligations, and the Services, are subject to Customer complying with the Customer obligations, assumptions and exclusions listed below. Successful and timely completion of the Services are subject to Customer meeting its obligations under this Service Description and Palo Alto Networks shall not be responsible for any delay due to Customer's non-compliance of its obligations.

Customer Obligations

Prior to the delivery of the Services, Customer will:

- Provide a project manager or other single point of contact ("SPOC") for the project who will be responsible for:
    - Providing all information, as requested by Palo Alto Networks, in a timely manner.
    - Acting as the central point of contact to Palo Alto Networks.
    - Coordination of Customer resources engaged in the project. Customer's technical resources should be qualified on Palo Alto Networks Products.
- Be responsible for procurement of any and all licenses for the Palo Alto Networks Products and provide to Palo Alto Networks professional services consultant(s) upon request.
- Provide Palo Alto Networks professional services consultant(s) with existing and up to date documentation including, but not limited to: topological diagrams, design documentation, up-to-date configurations, and change management policy documentation.

- Advise Palo Alto Networks of any:
    - Special security, health, and safety matters applicable.
    - Relevant project management meetings related to the project and/or Services, and permit Palo Alto Networks to attend such meetings as appropriate.
- Be responsible for managing all other vendors including, if applicable, Customer's managed services partner or systems integrator.
- Be responsible for any and all configuration changes to any non-Palo Alto Networks Products.
- Provide prompt written notice to Palo Alto Networks as soon as Customer becomes aware or has reason to believe that: Customer will not meet any of the Customer obligations under this Customer Obligations section, and/or if any of Palo Alto Networks assumptions will not occur or are inaccurate.
- Provide any additional equipment, such as network analyzers, test equipment and/or laboratory equipment that are not provided by Palo Alto Networks, but necessary to perform the Services.
- Ensure that Palo Alto Networks personnel may access and use Customer's and third-party licensors' proprietary materials as necessary for Palo Alto Networks to perform the Services. Customer warrants and represents that it has the right and authority to grant such access and use to Palo Alto Networks and hereby grants Palo Alto Networks the rights to use and access such proprietary materials as needed for Palo Alto Networks to perform the Services.

Assumptions

Throughout the delivery of the Services, Customer will:

- Upon request or as needed, provide access to the skilled subject matter and technical experts within Customer's (or their third-party vendor) organization for Palo Alto Networks to perform the Services.
- Perform all responsibilities and obligations specified under this Service Description in a professional workmanlike manner to facilitate timely completion of the Services.
- Provide direct remote access to the Palo Alto Networks equipment to be worked on via a Palo Alto Networks owned laptop.
    - Where direct remote access cannot be provided to Palo Alto Networks owned laptops, Customer shall provide alternative laptops with appropriate capabilities and connectivity or other functionally equivalent connectivity.

Exclusions

This Service Description is based upon, and is subject to, the following exclusions:

- The Services will not commence until Palo Alto Networks has received a non-cancellable PO for the Services.
- Palo Alto Networks is responsible for providing only the Services with the associated tasks and Deliverables described in this Service Description. Palo Alto Networks shall have no responsibility for other contractors or third parties engaged by Customer or

another third-party during delivery of the Services unless expressly agreed to in writing.
- Palo Alto Networks shall not be responsible for any delays caused by Customer or any third-party.
- Services are non-transferrable.

8. Fees and Payment

If Customer is purchasing the Services directly from Palo Alto Networks, payment terms for the Services are subject to the terms set forth in Section 2 of the Professional Services Agreement. Fees for Services purchased through an authorized reseller or distributor shall be paid directly to such authorized reseller or distributor.

9. Terms and Conditions

Palo Alto Networks professional services shall be subject to the Professional Services Agreement, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/palo-alto-networks-professional-services-agreement.pdf, unless the parties have entered into a separate written agreement that is identified as the governing agreement (either, "Agreement").

In either case, the applicable Agreement shall be incorporated by reference into this Service Description. In the event of any material conflict between the terms in the Agreement and the terms in this Service Description, the terms in this Service Description shall control.

3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com