SERVICE DESCRIPTION

Palo Alto Next Generation Firewall Deployment Service

Service Scope

Trustwave Implementation Services (“Services”) provide a set of offerings focused on the plan, design, and implement phases of your Palo Alto Next Gen Firewall solution. Trustwave implements the best practices vital to any successful security rollout and assists in effective maintenance of security solutions

The Services include specific pre-defined deliverables and will be completed at a time mutually agreed to between Client and Trustwave. The objective of the Services is to implement a firewall solution which may or may not encompass the entire Client environment and health assessment for the deployed environment.

The Trustwave project team will approach this engagement with the following perspectives in mind:

- Provide a practical approach to project execution;
- Maintain discipline and structure without constraining the project effort;
- Frame the project within the strategies of Client’s business requirements.

Trustwave has defined the effort into five (5) logical phases:

- Phase 1 – Project Initiation
- Phase 2 – Architecture
- Phase 3 – Implementation/migration
- Phase 4 – Knowledge Transfer
- Phase 5 – Maintenance (optional)

Assumptions

The following assumptions have been made in anticipation of this effort:

- Work under this SOW will be performed at Client’s facilities located at **CLIENT’S PREFERRED ADDRESS (to be identified to Trustwave)** except for any project-related activities which Trustwave and Client agree would be best performed remotely or at Trustwave’s premises in order to complete its obligations and responsibilities under this SOW.
- Any additional fees will be first agreed to in writing by Client.
- Trustwave will provide the Services under this SOW during normal business hours, 8:30 AM to 5:15 PM, local time, Monday through Friday, except holidays.
- Client provides sufficient access to the hardware and software environments being used for the project, including network connectivity and required authorizations.
- Client will provide resources with sufficient data security knowledge for this project.
- Client ensures sufficient security and compliance user participation.
- Client ensures sufficient access to Database administrators, Network and System Administrators as needed.

- Client will ensure that a proven backup and recovery strategy is in place for the systems being upgraded.
- Client will ensure that all hardware & software requirements have been met and configuration recommendations have been followed, prior to the start of the Project. Client acknowledges that Palo Alto Next Generation Firewalls will not be installed without minimum specifications being met and may not perform optimally unless system sizing recommendations have been met. Any delays encountered as a result of system specifications or recommendations not being met are the Client's responsibility.
- Client will test the Palo Alto solution according to the schedule and procedures outlined jointly with Trustwave.
- Client and Trustwave will ensure the steps outlined in the project plan are achieved in a timely manner.
- To complete certain Tasks and Deliverables under this engagemnt, Trustwave may request access to specific servers, network equipment, etc., as needed. Such access and related activities will only be performed with Client's explicit authorization, and always under direct Client supervision.
- Where used, "Duration" refers to man effort and not elapsed time.

Exclusions

- Trustwave will not provide Structure cabling, UPS, Patch Cords or Racks.
- Offering does not include performing Proof of Concept effort.
- Offering does not include customization or plug-in, (e.g. report, API, alert) unless otherwise stated.
- Offering does not include whole network or infra redesigning effort.
- Offering does not include Load/Performance testing.
- Offering does not include Vulnerability Testing/Penetration Testing.
- Offering does not include external backup, logging and monitoring solution.
- Support for operation tasks, such as change request, is not part of the scope. Username and password shall be handed over to customer operation team to perform operation tasks (e.g. check log, implementing Change Request, add/edit/remove policy).
- The Services do not include an assessment of the Client's organization, personnel, or IT infrastructure compliance to existing policies, practices, standards, guidelines, processes, or procedures, and is not intended to provide assurance of compliance with any industry, regulatory, or legislative requirements
- Any additional actions not defined in this description.
- Services in excess of the man-hours scoped in the order form.

Facilities

Client will provide Trustwave and its personnel with facilities that Trustwave may reasonably require to perform the Services, in particular: supplies, furniture, computer facilities, telephone/fax communications, and broadband access via network connectivity capability and other facilities while Trustwave is working on the project. The Trustwave project team will be located in an area adjacent to Client's subject matter experts and technical personnel and all necessary security badges and clearance will be provided for access to this area. Client will be responsible for ensuring that Client has appropriate backup, security and virus-checking procedures in place for any computer facilities Client provides or which may be affected by the Services.

Completion Criteria

Trustwave will have fulfilled its obligations under this SOW when any one of the following occurs:

1. Trustwave accomplishes the activities defined in the scope, in accordance with the terms and conditions set forth in the agreement between the parties, including but not limited to the warranties contained therein, including delivery to Client of the Materials agreed to, if any; or
2. Trustwave provides a certain number of man-hours of Services as specified in the order form;
3. Client or Trustwave terminates the project in accordance with the provisions of the Agreement; or
4. The end of the term specified in the order form.

Project Phases & Timelines

This section defines the major tasks for the project. The appropriate estimate, based on Trustwave's knowledge of the date of signatures in the scoping document and/or order form, will likely outline man-hour initiative as follows:

Phase 1: Project Initiation

Estimated duration to be agreed by the parties.

The purpose for this activity is to kick off the project and set expectations with the Client

Trustwave will work with the customer to review the current infrastructure, change control, and other project processes and expectations. Trustwave will initiate data gathering process to receive initial information about the customer environment.

	Task	Participants
1	Set project expectation with Client	Client and Trustwave
2	Provide initial environment information	Client

Data gathered from Client's environment:

a) Complete inventory of all networking devices, including but not limited to routers, switches, firewalls, and wireless devices
b) Device model, software version, firmware revision, IP addressing, MAC addressing
c) Current state network design

Note: For Clients that cannot provide the information above, an assigned Network Engineer should be scoped.

Phase 1 Deliverables:

- Initial Project Plan
- Network topology documentation

Phase 2: Design & Architecture

Estimated duration to be agreed by the parties.

The purpose of this activity is to help the project team scope and document the Palo Alto deployment. The Trustwave project team will work with Client to gather necessary data from network administrators and designers.

Phase 2 Requirements

- Complete the pre-engagement Data gathering

Phase 2 Tasks:

	Task	Participants
1	Existing topology documentation	Client
2	Scoping of new deployment functions and requirements	Client and Trustwave
3	Collection of key use cases and requirements such as High Availability or Disaster Recovery consideration	Client and Trustwave

5	Documentation of key applications/requirements and a test plan to ensure full validation during the deployment	Client and Trustwave
6	Development and documentation of a network diagram that details equipment and deployment location	Client and Trustwave
7	Creation of deployment design document	Trustwave
8	Update of project plan with timelines and responsibilities	Trustwave

The design document and accompanying network diagrams may cover the following elements

- Software Recommendation
- Network Topology
  - Current Topology
  - Future Topology
  - Migration Strategy
  - Global High-Level Topology
  - Any site-specific differences
  - High Availability
  - Network Structure
  - Network Interfaces
  - Zones
  - VPNs
  - Routing
  - Private Cloud
  - Public Cloud
- Management
  - Panorama Platforms
  - Device Groups
  - Templates
  - Logging
  - Rule Tuning Preparation
  - Dynamic Updates
  - Threat Prevention
  - Antivirus
  - Anti-Spyware
  - Vulnerability
  - File Blocking
  - URL Filtering/PANDB
  - WildFire/Cloud/WF-500
- Palo Alto Networks Next-Generation Features
  - App-ID
  - User-ID
  - GlobalProtect
  - SSL Decryption
  - Zone Protection Profiles and Denial of Service Protection
  - Quality of Service
  - Aperture
  - AutoFocus
  - Third-Party Integrations

Phase 2 Deliverables:

- Project Plan for migration
  - Migration/cutover task list
  - Roles and responsibilities
  - Timeline and milestones
- Overview and detailed network diagrams
- Use case/key requirements documentation and approach to resolve

Phase 3: Implementation and Validation

Estimated duration to be agreed by the parties.

During the implementation phase Trustwave will, with Client assistance, convert the existing firewall infrastructure to the new design and equipment scoped in Phase 2.

Guided by the agreed-on design documentation, the implementation phase will follow the Phase 3 Tasks outlined below. Trustwave will validate implementation according to the design document and remain onsite for up to one half day as well as provide remote standby where needed.

Phase 3 Requirements

The following must be completed prior to start of work:

- Client has agreed on the design documentation
- Hardware and software platforms prepared and available for implementation
- Designate a Project Technical Lead who will be the primary contact during the implementation
- Have appropriate change requests approved (if needed) and agreement on change control windows

Phase 3 Tasks

	Task	Participants
1	Firewall Policy Conversion - Trustwave will manage the conversion of current security policies (rules) and their elements (addresses, application objects and groups) for the migration from Client's legacy system configuration to the targeted Palo Alto NG Firewall configurations.	Client and Trustwave
2	Validate Conversion – Work with the Client closely to conduct a validation session to validate the policy conversion before migrating any production systems.	Client and Trustwave
3	Migration to Palo Alto Networks Platform - Trustwave will assist Client in performing scheduled migrations, including assistance with troubleshooting for production issues, verification of functionality, and assistance with Trustwave technical customer support (TAC) cases as needed.	Client and Trustwave
4	Post-Migration Threat Assessment – Trustwave will perform a post-migration Threat Assessment of live traffic. Based on the Analysis, Trustwave will provide additional documented changes to configurations to further secure the Client network. The results of the Threat Analysis will be appended to the approved design documentation	Trustwave

The migration task (#3) above may include the following tasks

User-ID

Trustwave will implement User-ID function in the Target User Domain as defined in the design documentation. Trustwave will provide User-ID to IP mapping. Tasks will include:

- Map User-ID to IP address information for the number of Authentication domains as defined in the design.
- Collect User Group information per defined authentication domain.
- Requirements review and definition of User domain environments.
- Use of system logs to gather User and IP address information.
- Map User-ID to IP information.

Any Authentication Domains not specified in the HLD are considered out-of-scope for this project.

App-ID

Trustwave will implement App-ID functionality in the Targeted Network/Policy.

- Convert all well-known applications from Port-based rules to application-based policies.
- Isolate all unknown TCP/UDP traffic rules.
- Perform three (3) separate App-ID scans of port-based policy and log information for determination of applications for each rule.
- Create initial App-ID policy and clone port-based rules after first App-ID scan.
- Confirm and modify App-ID policy on a second scan performed at an agreed scheduled time, subsequent to initial App-ID policy creation.
- Finalize and modify App-ID policy on a third scan performed at agreed scheduled time, subsequent to completion of the second App-ID scan.
- Remove Port-based rules.

Unknown TCP/UDP investigations and creation of Custom App-IDs are considered out-of-scope for this project

URL Content Filtering PANDB

Trustwave will configure PANDB Content Filtering on designated Palo Alto Network Perimeter Devices:

- Manually convert existing Content Filtering rules to PANDB URL Filtering profile.
- Block agreed high risk categories.
- Review with Client existing URL Filtering rules and determine necessary parameters for mapping into Palo Alto Networks URL Filtering categories.
- Manually convert an existing URL Content service to PANDB.
- Create and implement a PANDB URL Filtering policy.

URL Content filtering requires access to a Client subject matter expert help ensure mapping of categories between technologies is as accurate as possible.

SSL Decryption

Trustwave will assist in deployment and development of an SSL Decryption policy. Trustwave will deploy an active SSL Decryption policy for high risk categories as defined in the design.

- Enable SSL Decryption policy per select Palo Alto Network devices.
- Confirm actively encrypting SSL traffic via Monitor tab of defined categories.
- Palo Alto Networks to deploy Decryption defined categories.
- Review meeting with Client to determine SSL Decryption policies for implementation.
- Create SSL Decryption policy for agreed high risk categories.
- Create SSL Decryption Profile to handle exceptions.
- Test SSL Decrypt policy for deployed Categories.

- Provide knowledge transfer to Client for implementation of additional SSL Decryption categories beyond the initially defined categories.

Trustwave will develop and deploy initial SSL Decryption policies as defined in the design documentation. Additional SSL Decryption policies beyond those defined in the design can be developed by the Client.

Note: Decryption policies may be limited by the perimeter hardware capabilities (i.e. CPU and processing power).

For the avoidance of doubt, Decryption of "all URL Categories" is considered out-of-scope for this task.

Phase 3 Deliverables:

- Completed implementation as per design document (Phase 1).
- As built "run book": updated design documentation with any agreed changes made during deployment.

Phase 4: Knowledge Transfer

Estimated duration to be agreed by the parties.

Trustwave will assist Client in understanding the deployed solution. This will be achieved through a handover process. Knowledge transfer to the team occurs interactively during the engagement and covers the installation, configuration, and basic administration of the Firewall solution.

Phase 4 Tasks:

	Task	Participants
1	Review as-built document. This document consists of non-default setting/parameter configured during deployment, not a how-to guide.	Client and Trustwave
2	An overview of Knowledge Transfer Activities with reference to implementation solution.	Client and Trustwave
3	Review the actions taken and decisions made during the validation phase.	Client and Trustwave
4	Review the actions and remediations performed over the course of the project as part of an operations knowledge transfer.	Client and Trustwave
5	Review Procedures for contacting Trustwave Maintenance Support where applicable.	Client and Trustwave

Phase 5: Maintenance Health Check

Estimated duration to be agreed by the parties.

On a selected periodic basis, Trustwave staff will remotely access each of the security products deployed at the customer site to perform a system review.

Trustwave will review the following as part of a health check service:

- Current patch levels.
- Audit log review
    - Identification of any performance issues.
    - Identification of any potential security issues.
    - Identification of any potential server (hardware) issues.
- Fully shadowed rules check.
- Partially shadowed rules check.
- Expired or disabled rules check.
- Check for unused connections.
- Old or unused policies verification and recommendation, as applicable.
- Inconsistent naming conventions.
- Review rules that disallow access to the firewall.
- List of most used rules/recommendation on any rule order changes.

Note: Additional checks are regularly added based on Trustwave's best practices for deployment and maintenance.

Phase 5 Deliverables:

- Health Status report.
- Recommended remediation activities (if applicable).

Project Staffing

Trustwave will coordinate the Trustwave resources and provide project management inputs to Client's project manager.

Roles and Responsibilities

Success of this project is dependent on our mutual understanding of roles and responsibilities. This section details Client and consultant participation and responsibilities.

Client Project Manager

Prior to the start of this engagement, Client will designate a Client Project Manager to act as the focal point for Trustwave communications relative to this project and have the authority to act on behalf of Client in all matters regarding this project. Client's Project Manager's responsibilities include:

- Manage Client personnel and responsibilities for this project.
- Serve as the interface between Trustwave and all Client departments participating in the project.
- Administer the Project Change Control Procedure with the Trustwave Implementation Manager.
- Participate in project status meetings.
- Help resolve project issues and escalate issues within Client's organization, as necessary.
- Review with the Trustwave Implementation Manager any of Client's invoice or billing requirements. Requirements that deviate from Trustwave's standard invoice format or billing procedures may have an effect on price and will be managed through an Addendum.

Client IT Responsibilities

- Provide supervised access to hardware, software, database, and network, when needed.
- Validate deployed solution and assume maintenance at the end of implementation phase.

Client Network Security Manager

- Provide appropriate subject matter experts to participate in the project.
- Provide policy and reporting requirements.
- Review and approve solution designs.
- Design and develop any new change control processes required to maintain Palo Alto solution.
- Approve the promotion of the system to production.

Trustwave Project Management

- Create project plan with timelines as well as roles and responsibilities based on Design Document.
- Align Trustwave resources with tasks and coordinate work schedule. Work with Client Project manager to ensure appropriate resources are booked as required while deployment work is in progress.
- Lead weekly project status meetings to ensure all parties are in line with progress and next steps.
- Track project progression and measured milestones to ensure timely delivery.

Trustwave Network Engineer

- Provide input in requirements gathering to tailor Palo Alto solution to Client environment.
- Provide expertise in deployment and customization of deployed hardware and software.
- Provide product knowledge transfer to Client staff. This supplements formal Palo Alto training with specifics of how solution was customized for Client's network.
- Provide standard product documentation, as necessary.
- Provide all Trustwave deliverables for signoff.