**{{Customer}}**

**Palo Alto Networks Deployment**

***Network Integration As-Built Document***

***{{Month}},{{Year}}***

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

© 2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at http://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

**Table of Contents**

[Introduction 5](#_Toc22810824)

[Executive Summary 5](#_Toc22810825)

[Open Issues 5](#_Toc22810826)

[Platform 6](#_Toc22810827)

[Deployed Security Platforms 6](#_Toc22810828)

[Procured Systems 6](#_Toc22810829)

[Device Licensing 6](#_Toc22810830)

[PAN-OS Version 6](#_Toc22810831)

[Panorama Systems 6](#_Toc22810832)

[Panorama Licensing 6](#_Toc22810833)

[Platform Administration 7](#_Toc22810834)

[Network Integration 7](#_Toc22810835)

[Virtual Systems 7](#_Toc22810836)

[Virtual Router 7](#_Toc22810837)

[High Availability 8](#_Toc22810838)

[Interfaces 9](#_Toc22810839)

[Operational Interfaces 9](#_Toc22810840)

[Management Interfaces 9](#_Toc22810841)

[Logging Interfaces 10](#_Toc22810842)

[Security Zones 10](#_Toc22810843)

[IPSec VPNs 11](#_Toc22810844)

[GlobalProtect 12](#_Toc22810845)

[Portals 12](#_Toc22810846)

[Gateways 12](#_Toc22810847)

[HIP Profile Information 12](#_Toc22810848)

[Panorama 13](#_Toc22810849)

[Templates 13](#_Toc22810850)

[Device Groups 14](#_Toc22810851)

[Device Group Tree 14](#_Toc22810852)

[Log Forwarding 14](#_Toc22810853)

[Security Profiles 15](#_Toc22810854)

[Security Profile Groups 17](#_Toc22810855)

[{{Customer}} Security Profiles Configuration 17](#_Toc22810856)

[Dynamic Updates 17](#_Toc22810857)

[User-ID 17](#_Toc22810858)

[User-ID Sources 17](#_Toc22810859)

[Group Mapping Profiles 18](#_Toc22810860)

[SNMP 18](#_Toc22810861)

[SNMP Server Profile 18](#_Toc22810862)

[SNMPv2 Settings 18](#_Toc22810863)

[SNMPv3 Settings 18](#_Toc22810864)

[Reporting 18](#_Toc22810865)

[Cloud Services and Integration Pieces 19](#_Toc22810866)

[Cortex Data Lake 19](#_Toc22810867)

[Prisma Access / Prisma Public Cloud / Prisma SaaS 19](#_Toc22810868)

[Cortex 19](#_Toc22810869)

[VM Series 19](#_Toc22810870)

[AutoFocus 19](#_Toc22810871)

[Threat Vault 19](#_Toc22810872)

[Third Party Integrations 19](#_Toc22810873)

[Document Properties 20](#_Toc22810874)

[Contributors 20](#_Toc22810875)

[Revision History 20](#_Toc22810876)

[Palo Alto Networks Resources 21](#_Toc22810877)

[Customer Resources 21](#_Toc22810878)

**As Built Template Instructions**

This template is designed as a tool to help generate as built documentation for Palo Alto Networks Professional Services Consultants after completion of a firewall migration. The as built documentation is included in the firewall migration Silver and Gold bundles as a deliverable. Each final document should be highly customized to detail the specific installation and configurations of the Palo Alto Networks Security Platform integration into the customer’s environment. To maintain consistency and completeness, however, this template should be used across all of PSO.

The blue outdented italic notes are instructions for each section. Remove all template instruction notes before generating the final document. The standard blue text is example text for each section. Replace this with a description of customers deployment. Replace all instances of [CUSTOMER] with the customer’s name, and any other capitalized text in brackets with the correct information.

Remove any section that does not apply to the deployed solution, i.e. site to site VPNs or Cloud Services.

Introduction

The purpose of this document is to detail the specific configuration and installation of each Palo Alto Networks security platform in {{Customer}} environment.

Executive Summary

Provide a high-level description of the project in 1-2 paragraphs. Name the customer and the purpose in choosing and deploying the Palo Alto Networks solution. Use “find and replace” to substitute {{Customer}} with the value on the Title Page throughout this document. An example could be something like the following:

To better improve security and visibility into internet and DMZ traffic, {{Customer}} purchased and deployed four PA-5260 Palo Alto Networks security platforms. These were deployed in two data centers in a high availability pair. Palo Alto Networks Professional Services worked closely with the {{Customer}} team to deploy the Palo Alto Networks security platform in their New Jersey and Virginia data centers. Two ASA H/A pairs in each data center were replaced with a single multi vsys PA-5260 H/A pair managed by their existing VM series Panorama. The PA-5260 H/A pair secure communications between the internet, DMZ, and internal for {{Customer}} customers and users. The security policy is shared between the two sites for easier management and to ensure a synchronized configuration at each site in the event of traffic failover to ensure a consistent user experience.

Each PA-5260 H/A pair was installed in separate maintenance windows. In addition to migrating to the PA-5260s, load balancer and routing changes were implemented to allow for inspection of all traffic to the DMZ VIPs. This included net new interfaces, security zones, and security policies.

Detail any open issues such as remaining work or open Support tickets.

Open Issues

Each migration was successful. There are no open issues.

Platform

In this section, provide detail of the platform configurations including model, serial numbers, PAN-OS version and deployment locations. Also include Panorama, even if Panorama was already present in the environment.

This section of the document provides details of the deployed configuration of the Palo Alto Networks security platform in the {{Customer}} environment.

Deployed Security Platforms

All data in the following tables are examples. Fill in with appropriate customer level information.

This section describes the Palo Alto Networks platforms, physical and virtual, that have been deployed at each {{Customer}} location identified.

Procured Systems

Table 1 shows the security appliances with their corresponding locations, operating systems, and serial number information.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Device Name** | | **Platform Model** | | **Location** | **Serial Number** | |
| {%tr for item in t1%} | | | | | | |
| *{{item.t1devicename}}* | *{{item.t1model}}* | |  | | | *{{item.t1serial}}* |
| {%tr endfor %} | | | | | | |

Device Licensing

Table 2 shows the security appliances with their corresponding procured licensing.

Table 2 – Procured Licensing

|  |  |
| --- | --- |
| **Device Name** | **License** |
| {%tr for item in t2%} | |
| *{{item.t2devicename}}* | *{{item.t2licenses}}* |
| {%tr endfor %} | |

PAN-OS Version

Table 3 shows the version of PAN-OS installed on each security appliance deployed in the {{Customer}} environment.

Table 3 – Installed PAN-OS Version

|  |  |  |
| --- | --- | --- |
| **Device Name** | **PanOS Deployed** | **Notes** |
| {%tr for item in t3%} | | |
| *{{item.t3devicename}}* | *{{item.t3panos}}* |  |
| {%tr endfor %} | | |

Panorama Systems

This section describes the Palo Alto Networks Panorama systems, physical and virtual, that have been deployed at the {{Customer}} location identified. The Panorama systems are shown in Table 4.

Table 4 – Panorama Appliances

|  |  |  |  |
| --- | --- | --- | --- |
| **Device Name** | **Platform Model** | **Location to be Deployed** | **Serial Number(s)** |
| {%tr for item in t4%} | | | |
| *{{item.t4devicename}}* | *{{item.t4model}}* |  | *{{item.t4serial}}* |
| {%tr endfor %} | | | |

Panorama Licensing

Table 5 shows the Panorama appliances with their corresponding procured licensing.

Table 5 – Panorama Licensing

|  |  |  |
| --- | --- | --- |
| **Device Name** | **License** | **Role** |
| {%tr for item in t5%} | | |
| *{{item.t5devicename}}* | *{{item.t5licenses}}* | *{{item.t5role}}* |
| {%tr endfor %} | | |

Table 6 shows the version of PAN-OS deployed on each Panorama management appliance.

Table 6 – Panorama PAN-OS Versions

|  |  |  |
| --- | --- | --- |
| **Device Name** | **PAN-OS Deployed** | **Notes** |
| {%tr for item in t6%} | | |
| *{{item.t6devicename}}* | *{{item.t6panos}}* |  |
| {%tr endfor %} | | |

Platform Administration

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/firewall-administration.html>

Describe the administrator settings for Panorama and the firewall to include authentication type, admin roles and admin domains.

Table 7 shows the administrator settings for the Palo Alto Networks appliances.

Table 7 – Administrators

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Device Name** | **Name** | **Role** | **Auth Profile** | **Pass Profile** | **Role Profile** | **Access Domain** |
| {%tr for item in t7%} | | | | | | |
| *{{item.t7devicename}}* | *{{item.t7adminname}}* | *{{item.t7adminrole}}* | *{{item.t7authprofile}}* | *{{item.t7passprofile}}* | *{{item.t7roleprof}}* | *{{item.t7accessdomain}}* |
| {%tr endfor %} | | | | | | |

Panorama

<https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin.html>

If the customer has an existing Panorama, give a general description of the deployment, but detail the templates and device groups relevant to the project.

For the data center migration, {{Customer}} utilized their existing stand-alone M-500 series Panorama running in Panorama mode. Panorama currently manages 34 firewalls across the organization. All firewalls are managed using device groups and templates with no local configuration.

Table 24 shows the Panorama interface information.

Table 24 – MGT Port Settings

|  |  |  |
| --- | --- | --- |
| **Device Name** | **MGT Port Settings** | **Settings** |
| {%tr for item in t24%} | | |
| {{item.t24devicename}} | IP Address  Mask  Gateway  IPv6 address  Speed  MTU  Services  H/A Priority  Permitted IP | *{{item.t24mgmtIP}}*  *{{item.t24mgmtnetmask}}*  *{{item.t24mgmtgateway}}*  *{{item.t24mgmtipv6}}*  *{{item.t24mgmtspeed}}*  *{{item.t24mgmtmtu}}*  *{{item.t24mgmtservices}}*  *{{item.t24hapriority}}*  *{{item.t24mgmtpermittedips}}* |
| {%tr endfor %} | | |

Add a second table if additional interfaces are used on Panorama and list which function/service is configured on the interfaces.

Templates

[https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-firewalls/manage-templates-and-template-stacks.html#](https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-firewalls/manage-templates-and-template-stacks.html)

{{Customer}} is utilizing Template Stacks to manage their firewalls. The firewall specific template is at the top of the template stack with PROD-SHARED-SETTINGS at the bottom for the PA-5260 H/A pairs at each data center. The PROD-SHARED-SETTINGS template has the common configuration for all firewalls to share. This template is at the bottom of the stack in the event a more specific site configuration needs to be applied to the firewalls and override the common shared configuration.

Table 25 shows the Panorama template information.

Table 25 – Panorama Templates

|  |  |  |  |
| --- | --- | --- | --- |
| **Device Name** | **Template Name** | **Stack** | **Stack Members** |
| {%tr for item in t25%} | | | |
| *{{item.t25devicename}}* | *{{item.t25templatename}}* | *{{item.t25stackname}}* | *{{item.t25stackmembers}}* |
| {%tr endfor %} | | | |

Device Groups

<https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-firewalls/manage-device-groups.html>

Due to the similarity of the function and security policy at each data center, {{Customer}} is sharing the device group between data centers. The device group hierarchy for the inside virtual system is Shared > Prod > DMZ Inside. The device group hierarchy for the outside virtual system vsys is Shared > Prod > DMZ Outside. All objects are at the Shared > Prod device group level.

All security policies are pushed to both PA-5260 H/A pairs. The NAT policies are in the DMZ Outside device group but are targeted to their respective data center firewalls.

Device Group Tree

Table 26 represents the structure of the device groups.

Table 26 – Device Group Tree Structure

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Device Name** | **1st Tier** | **2nd Tier** | **3rd Tier** | **4th Tier** | **Master Device** |
| {%tr for item in t26%} | | | | | |
| *{{item.t26devicename}}* | *{{item.t26tier1}}* | *{{item.t26tier2}}* | *{{item.t26tier3}}* | *{{item.t26tier4}}* | *{{item.t26masterdevice}}* |
| {%tr endfor %} | | | | | |

Reporting

Describe the customers reporting settings. Include any customer reports created, email profiles and report groups.

Cloud Services and Integration Pieces

This section is devoted to the documentation of the configured Cloud Services and Plugin Integrations for Panorama. Include details such as version of plugin, configured region, subscription model, etc.

Cortex Data Lake

*< Enter details in an organized format. Could be a table, a bullet list, or a form. >*

Prisma Access / Prisma Public Cloud / Prisma SaaS

*< Enter details in an organized format. Could be a table, a bullet list, or a form. >*

Cortex

*< Enter details in an organized format. Could be a table, a bullet list, or a form. >*

VM Series

Amazon Web Services (AWS), GCP, Microsoft Azure, Oracle Cloud, Alibaba Cloud, and VMware NSX

*< Enter details in an organized format. Could be a table, a bullet list, or a form. >*

AutoFocus

*< Enter details in an organized format. Could be a table, a bullet list, or a form. >*

Threat Vault

*< Enter details in an organized format. Could be a table, a bullet list, or a form. >*

Third Party Integrations

This section is devoted to the documentation of the any third-party tools integrated into the Palo Alto Networks deployed solution. This can include an XML API integrations and technology partners such as Tufin.

Document Properties

This document is prepared for the sole use by {{Customer}}.

Contributors

Enter complete information for all people with their role, could include customer resources:

Role types: Author/Contributor/Reviewer

Title example: Professional Services Consultant

Table 45 – Contributors

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Role | Title | Contact Information |
| *John Doe* | *Pro-Serv* | *Sr. Professional Service Consultant* | [*jdoe@paloaltonetworks.com*](mailto:jdoe@paloaltonetworks.com) |
|  |  |  |  |

Revision History

Enter complete information for all revisions and be concise on comments:

Status types: Draft/In Review/Complete

Comments example: Initial draft/Added to Management and Routing sections/Draft complete – in review

Table 46 – Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Date* | *Revision* | *Changes By* | *Status* | *Comments* |
| *dd MON yyyy* | *<x.y>* | *<your name>* | *<status>* | *<comments on version/changes>* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Palo Alto Networks Resources

Palo Alto Networks has a team of resources committed to making the {{Customer}} deployment successful. The following individuals are assigned to work on the {{Customer}} deployment.

Describe each member of the Palo Alto Networks team, their role, and contact information.

Table 47 – Palo Alto Networks Resources

|  |  |  |
| --- | --- | --- |
| *Role* | *Name* | *Contact Information* |

|  |  |  |
| --- | --- | --- |
| *Professional Services Engineer* | *Engineer Name* | *engineer@paloaltonetworks.com* |
| *Professional Services PM* | *Project Manager Name* | *pm@paloaltonetworks.com* |

Customer Resources

Describe each member of the customer team, their role, and contact information.

Table 48 – Customer Resources

|  |  |  |
| --- | --- | --- |
| *Role* | *Name* | *Contact Information* |

|  |  |  |
| --- | --- | --- |
| *Customer Role Title 1* | *Customer Name* | *customer@company.com* |
| *Customer Role Title 2* | *Customer Name* | *customer@company.com* |