**{{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.

Table 1 – Procured Systems

|  |  |  |  |
| --- | --- | --- | --- |
| **Device Name** | **Platform Model** | **Location** | **Serial Number** |
| *«t1devicename»* | *«t1model»* |  | *«t1serial»* |

Device Licensing

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

Table 2 – Procured Licensing

|  |  |
| --- | --- |
| **Device Name** | **License** |
| *«t2devicename»* | *«t2licenses»* |

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** |
| *«t3devicename»* | *«t3panos»* |  |

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)** |
| *«t4devicename»* | *«t4model»* |  | *«t4serial»* |

Panorama Licensing

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

Table 5 – Panorama Licensing

|  |  |  |
| --- | --- | --- |
| **Device Name** | **License** | **Role** |
| *«t5devicename»* | *«t5licenses»* | *«t5role»* |

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** |
| *«t6devicename»* | *«t6panos»* |  |

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** |
| *«t7devicename»* | *«t7adminname»* | *«t7adminrole»* | *«t7authprofile»* | *«t7passprofile»* | *«t7roleprof»* | *«t7accessdomain»* |

Network Integration

Virtual Systems

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

If firewalls were deployed with multi vsys, describe the deployment below and fill in the appropriate tables.

Each {{Customer}} PA-5260 H/A pair is configured for multiple virtual systems. Each pair has three virtual systems defined. Inter-vsys communication is routed external from the platform.

* Vsys 1: Default vsys to be used for any configuration that needs to be shared across all virtual systems.
* VSYS-OUTSIDE: The outside vsys performs network segmentation between the internet and DMZ and internal resources. The outside vsys also handles NAT for inbound and outbound internet traffic for users and services.
* VSYS-INSIDE: The inside vsys performs network segmentation between each Windows and Linux DMZ, and internal resources.

Table 8 shows the {{Customer}} vsys deployment.

Table 8 – VSYS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device Name** | **VSYS ID** | **VSYS Name** | **Interfaces** | **Virtual Router** |
| *«t8devicename»* | *«t8vsysid»* | *«t8vsysname»* | *«t8interfaces»* | *«t8vr»* |

Virtual Router

[https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/virtual-routers.html#](https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/virtual-routers.html)

Describe the routing protocols in use at the customer site including protocols, redistribution, route filtering, etc. The example below is for static routing on a multi-vsys chassis.

Each {{Customer}} PA-5260 H/A pair has a virtual router per vsys. Each Layer 3 interface is assigned to the appropriate virtual router. {{Customer}} is using static routing on each vsys. No dynamic routing protocols are configured.

Table 9 shows the virtual router configuration.

Table 9 – Virtual Routers General Settings

|  |  |  |  |
| --- | --- | --- | --- |
| **Device Name** | **Virtual System** | **Virtual Router** | **Routing Protocols** |
| *«t9devicename»* | *«t9vsysname»* | * *«t9vr»* | * *«t9protocols»* |

High Availability

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

Describe the high availability configuration in use at the customer site.

{{Customer}} deployed the Palo Alto Networks platforms in an active/passive high availability configuration. Link and path monitoring are enabled. Each AE interface group is monitored with a failure condition of all. This will allow for one interface in the AE group to go down without causing a firewall failover. This allows for upstream and downstream switch maintenance without impacting the firewall HA state. Path monitoring is also enabled to monitor multiple upstream and downstream IP addresses for reachability. Each virtual router is configured for path monitoring.

The dedicated HA1-A and HA1-B interfaces are used for HA1. HA2 is using the dedicated hsci interface. Ethernet 1/4 is configured as the HA2 Backup interface. Interfaces are directly connected.

Table 10 shows the {{Customer}} high availability deployment.

Table 10 – HA Firewall Deployment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Firewall Name** | **HA Mode** | **HA1 IP** | **HA1B IP** | **HA2 IP** | **HA2B IP** |
| «t10devicename» | «t10hamode» | *«t10ha1a»* | *«t10ha1b»* | *«t10ha2a»* | *«t10ha2b»* |

Table 11 shows the configured high availability (HA) settings to be standardized across all HA active/passive and active/active deployments in the {{Customer}} environment.

Table 11 – Standardized HA Settings

|  |  |  |
| --- | --- | --- |
| **Device Name** | **A/P HA Settings** | **Configuration** |
| «t11devicename» | Passive Link State  Monitor Fail Hold Down Time  Device Priority  Preemptive  Heartbeat backup  HA Timer Settings  Backup Links  Link Monitoring  Path Monitoring | *«t11passivelinkstate»*  *«t11mfhdtime»*  *«t11priority»*  *«t11preemptive»*  *«t11heartbeat»*  *«t11hatimer»*  *«t11backup»*  *«t11linkmonitoring»*  *«t11pathmonitoring»* |

Interfaces

There are many different types of interfaces configured. These will be described in detail below as it pertains to the deployment around:

* Operational interfaces
* Management interfaces
* Logging interfaces

Operational Interfaces

[https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces.html#](https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces.html)

Describe the customer interface configuration below

{{Customer}} is utilizing aggregate ethernet (AE) interfaces to increase bandwidth and provide redundant connections to upstream devices. Each interface is configured as Layer 3. Sub-interfaces are configured to allow multiple VLANs across the same aggregate ethernet interface group. All interfaces are set to auto for speed and duplex. AE1 consist of two 10Gpbs interfaces. AE2 consists of two 40Gbps interfaces. Management profiles are assigned to all Layer 3 interfaces.

Table 12 shows the {{Customer}} interface configuration.

Table 12 – Operational Interface Settings

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Device Name** | **Interface** | **Type** | **Mgt Profile** | **IP** | **Virtual Router** | **VLAN** | **Vsys** | **Zone** |
| *«t12devicename»* | *«t12interfacename»* | *«t12type»* | *«t12mgtprof»* | *«t12ip»* | *«t12vr»* | *«t12vlan»* | *«t12vsys»* | *«t12zone»* |

Management Interfaces

[https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/firewall-administration/management-interfaces.html#](https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/firewall-administration/management-interfaces.html)

Describe the management settings for each device deployed.

Table 13 shows the management settings for each deployed device.

Table 13 – MGT Port Settings

|  |  |  |
| --- | --- | --- |
| **Device Name** | **MGT Port** | **Settings** |
| *«t13devicename»* | *IP Address*  *Mask*  *Gateway*  *IPv6 address*  *Speed*  *MTU*  *Services*  *Permitted IP’s* | *«t13mgmtIP»*  *«t13mgmtnetmask»*  *«t13mgmtgateway»*  *«t13mgmtipv6»*  *«t13mgmtspeed»*  *«t13mgmtmtu»*  *«t13mgmtservices»*  *«t13mgmtpermittedips»* |

Logging Interfaces

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/network/network-interfaces/log-card-interface.html>

Describe the log card interface configuration. If the firewalls deployed do not have a dedicated logging interface or using service routes for forwarding logs, this section can be removed.

Table 14 shows the log interface settings.

Table 14 – Log Interface Settings

|  |  |  |  |
| --- | --- | --- | --- |
| **Device Name** | **Log Interface** | **Settings** | **Notes** |
| «t14devicename» | Interface Name  IP Address  Mask  Gateway  IPv6 address  Speed  MTU | *«t14interface»*  *«t14ip»*  *«t14mask»*  *«t14gw»*  *«t14ipv6»*  *«t14speed»*  *«t14mtu»* |  |

Security Zones

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/network/network-zones.html>

Describe the configured security zones, including vsys, zone protection profiles, and if User-ID is enabled.

Each {{Customer}} firewall is configured to use Layer-3 interfaces. There are four security zones configured to secure traffic between the internet, DMZ and inside resources. The Guest security zone is assigned to vsys2 and secures Guest traffic to the internet. {{Customer}} has configured a zone protection profile, “Recon Alert”, to alert on TCP/UDP port scans and host sweeps. This will be monitored over the next two weeks and modified to block traffic if needed.

Table 15 shows the configured security zones.

Table 15 – Security Zones

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Device Name** | **Zone Name** | **Type** | **Zone Protection** | **User-ID** | **VSYS** |
| *«t15devicename»* | *«t15zonename»* | *«t15zonetype»* | *«t15zoneprotection»* | *«t15userid»* | *«t15vsys»* |

IPSec VPNs

[https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/vpns/site-to-site-vpn-overview.html#](https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/vpns/site-to-site-vpn-overview.html)

Describe the IPSec VPN configuration. Include details for each tunnel configured. If not, VPN tunnels are deployed, and this section can be removed.

Table 16 through Table 19 shows the IPSec VPN configuration.

Table 16 – IKE Profile

|  |  |  |
| --- | --- | --- |
| **Device Name** | **IKE Profile** | **Settings** |
| «t16devicename» | Name  DH Group  Authentcation  Encryption  Key Lifetime  IKEv2 Authentication Multiple | *«t16ikeprofilename»*  *«t16dhgroup»*  *«t16authentication»*  *«t16encryption»*  *«t16keylifetime»*  *«t16ikev2authentication»* |

Table 17 – IPSec Profile

|  |  |  |
| --- | --- | --- |
| **Device Name** | **IPSec Profile** | **Settings** |
| «t17devicename» | Name  IPSec Protocol  Encryption (ESP protocol only)  Authentication  DH Group  Lifetime  Lifesize | *«t17ipsecprofilename»*  *«t17ipsecprotocol»*  *«t17encryption»*  *«t17authentication»*  *«t17dhgroup»*  *«t17lifetime»*  *«t17lifesize»* |

Table 18 – IKE Gateway Configuration

|  |  |  |
| --- | --- | --- |
| **Device Name** | **IKE Gateway** | **Settings** |
| «t18devicename» | Name  Version  Address Type  Interface  Local IP Address  Peer IP Address Type  Peer IP address  Authentication  Local ID  Peer ID  IKE Crypto Profile | *«t18ikegwname»*  *«t18ikeversion»*  *«t18addresstype»*  *«t18interface»*  *«t18localaddress»*  *«t18peeraddresstype»*  *«t18peeraddress»*  *«t18authentication»*  *«t18localid»*  *«t18peerid»*  *«t18ikecryptoprofile»* |

Table 19 – IPSec Tunnel Configuration

|  |  |  |
| --- | --- | --- |
| **Device Name** | **IPSec Tunnel** | **Settings** |
| «t19devicename» | Name  Tunnel Interface  Type  Address Type  IKE Gateway  IPSec Crypto Profile  Advanced Options  Proxy IDs | *«t19tunnelname»*  *«t19interface»*  *«t19type»*  *«t19addresstype»*  *«t19ikegateway»*  *«t19ipseccrypto»*  *«t19advancedoptions»*  *«t19proxyids»* |

GlobalProtect

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

Describe the customer GlobalProtect deployment. Include use cases, gateways, hip checks, etc

To provide secure remote access to internal resources and to provide always on security for mobile users, {{Customer}} deployed GlobalProtect. The GlobalProtect Portal and Gateway are running on the Corporate edge firewall. HIP checks are configured to ensure endpoints meet minimum requirements to access internal resources. The GlobalProtect client is configured for On-demand using LDAP authentication.

Table 20 through Table 23 show the GlobalProtect environment.

Portals

Table 20 – GlobalProtect Portal Information

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Device Name** | **Interface** | **Auth Profile** | **IP Address** | **FQDN** | **Agent Profiles** | **Gateways / Agent Profile** |
| «t20devicename» | «t20interface» | «t20authprofile» | *«t20ipaddress»* |  | *«t20agentprofiles»* | *«t20gateways»* |

Gateways

Table 21 – External GlobalProtect Gateway Information

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Device Name** | **Interface** | **Auth Profile** | **IP Address** | **FQDN** | **Agent Profiles** | **Client DHCP Pool** | **Tunnel Mode** |
| «t21devicename» | «t21interface» | «t21authprofile» | *«t21ipaddress»* |  | *«t21agentprofiles»* | *«t21dhcppool»* | *«t21tunnelmode»* |

Table 22 – Internal GlobalProtect Gateway Information

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Device Name** | **Interface** | **Auth Profile** | **IP Address** | **FQDN** | **Agent Profiles** | **Client DHCP Pool** | **Tunnel Mode** |

HIP Profile Information

Table 23 – HIP Profile Information

|  |  |  |
| --- | --- | --- |
| **Device Name** | **HIP Name** | **Parameters** |
| «t23devicename» | «t23name» | *«t23parameters»* |

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** |
| *«t24devicename»* | IP Address  Mask  Gateway  IPv6 address  Speed  MTU  Services  H/A Priority  Permitted IP | *«t24mgmtIP»*  *«t24mgmtnetmask»*  *«t24mgmtgateway»*  *«t24mgmtipv6»*  *«t24mgmtspeed»*  *«t24mgmtmtu»*  *«t24mgmtservices»*  *«t24hapriority»*  *«t24mgmtpermittedips»* |

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** |
| *«t25devicename»* | *«t25templatename»* | *«t25stackname»* | *«t25stackmembers»* |

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** |
| *«t26devicename»* | *«t26tier1»* | *«t26tier2»* | *«t26tier3»* | *«t26tier4»* | *«t26masterdevice»* |

Log Forwarding

[https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-log-collection/configure-log-forwarding-to-panorama.html#](https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-log-collection/configure-log-forwarding-to-panorama.html)

{{Customer}} has a single VM Series Panorama deployed in Panorama mode. This allows for the VM appliance to be used for firewall management and log collecting. All managed firewalls are forwarding logs to Panorama’s log collector. Each security policy is configured with a Log Forwarding profile named *default*. This log forwarding profile is sending all traffic, threat, URL, Data and WildFire logs to Panorama and QRadar syslog server.

Table 27 shows the Panorama Log Forwarding profile.

Table 27 – Log Forwarding Profile

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Device Name** | **Profile Name** | **Log Type** | **Panorama** | **SNMP** | **Email** | **Syslog** |
| *«t27devicename»* | *«t27profilename»* | *«t27logtype»* | *«t27panorama»* | *«t27snmp»* | *«t27email»* | *«t27syslog»* |

Security Profiles

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

Describe each security profile that the customer has configured an update the tables for each to include action.

The Antivirus profile details are shown in Table 28.

Table 28 – Antivirus Profile

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device Name** | **Profile Name** | **Decoder** | **Action** | **WildFire-Action** |
| *«t28devicename»* | *«t28avprofilename»* | *«t28decoders»* | *«t28actions»* | *«t28wfactions»* |

The Anti-Spyware profile details are shown in Table 29.

Table 29 – Anti-Spyware Profile

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device Name** | **Profile Name** | **Severity** | **Action** | **DNS Sinkhole?** |
| *«t29devicename»* | *«t29asprofilename»* | *«t29severity»* | *«t29actions»* | *«t29dnssink»* |

The Vulnerability profile details are shown in Table 30.

Table 30 – Vulnerability Profiles

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device Name** | **Profile Name** | **Rule Name** | **Severity** | **Action** |
| *«t30devicename»* | *«t30vprofilename»* | *«t30rulename»* | *«t30severity»* | *«t30action»* |

The URL Filtering profile details are shown in Table 31.

Table 31 – URL Filtering Profiles

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Device Name** | **URL Filtering Profile Name** | **Blocked Categories** | **Allow Categories** | **Alert Categories** | **Continue**  **Categories** | **Override Categories** | **User Credential Submission** |
| *«t31devicename»* | *«t31profilename»* | *«t31blocked»* | *«t31allow»* | *«t31alert»* | *«t31continue»* | *«t31override»* | *«t31credential»* |

The WildFire profile details are shown in Table 32.

Table 32 – WildFire Profile Details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Device Name** | **Profile Name** | **Applications** | **File Types** | **Direction** | **Analysis** |
| *«t32devicename»* | *«t32profilename»* | *«t32applications»* | *«t32filetypes»* | *«t32direction»* | *«t32analysis»* |

The File Blocking profile details are shown in Table 33.

Table 33 – File Blocking Profile Details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Device Name** | **Rule Name** | **Applications** | **File Types** | **Direction** | **Action** |
| *«t33devicename»* | *«t33rulename»* | *«t33applications»* | *«t33filetypes»* | *«t33direction»* | *«t33action»* |

Data pattern objects details are shown in Table 34.

Table 34 – Data Pattern Objects

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Device Name** | **Profile Name** | **Pattern Type** | **Name** | **File Types** | **Pattern** |
| *«t34devicename»* | *«t34profilename»* | *«t34patterntype»* | *«t34name»* | *«t34filetypes»* | *«t34pattern»* |

Data Filtering profile details are shown in Table 35.

Table 35 – Data Filtering Profile Details

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Device Name** | **Rule Name** | **Apps** | **File Types** | **Pattern(s)** | **Direction** | **Alert Threshold** | **Block Threshold** |
| *«t35devicename»* | *«t35rulename»* | *«t35apps»* | *«t35filetype»* | *«t35patterns»* | *«t35direction»* | *«t35alert»* | *«t35block»* |

The DoS profile details are shown in Table 36.

Table 36 – DoS Profile Details

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Device Name** | **DoS Profile Name** | **Type** | **SYN Flood** | **UDP Flood** | **ICMP Flood** | **ICMPV6 Flood** | **Other IP Flood** | **Resource Protection (Sessions)** |
| *«t36devicename»* | *«t36profilename»* | *«t36type»* | *«t36syn»* | *«t36udp»* | *«t36icmp»* | *«t36icmp6»* | *«t36flood»* | *«t36rps»* |

Security Profile Groups

Describe the customers security profile groups configured and if they are applied to security policies.

The security profile group details are shown in Table 37.

Table 37 – Security Profile Group Details

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Device Name** | **Group Name** | **Antivirus** | **Anti-**  **Spyware** | **Vulnerability** | **File Blocking** | **Data Filtering** | **WildFire** | **URL** |
| *«t37devicename»* | *«t37groupname»* | *«t37av»* | *«t37as»* | *«t37vp»* | *«t37fb»* | *«t37df»* | *«t37wf»* | *«t37url»* |

{{Customer}} Security Profiles Configuration

Describe the customers use of security profiles on security policy. Identify the profiles or profile groups in use. Also note if any security policies do not have security profiles assigned and the reason they are not in use.

Dynamic Updates

[https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates/dynamic-content-updates.html#](https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/software-and-content-updates/dynamic-content-updates.html)

Describe the Dynamic Update schedule. Be sure to include if there are any thresholds configured. Also note if new applications are disabled in content updates.

The dynamic content updates schedule details are shown in Table 38.

Table 38 – Dynamic Updates Schedule Details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Device Name** | **Type** | **Recurrence** | **Time** | **Action** | **Threshold Hours** |
| *«t38devicename»* | *«t38type»* | *«t38recurrence»* | *«t38time»* | *«t38action»* | *«t38threshold»* |

User-ID

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

Describe the customers User-ID configuration and if used for visibility and/or enforcement

{{Customer}} has configured the integrated User-ID agent to gather User-ID mappings from three domain controllers. Group Mapping is also configured to learn Active Directory Groups used in security policies. User-ID is configured for visibility and enforcement.

User-ID Sources

Table 39 shows User-ID source details.

Table 39 - User-ID Source Details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Device Name** | **User-ID Source** | **Type** | **IP Address** | **Port** | **Configured Interface** |
| *«t39devicename»* | *«t39source»* | *«t39type»* | *«t39ipaddress»* | *«t39port»* | *«t39interface»* |

Group Mapping Profiles

Group mapping configuration details are shown in Table 40.

Table 40 – Group Mapping Profile Details

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Device Name** | **Server Profile** | **Domain Setting** | **Group Object class** | **User Object Class** | **User and Group Attributes** | **Group Include List** |
| *«t40devicename»* | *«t40serverprofile»* | *«t40domain»* | *«t40group»* | *«t40user»* | *«t40attributes»* | *«t40includelist»* |

SNMP

[https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/snmp-monitoring-and-traps.html#](https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/snmp-monitoring-and-traps.html)

Document SNMP settings here for firewalls and Panorama.

SNMP Server Profile

Table 41 shows the SNMP server profile details.

Table 41 – SNMP Server Profile

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device Name | SNMP Profile Name | SNMP Manger Name | SNMP Manager IP/FQDN | Community String |
| *«t41devicename»* | *«t41profilename»* | *«t41managername»* | *«t41managerip»* | *«t41communitystring»* |

SNMPv2 Settings

SNMPv2 settings are shown in Table 42.

Table 42 – SNMPv2 Settings

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device Name | Physical Location | Contact | Version | Community String |
| *«t42devicename»* | *«t42location»* | *«t42contact»* | *«t42version»* | *«t42community»* |

SNMPv3 Settings

SNMPv3 settings are shown in Table 43 and Table 44.

Table 43 – Views

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device Name | Name | View | OID | Option | Mask |
| *«t43devicename»* | *«t43name»* | *«t43view»* | *«t43oid»* | *«t43option»* | *«t43mask»* |

Table 44 – Users

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device Name | Users | View | Auth Password | Priv Password |
| *«t44devicename»* | *«t44users»* | *«t44view»* |  |  |

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* |