DIR-TSO-4095 Appendix D

Service Agreement Statement of Work #xxxxxx

SAMPLE Palo Alto Networks Firewall Conversion and Installation

CUSTOMER_NAME

solid border

NETWORK SECURITY RESELLER

solid border
NETWORK SECURITY RESELLER

+

paloalto NETWORKS

Summary

Solid Border has been contracted to provide firewall configuration, installation and knowledge sharing services to Customer_Name for Palo Alto Networks firewall(s). Due to the nature of an RFP response, this scope of work is considered in process. A complete, more detailed scope of work will be provided if awarded.

The primary objectives for these services are to: create a new firewall policy ruleset based on an existing firewall rules, setup & configure Palo Alto Networks firewall(s), Panorama (optional centralized reporting), create security profiles and to setup a best practice gateway security framework.

For this project, we have quoted a bundle of X days.

Preparation

Solid Border will assign a PCNSE certified staff (Palo Alto Certified Network Security Engineer - https://www.paloaltonetworks.com/services/education/pcnse) to this project.

Customer_Name will be responsible for the following prior to the start of the project:

- Providing Solid Border with a current firewall configuration
- Maintaining a list of servers/services to be tested internally and/or remotely both before and after the firewall install
- Notifying any ISPs of a firewall conversion
- Notifying site-to-site VPN partners of a firewall conversion
- Scheduling and notification of any outage windows
- Providing SSL certificates for client VPN use (wildcards preferred), if applicable.
- At least one Windows Server that is part of the AD domain available to install lightweight User-ID Agent services. These may be an existing or new server(s).
- The availability of someone to create a service account for use with LDAP and User-ID integration, if an account has not already been created.

Planning / Pre-Deployment

To kick off this project, Solid Border and Customer_Name will have an onsite or phone conference to discuss both plan of action and timetable. For this meeting, we will discuss and cover any requirements, contacts, and scheduling. We will discuss the existing environment and desired final network picture. Network diagrams are helpful, but not required.

During this meeting we will discuss if a positive or negative security model will be the best fit for how Customer_Name will manage their security policies. Solid Border will use this information to work on a security rule set plan.

Some of this meeting may fall outside the scope of firewalls and into network and routing design. Solid Border is very comfortable working with Customer_Name IT staff to make sure everyone is on board with the planned architecture and deployment strategy to maximize security, resiliency and efficiency.

After the initial meeting, Customer_Name will need to provide Solid Border with their most recent, existing firewall configuration, as well as any information regarding site-to-site VPN tunnels, their priorities, and client VPN information.

It will be the responsibility of Customer_Name to get the Palo Alto Networks firewall(s) and Panorama racked and configured with an initial IP address for each firewall and Panorama for management use. Remote access for Solid Border is preferred to begin initial setup steps -- updates, general interface setup, and HA configuration, if applicable. Either VPN or a locked down firewall rule with direct access to the new firewall will be acceptable.

Content scanning such as IPS, Anti-malware scanning, URL filtering and Wildfire will be setup with our recommended settings (set to block), unless otherwise requested. Routing tables and any static or dynamic routes will be reviewed for clarifications.

We will also provide instructions for setting up User-ID on a Customer_Name Windows Server to provide the firewall with user and group awareness. Optionally, we will configure LDAP, Kerberos and/or RADIUS for authentication-use if Customer_Name decides to use Captive Portal or GlobalProtect, the built-in client VPN.

Conversion

Once Solid Border has a copy of the existing firewall configuration, we will use a combination of tools provided by Palo Alto Networks, and our own tools to create a base configuration for the Palo Alto Networks firewall(s). Remotely we will stage the firewall(s) with this configuration and ready the box for production.

Installation and Deployment

Migrating to the PA firewall remains to be scheduled. We assume an after-business-hours firewall installation and will work with whatever timetable Customer_Name and Solid Border agree upon. Solid Border will be onsite for the physical migration.

We strongly recommend opening a trouble-ticket or notifying any ISPs, VPN partners or VPN clients that are used in advance of the migration.

Once the cut-over has started, Solid Border will begin testing connectivity and troubleshooting.

It is a very good practice to have a testing checklist to be used both before and after a firewall swap to verify service/application availability. The creation and testing of this list is the responsibility of Customer_Name.

Once the cut-over has started, and previously identified services are operational, Solid Border will begin bringing up site-to-site VPN tunnels. The priorities of these connections will need to be determined

Post-Installation/Migration

Solid Border will be available either onsite or remotely the following business day to ensure a successful migration and troubleshoot any technical issues that arise.

Documentation and network architecture diagrams, if applicable, are the responsibility of Customer_Name. Solid Border can answer any questions related to the setup, configuration, migration process, specific rules, specific NATs, security profiles, or other Palo Alto Networks-related questions after the installation.

The remaining days of onsite services will be comprised of remediation of any issues related to the firewall conversion, as well as continuing setup of User-ID, additional

security features, sharing best practices, and knowledge transfer. Meetings will have a strong focus on usage, care-and-feeding, upgrade procedures and troubleshooting. We will use your data to show you your traffic and how to create filters to pinpoint data quickly, among other troubleshooting tips.

All remaining time can be used for consulting and training (no materials, as Solid Border is not a substitute for classroom-style training). This ad-hoc training can be used to focus on diving deeper into whichever features are most important Customer_Name. Options include, but are not limited to: QoS, reporting, VPN, log integration, IPS, WildFire, Application Filtering, security policy hardening, long-term security policy planning, User-ID, client VPN, and/or troubleshooting.

Terms & Conditions

DIR

Terms are limited to the terms and conditions referenced in Appendix A for Texas DIR contract DIR-TSO-XXXX.

TRAVEL

All travel and expenses for this engagement have been included in the daily rate.

PRIVACY AND CONFIDENTIALITY

We take great responsibility in respecting the privacy, trade secrets, and confidential and proprietary data of our Customers. All non-public data, databases, reports, policies, procedures and other information (including Customer_Name security systems and procedures) relating to Customer_Name's business, operations, proprietary information, systems, networks, suppliers, contractors, or customers learned by or acquired by Solid Border as a result of performance of the Services and the Customer IP are "Customer Confidential Information". Customer Confidential Information shall not be used by Solid Border for any purpose other than provision of these Services and shall not be disclosed by Solid Border to anyone other than its own employees, who have a need to know the information in order to perform the Services and are bound by Solid Border to keep such information confidential. Solid Border shall protect Customer Confidential Information with the same degree of care that it uses to protect its own most confidential information, but in no event less than a reasonable standard of care.

solid border
NETWORK SECURITY RESELLER

+

paloalto NETWORKS

About Solid Border

Since 2002, Solid Border has been bringing efficient & reliable network security products to the broad range of customers we serve. Ever-changing technology means you can't rely on resellers who bury their engineers' voices under layers of bureaucracy. The products we offer have been hand-selected by our engineers because they actually make your work-life easier. We know; we've used them. From start to finish, Solid Border is there to help you build a safer and more secure network, so you can get down to business.

References specific to customer's size and industry are available upon request.

solid border
NETWORK SECURITY RESELLER

+

paloalto NETWORKS

Acceptance Signatures

Once signed by both Customer_Name and Solid Border, this statement of work will be approved for any services provided within the Scope. Any changes to the Scope must be approved in writing prior to commencement of work and shall be attached to this document. This Statement of Work precedes all documents of engagement unless amended and signed by both parties.

Signature	Signature
Printed Name	Printed Name
Date	Date
Solid Border, Inc	Customer_Name