**{{Customer}}**

**Palo Alto Networks Deployment**

***<Type of As-Built>***

***As-Built Document***

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

**Contact Information**

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

© 2022 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. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

**Table of Contents**

[**Introduction**](#_heading=h.30j0zll) **7**

[Executive Summary](#_heading=h.1fob9te) 7

[Open Issues](#_heading=h.3znysh7) 8

[**Platform**](#_heading=h.tyjcwt) **9**

[Deployed Security Platforms](#_heading=h.3dy6vkm) 9

[*Procured Systems*](#_heading=h.1t3h5sf) *9*

[*Device Licensing*](#_heading=h.2s8eyo1) *9*

[*PAN-OS Version*](#_heading=h.lnxbz9) *9*

[*Panorama Systems*](#_heading=h.35nkun2) *9*

[*Panorama Licensing*](#_heading=h.44sinio) *10*

[Platform Administration](#_heading=h.2jxsxqh) 10

[**Network Integration**](#_heading=h.3j2qqm3) **10**

[Virtual Systems](#_heading=h.1y810tw) 10

[Virtual Router](#_heading=h.2xcytpi) 11

[High Availability](#_heading=h.3whwml4) 11

[Interfaces](#_heading=h.1pxezwc) 12

[*Operational Interfaces*](#_heading=h.49x2ik5) *12*

[*Management Interfaces*](#_heading=h.147n2zr) *13*

[*Logging Interfaces*](#_heading=h.23ckvvd) *13*

[Security Zones](#_heading=h.32hioqz) 14

[IPSec VPNs](#_heading=h.2grqrue) 15

[GlobalProtect](#_heading=h.1v1yuxt) 16

[*Portals*](#_heading=h.4f1mdlm) *17*

[*Gateways*](#_heading=h.3tbugp1) *17*

[*HIP Profile Information*](#_heading=h.28h4qwu) *17*

[**Prisma Access**](#_heading=h.i8yyaf419iro) **18**

[Plugin Version](#_heading=h.b7mh3kabjr06) 18

[Prisma Access Version](#_heading=h.otfk6di2avnh) 18

[Tenant ID(s)](#_heading=h.6cm1cgdy8mq4) 18

[Project Goals](#_heading=h.9575uy3htk3m) 19

[Specifications](#_heading=h.d1ky10nbs11h) 19

[High Level Topology](#_heading=h.x6fm1n4soslr) 19

[Cloud Services Onboarding](#_heading=h.4z2h7wo3o7pk) 20

[Service Setup](#_heading=h.41lzf4cq6jt) 20

[General Settings](#_heading=h.k2fsul3lt2jm) 21

[Internal Domain List](#_heading=h.tslpuloldgwl) 21

[Advanced Settings](#_heading=h.338iszp3wzi2) 21

[Routing](#_heading=h.w5bg1zcu2i06) 21

[HIP Redistribution](#_heading=h.kwq2ld2sl9p) 21

[Retrieve IP Addresses for Prisma Access](#_heading=h.d21umijzy88r) 21

[Mobile Users – GlobalProtect](#_heading=h.jix11w6gwx92) 21

[General Settings](#_heading=h.ekwqkpfgvvk2) 21

[Zone Mapping](#_heading=h.avt1qigehtdr) 21

[Onboarding](#_heading=h.38y7vxtbbtb0) 21

[General](#_heading=h.baa66vo6vurq) 21

[Locations](#_heading=h.4o0of0o91b49) 21

[IP Pools](#_heading=h.to3w9kvlixiq) 22

[Network Services](#_heading=h.q0rmf5x2rxbw) 22

[Manual Gateway Locations](#_heading=h.qsrdx8febmhg) 22

[GlobalProtect Portal Settings](#_heading=h.18ucjo274508) 22

[GlobalProtect Gateway Settings](#_heading=h.50ja5582n5qz) 22

[GlobalProtect App Settings](#_heading=h.8fjq5493v899) 22

[Mobile Users – Explicit Proxy](#_heading=h.s0irs4hflsvn) 22

[General Settings](#_heading=h.6llihlp867gw) 22

[Settings](#_heading=h.fqb1619zxdt1) 22

[Group Mapping Settings](#_heading=h.cj7kf5kdjeaw) 22

[Authentication Settings](#_heading=h.6qb16ihoj9tn) 22

[Explicit Proxy Connection Setup](#_heading=h.r5sfri6voxez) 22

[Settings](#_heading=h.4zi1ebysed74) 22

[Locations](#_heading=h.oucwfcdfbmvj) 22

[Remote Networks](#_heading=h.d0nwekk0rmdo) 22

[General Settings](#_heading=h.k46rryo855ai) 23

[Settings](#_heading=h.rkcu63gfb4c9) 23

[DNS Proxy](#_heading=h.wddee3uo657p) 23

[Group Mapping Settings](#_heading=h.pevxdtqn1czx) 23

[Zone Mapping](#_heading=h.rb2cj5umv533) 23

[Aggregate Bandwidth](#_heading=h.jgxwwmi0s6m0) 23

[Remote Networks Onboarding](#_heading=h.r5dfnwb1osrw) 23

[Inbound Access Remote Networks Onboarding](#_heading=h.3y9mfm5m053z) 23

[Service Connections](#_heading=h.c3m043r17fp7) 23

[Onboarding](#_heading=h.sl3sbdo5zg94) 23

[Traffic Steering](#_heading=h.i7zvz5km3qxp) 23

[General Settings](#_heading=h.tyixs2wffv9s) 23

[Target Service Connections for Traffic Steering](#_heading=h.ammpqar143o) 23

[Traffic Steering Rules](#_heading=h.wh1q0747osv1) 23

[HIP](#_heading=h.6trktp8d0ipw) 23

[Autonomous Digital Experience Management (ADEM)](#_heading=h.d8wzhfhg0583) 24

[Prisma Access Insights](#_heading=h.je9t2axpepf) 24

[Alert Subscription](#_heading=h.j07sueo9iqoo) 24

[Mobile User IP Pool](#_heading=h.jcc7vkibzxum) 25

[**Panorama**](#_heading=h.1mrcu09) **25**

[Templates](#_heading=h.2lwamvv) 26

[Device Groups](#_heading=h.3l18frh) 26

[Device Group Tree](#_heading=h.206ipza) 27

[Log Forwarding](#_heading=h.2zbgiuw) 27

[Security Profiles](#_heading=h.3ygebqi) 27

[Security Profile Groups](#_heading=h.kgcv8k) 29

[*{{Customer}}Security Profiles Configuration*](#_heading=h.1jlao46) *29*

[Dynamic Updates](#_heading=h.43ky6rz) 30

[**User-ID**](#_heading=h.xvir7l) **30**

[User-ID Sources](#_heading=h.3hv69ve) 30

[LDAP Group Mapping Profiles](#_heading=h.4h042r0) 31

[Cloud Identity Engine Group Mapping](#_heading=h.wjnovuk7c6rw) 31

[**SNMP**](#_heading=h.1baon6m) **31**

[SNMP Server Profile](#_heading=h.3vac5uf) 31

[*SNMPv2 Settings*](#_heading=h.pkwqa1) *31*

[*SNMPv3 Settings*](#_heading=h.1opuj5n) *32*

[*Reporting*](#_heading=h.1302m92) *32*

[**Cloud Services and Integration Pieces**](#_heading=h.3mzq4wv) **32**

[Cortex Data Lake](#_heading=h.2250f4o) 32

[Cloud Services Plug-In](#_heading=h.haapch) 32

[Prisma Public Cloud](#_heading=h.qi0bgp48f8kc) 32

[SaaS Security API/In-Line](#_heading=h.jyzfjgfutt8o) 32

[Cortex](#_heading=h.319y80a) 32

[VM-Series](#_heading=h.1gf8i83) 33

[AutoFocus](#_heading=h.40ew0vw) 33

[Threat Vault](#_heading=h.2fk6b3p) 33

[**Best Practice Assessment (BPA)**](#_heading=h.upglbi) **33**

[BPA Report](#_heading=h.k27lh9h7aivw) 33

[Best Practices Guides](#_heading=h.ib1lq71w43dy) 34

[**Third Party Integrations**](#_heading=h.ehn0w1q70ee7) **35**

[**Document Properties**](#_heading=h.1tuee74) **36**

[Contributors](#_heading=h.4du1wux) 36

[Revision History](#_heading=h.184mhaj) 36

[**Palo Alto Networks Resources**](#_heading=h.279ka65) **37**

[**Customer Resources**](#_heading=h.meukdy) **37**

***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 QuickStart Service 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 outdented italic notes are instructions for each section. Remove all template instruction notes before generating the final document. The standard red 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 tosite 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 the {{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:*

Strata Implementation:

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 secures 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.

Prisma Access Implementation:

Prisma Access helps your organization deliver consistent security to your remote networks and mobile users. It’s a generational step forward in cloud security, using a cloud-delivered architecture to connect all users to all applications.

All your users—whether at your headquarters, branch offices, or on the road—connect to Prisma Access to safely use cloud and data center applications as well as the internet. Prisma Access consistently inspects all traffic across all ports and provides bidirectional networking to enable branch-to-branch as well as branch-to-HQ traffic.

Prisma Access delivers protection at scale with global coverage so you don’t have to worry about things like sizing and deploying hardware firewalls at your branches, or building out and managing appliances in colocation facilities.

Prisma Access uses Cortex Data Lake for centralized analysis, reporting, and forensics.

Palo Alto Networks Professional Services has documented the specific configuration details for this project, and they are outlined below to enable the [CUSTOMER] team to understand the deployment.

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

## Open Issues

Case 000000 - Licenses not properly provisioned - Closed

Case 000001 - PA-220 RMA - Device was non-functional after arrival - Closed

# 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** | |
| {%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 %} | | |

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

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

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

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration.html>

<https://docs.paloaltonetworks.com/pan-os/10-0/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 %} | | | | | | |

# Network Integration

## Virtual Systems

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

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

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/virtual-systems.html>

<https://docs.paloaltonetworks.com/pan-os/10-0/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 8shows the {{Customer}}vsys deployment.

Table 8– VSYS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device Name** | **VSYS ID** | **VSYS Name** | **Interfaces** | **Virtual Router** |
| {%tr for item in t8%} | | | | |
| *{{item.t8devicename}}* | *{{item.t8vsysid}}* | *{{item.t8vsysname}}* | *{{item.t8interfaces}}* | *{{item.t8vr}}* |
| {%tr endfor %} | | | | |

## Virtual Router

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

[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)

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/virtual-routers.html>

<https://docs.paloaltonetworks.com/pan-os/10-0/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 9shows the virtual router configuration.

|  |  |  |  |
| --- | --- | --- | --- |
| **Device Name** | **Virtual System** | **Virtual Router** | **Routing Protocols** |
| {%tr for item in t9%} | | | |
| *{{item.t9devicename}}* | *{{item.t9vsysname}}* | *{{item.t9vr}}* | *{{item.t9protocols}}* |
| {%tr endfor %} | | | |

## High Availability

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

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

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability.html>

<https://docs.paloaltonetworks.com/pan-os/10-0/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 10shows the {{Customer}}high availability deployment.

Table 10– HA Firewall Deployment

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Firewall Name** | **HA Mode** | **HA1 IP** | **HA1B IP** | **HA2 IP** | **HA2B IP** |
| {%tr for item in t10%} | | | | | |
| {{item.t10devicename}} | {{item.t10hamode}} | {{item.t10ha1a}} | {{item.t10ha1b}} | {{item.t10ha2a}} | {{item.t10ha2b}} |
| {%tr endfor %} | | | | | |

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** |
| {%tr for item in t11%} | | |
| {{item.t11devicename }} | Passive Link State  Monitor Fail Hold Down Time  Device Priority  Preemptive  Heartbeat backup  HA Timer Settings  Backup Links  Link Monitoring  Path Monitoring | *{{item.t11passivelinkstate}}*  *{{item.t11mfhdtime}}*  *{{item.t11priority}}*  *{{item.t11preemptive}}*  *{{item.t11heartbeat}}*  *{{item.t11hatimer}}*  *{{item.t11backup}}*  *{{item.t11linkmonitoring}}*  *{{item.t11pathmonitoring}}* |
| {%tr endfor %} | | |

## 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

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

[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)

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/configure-interfaces.html>

<https://docs.paloaltonetworks.com/pan-os/10-0/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 consists of two 10 Gbps interfaces. AE2 consists of two 40 Gbps 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** |
| {%tr for item in t12%} | | | | | | | | |
| *{{item.t12devicename}}* | *{{item.t12interfacename}}* | *{{item.t12type}}* | *{{item.t12mgtprof}}* | *{{item.t12ip}}* | *{{item.t12vr}}* | *{{item.t12vlan}}* | *{{item.t12vsys}}* | *{{item.t12zone}}* |
| {%tr endfor %} | | | | | | | | |

*Table 12 – Operational Interface Settings*

### Management Interfaces

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

[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)

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/management-interfaces.html>

<https://docs.paloaltonetworks.com/pan-os/10-0/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** |
| {%tr for item in t13%} | | |
| *{{item.t13devicename}}* | *IP Address*  *Mask*  *Gateway*  *IPv6 address*  *Speed*  *MTU*  *Services*  *Permitted IP’s* | *{{item.t13mgmtIP}}*  *{{item.t13mgmtnetmask}}*  *{{item.t13mgmtgateway}}*  *{{item.t13mgmtipv6}}*  *{{item.t13mgmtspeed}}*  *{{item.t13mgmtmtu}}*  *{{item.t13mgmtservices}}*  *{{item.t13mgmtpermittedips}}* |
| {%tr endfor %} | | |

### Logging Interfaces

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

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

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/network/network-interfaces/log-card-interface.html>

<https://docs.paloaltonetworks.com/pan-os/10-0/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 use 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** |
| {%tr for item in t14%} | | | |
| *{{item.t14devicename}}* | Interface Name  IP Address  Mask  Gateway  IPv6 address  Speed  MTU | *{{item.t14interface}}*  *{{item.t14ip}}*  *{{item.t14mask}}*  *{{item.t14gw}}*  *{{item.t14ipv6}}*  *{{item.t14speed}}*  *{{item.t14mtu}}* |  |
| {%tr endfor %} | | | |

|  |  |  |  |
| --- | --- | --- | --- |

## Security Zones

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

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

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/network/network-zones.html>

<https://docs.paloaltonetworks.com/pan-os/10-0/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** |
| {%tr for item in t15%} | | | | | |
| *{{item.t15devicename}}* | *{{item.t15zonename}}* | *{{item.t15zonetype}}* | *{{item.t15zoneprotection}}* | *{{item.t15userid}}* | *{{item.t15vsys}}* |
| {%tr endfor %} | | | | | |

## IPSec VPNs

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

[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)

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/vpns/site-to-site-vpn-overview.html>

<https://docs.paloaltonetworks.com/pan-os/10-0/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** |
| {%tr for item in t16%} | | |
| *{{item.t16devicename}}* | Name  DH Group  Authentcation  Encryption  Key Lifetime  IKEv2 Authentication Multiple | *{{item.t16ikeprofilename}}*  *{{item.t16dhgroup}}*  *{{item.t16authentication}}*  *{{item.t16encryption}}*  *{{item.t16keylifetime}}*  *{{item.t16ikev2authentication}}* |
| {%tr endfor %} | | |

Table 17– IPSec Profile

|  |  |  |
| --- | --- | --- |
| **Device Name** | **IPSec Profile** | **Settings** |
| {%tr for item in t17%} | | |
| *{{item.t17devicename}}* | Name  IPSec Protocol  Encryption (ESP protocol only)  Authentication  DH Group  Lifetime  Lifesize | *{{item.t17ipsecprofilename}}*  *{{item.t17ipsecprotocol}}*  *{{item.t17encryption}}*  *{{item.t17authentication}}*  *{{item.t17dhgroup}}*  *{{item.t17lifetime}}*  *{{item.t17lifesize}}* |
| {%tr endfor %} | | |

Table 18– IKE Gateway Configuration

|  |  |  |
| --- | --- | --- |
| **Device Name** | **IKE Gateway** | **Settings** |
| {%tr for item in t18%} | | |
| *{{item.t18devicename}}* | Name  Version  Address Type  Interface  Local IP Address  Peer IP Address Type  Peer IP address  Authentication  Local ID  Peer ID  IKE Crypto Profile | *{{item.t18ikegwname}}*  *{{item.t18ikeversion}}*  *{{item.t18addresstype}}*  *{{item.t18interface}}*  *{{item.t18localaddress}}*  *{{item.t18peeraddresstype}}*  *{{item.t18peeraddress}}*  *{{item.t18authentication}}*  *{{item.t18localid}}*  *{{item.t18peerid}}*  *{{item.t18ikecryptoprofile}}* |
| {%tr endfor %} | | |

Table 19– IPSec Tunnel Configuration

|  |  |  |
| --- | --- | --- |
| **Device Name** | **IPSec Tunnel** | **Settings** |
| {%tr for item in t19%} | | |
| *{{item.t19devicename}}* | Name  Tunnel Interface  Type  Address Type  IKE Gateway  IPSec Crypto Profile  Advanced Options  Proxy IDs | *{{item.t19tunnelname}}*  *{{item.t19interface}}*  *{{item.t19type}}*  *{{item.t19addresstype}}*  *{{item.t19ikegateway}}*  *{{item.t19ipseccrypto}}*  *{{item.t19advancedoptions}}*  *{{item.t19proxyids}}* |
| {%tr endfor %} | | |

## GlobalProtect

*This section is reserved for the on-premises deployment of GlobalProtect and should not be used for Prisma Access.*

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

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

<https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin.html>

<https://docs.paloaltonetworks.com/globalprotect/10-0/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–GlobalProtectPortal Information

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Device Name** | **Interface** | **Auth Profile** | **IP Address** | **FQDN** | **Agent Profiles** | **Gateways / Agent Profile** |
| {%tr for item in t20%} | | | | | | |
| *{{item.t20devicename}}* | {{item.t20interface}} | {{item.t20authprofile}} | {{item.t20ipaddress}} |  | {{item.t20agentprofiles}} | {{item.t20gateways}} |
| {%tr endfor %} | | | | | | |

### Gateways

Table 21–External GlobalProtect Gateway Information

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Device Name** | **Interface** | **Auth Profile** | **IP Address** | **FQDN** | **Agent Profiles** | **Client DHCP Pool** | **Tunnel Mode** |
| {%tr for item in t21%} | | | | | | | |
| *{{item.t21devicename}}* | {{item.t21interface}} | {{item.t21authprofile}} | {{item.t21ipaddress}} |  | {{item.t21agentprofiles}} | {{item.t21dhcppool}} | {{item.t21tunnelmode}} |
| {%tr endfor %} | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |

*Table 22 – Internal GlobalProtect Gateway Information*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Device Name** | **Interface** | **Auth Profile** | **IP Address** | **FQDN** | **Agent Profiles** | **Client DHCP Pool** | **Tunnel Mode** |
| {%tr for item in t22%} | | | | | | | |
| *{{item.t22devicename}}* | {{item.t22interface}} | {{item.t22authprofile}} | {{item.t22ipaddress}} |  | {{item.t22agentprofiles}} | {{item.t22dhcppool}} | {{item.t22tunnelmode}} |
| {%tr endfor %} | | | | | | | |

### HIP Profile Information

Table 23– HIP Profile Information

|  |  |  |
| --- | --- | --- |
| **Device Name** | **HIP Name** | **Parameters** |
| {%tr for item in t23%} | | |
| {{item.t23devicename}} | {{item.t23name}} | {{item.t23parameters}} |
| {%tr endfor %} | | |

# Prisma Access

## Plugin Version

*Delete the Cloud Services Versions that are not related to the customer. If not listed, add the appropriate version. If Cloud managed, delete this section.*

Prisma Access 2.2.0-h25 Preferred

Prisma Access 2.2.0-h22 Preferred

Prisma Access 2.2.0-h7 Preferred

Prisma Access 2.2.0 Preferred

Prisma Access 2.1.0-h8 Preferred

Prisma Access 2.1.0-h4 Preferred

Prisma Access 2.1.0-h11 Innovation

Prisma Access 2.1.0-h6 Innovation

Prisma Access 2.1.0 Innovation

## Prisma Access Version

*Delete the Prisma Access Versions that are not related to the customer. If not listed, add the appropriate version.*

Prisma Access 2.1 Preferred

Prisma Access 2.1 Innovation

Prisma Access 2.2 Preferred

Prisma Access 3.0 Preferred

## Tenant ID(s)

*Populate the Tenant ID(s) configured.*

| **Name** | *paloaltonetworksprismaaccesspslab* |
| --- | --- |
| **Super Tenant ID** | *1433836293* |
| **Tenant/Account ID** | *1433836293* |

*Delete the Prisma Access document links that are not related to the Customer’s environment.*

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin.html>

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin.html>

## Project Goals

*List the goals achieved on this project.*

* Configured Panorama Plug-in for Prisma Access
* Configured Log Forwarding to Cortex Data Lake
* Configured # Service Connections to DC in Irvine
* Configured # Gateways
* Enabled User-ID
* Created # policies for the # of user groups that will connect remotely using Prisma Access
* Configured # Profiles
* Onboarded # of Users

## 

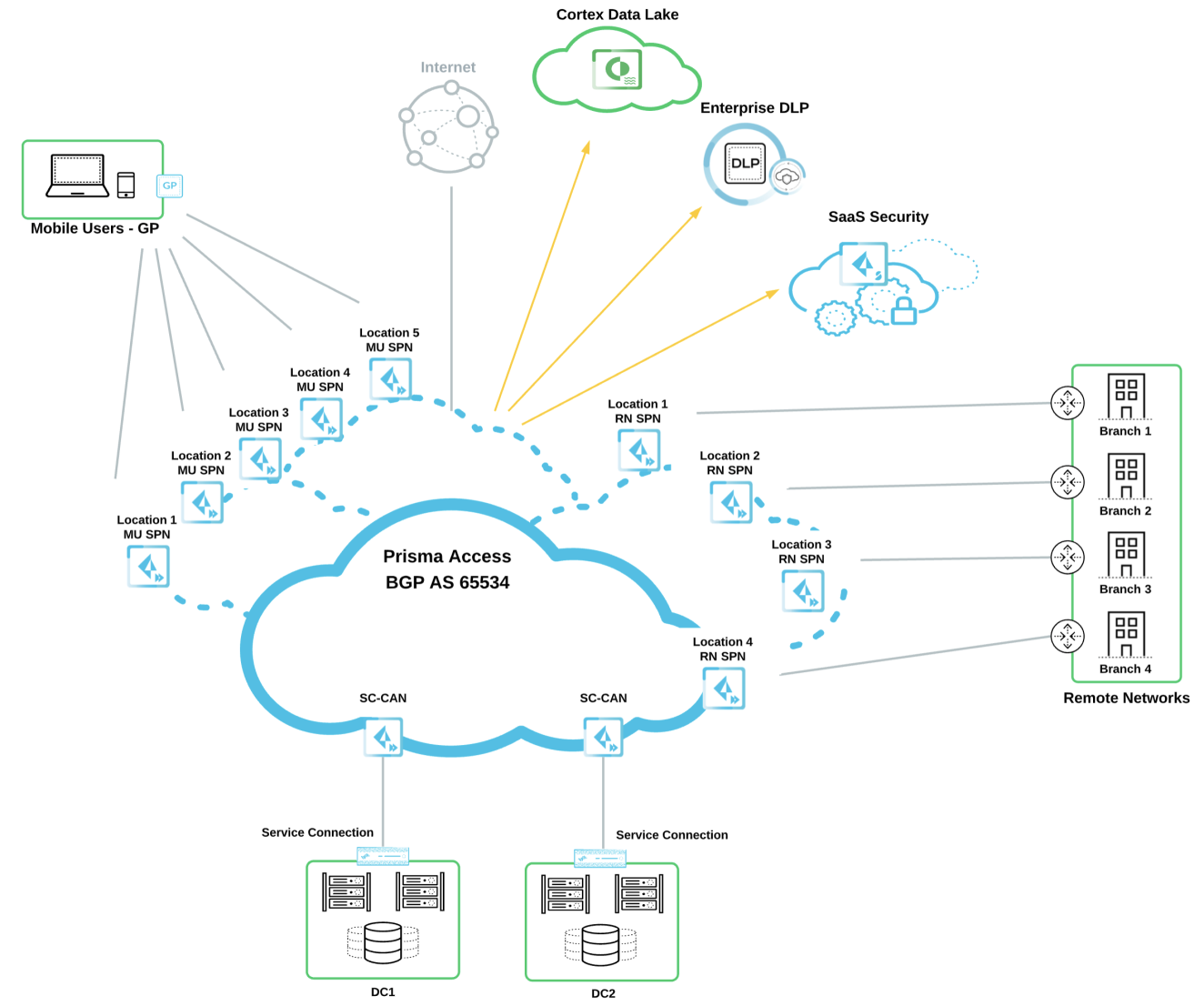
## Specifications

### High Level Topology

Two Service Connections were configured to provide the Mobile Users access to the customer’s primary and backup datacenters. Five gateway locations were enabled across the US to provide regional connectivity to the distributed workforce across the US. Additionally, four Remote Networks were configured to provide Internet filtering out of each branch through Prisma Access. All logs are being forwarded to the Cortex Data Lake. The Enterprise DLP add-on and SaaS Security API add-on have been purchased but will be configured in a follow-up engagement.

*Create a simple network diagram based on the customer’s setup.*

*Lucidchart Template -* [*https://lucid.app/lucidchart/7ed504b7-268c-40b5-8cd3-fc490ea03854/edit?invitationId=inv\_079dafca-540d-4f13-ad1f-cd9fd75bdac1*](https://lucid.app/lucidchart/7ed504b7-268c-40b5-8cd3-fc490ea03854/edit?invitationId=inv_079dafca-540d-4f13-ad1f-cd9fd75bdac1)



*Figure 1 - High Level Diagram*

## Cloud Services Onboarding

### Service Setup

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prepare-the-prisma-access-infrastructure/enable-the-service-infrastructure.html#id174DBE00YY4>

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/prisma-access-service-infrastructure/set-up-the-prisma-access-service-infrastructure.html>

**General Settings**

Table 49– shows service Infrastructure

|  |  |
| --- | --- |
| **Service Infrastructure** | |
| {%tr for item in t49%} | |
| Infrastructure Subnet IPv4  Enable IPv6 Status  Infrastructure Subnet IPv6  Infrastructure BGP AS | *{{item.t49infrastructuresubnetipv4}}*  *{{item.t49enableipv6status}}*  *{{item.t49infrastructuresubnetipv6}}*  *{{item.t49infrastructurebjpas}}* |
| {%tr endfor %} | |

#### Table 50– Template Stack

|  |  |
| --- | --- |
| **Template Stack** | |
| {%tr for item in t50%} | |
| Template Stack Name  Templates | *{{item.t50templatestackname}}*  *{{item.t50templates}}* |
| {%tr endfor %} | |

#### Table 51– Device Group

|  |  |
| --- | --- |
| **Device Group** | |
| {%tr for item in t51%} | |
| Device Group Name  Parent Device Group | *{{item.t51devicegroupname}}* |
| {%tr endfor %} | |

#### **Internal Domain List**

#### Table 52– DNS

|  |  |  |
| --- | --- | --- |
| **Domain Names** | **Primary DNS** | **Secondary DNS** |
| {%tr for item in t52%} | | |
| *{{item.t52domainnames}}* | *{{item.t52primarydns}}* | *{{item.t52secondarydns}}* |
| {%tr endfor %} | | |

#### **Advanced Settings**

##### Routing

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prepare-the-prisma-access-infrastructure/how-bgp-advertises-mobile-user-ip-address-pools.html>

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prepare-the-prisma-access-infrastructure/route-preferences-for-service-connection-traffic.html>

#### Table 53– Routing

|  |  |
| --- | --- |
| **Routing** | |
| {%tr for item in t53%} | |
| Routing Preference  Backbone Routing  Withdraw Static Routes  Enable Auto IKE peer host routes  Outbound Routes for the Service (Max. 10) | *{{item.t53routingpreference}}*  *{{item.t53backbonerouting}}*  *{{item.t53withdrawstaticroutes}}*  *{{item.t53enableautoikepeerhostroutes}}*  *{{item.t53outboundroutesfortheservice}}* |
| {%tr endfor %} | |

#### Table 54-HIP Redistribution

|  |  |
| --- | --- |
| **HIP Redistribution** | |
| {%tr for item in t54%} | |
| Enable HIP Redistribution  Enable Quarantine List Redistribution | *{{item.t54enablehipredistribution}}*  *{{item.t54enablequarantinelistredistribution}}* |
| {%tr endfor %} | |

### Mobile Users – GlobalProtect

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prisma-access-for-users/configure-prisma-access-for-users.html#id174HA00B0Y4>

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/secure-mobile-users-with-prisma-access/globalprotect-app.html#id2c19e575-0c09-4353-8ca1-48c5136ed8a3>

#### **General Settings**

#### Table 55–Template Stack for Mobile Users – Global Protect

|  |  |
| --- | --- |
| **Template Stack** | |
| **Templates** | **Template Stack Name** |
| {%tr for item in t55%} | |
| *{{item.t55templatename}}* | *{{item.t55stackname}}* |
| {%tr endfor %} | |

#### Table 56–Device Group for Mobile Users-Global Protect

|  |  |
| --- | --- |
| **Device Group** | |
| {%tr for item in t56%} | |
| Device Group Name  Parent Device Group  Master Device | *{{item.t56devicegroupname}}* |
| {%tr endfor %} | |

Table 57- Enable Directory Sync Integration

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | | **Directory Attributes** | |
| {%tr for item in t57%} | | |
| Primary User Name  Email  Alternate Username 1  Alternate Username 2  Alternate Username 3 | *{{item.t57primaryusername}}*  *{{item.t57email}}* | |
| {%tr endfor %} | | |

#### Table 58- Zone Mapping

|  |  |  |
| --- | --- | --- |
| **Zone Mapping** | | |
| {%tr for item in t58%} | |
| **Trusted Zones** | *{{item.t58trustedzones}}* |
| **Untrusted Zones** | *{{item. t58untrustedzones }}* |
| {%tr endfor %} | |

#### **Onboarding**

#### Table 59- General onboarding info

|  |  |
| --- | --- |
| **General** | |
| {%tr for item in t59%} | |
| Portal Host Name  Portal DNS CNAME  SSL-TLS Service Profile  **Internal Host Detection**  IP Address  Hostname | *{{item. t59portalhostname }}*  *{{item. t59portaldnsmcname }}*  *{{item. t59ssl-tlsserviceprofile }}*  *{{item. t59internalhostdetection }}*  *{{item. t59ipaddress}}*  *{{item. t59hostname }}* |
| {%tr endfor %} | |

#### Table 60- General on boarding locations info

|  |  |
| --- | --- |
| **Locations** | |
| {%tr for item in t60%} | |
| Africa, Europe & Middle East  Asia, Australia & Japan  North America & South America |  |
| {%tr endfor %} | |

#### Table 61- General on boarding IP Pool IPv4

|  |  |
| --- | --- |
| **IP Pool IPv4** | |
| {%tr for item in t61%} | |
| Africa, Europe & Middle East  Asia, Australia & Japan  North America & South America  Worldwide |  |
| {%tr endfor %} | |

#### Table 62- General on boarding IP Pool IPv6

|  |  |
| --- | --- |
| **IP Pool IPv6** | |
| {%tr for item in t62%} | |
| Worldwide |  |
| {%tr endfor %} | |

##### **Network Services**

#### Table 63- Manual Gateway Locations

|  |  |
| --- | --- |
| **Manual Gateway Locations** | |
| {%tr for item in t63%} | |
| Africa, Europe & Middle East  Asia, Australia & Japan  North America & South America |  |
| {%tr endfor %} | |

#### Mobile\_User\_Template GlobalProtect Settings for Prisma Access

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

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

<https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin.html>

<https://docs.paloaltonetworks.com/globalprotect/10-0/globalprotect-admin.html>

###### **General Settings**

Table 64- Appearance info

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Appearance** | | |
| {%tr for item in t64%} | | |
| GlobalProtect\_Portal | *Portal Login Page*  *Portal Landing Page*  *App Help Page* | *{{item.t64portalloginpage}}*  *{{item.t64portallandingpage}}*  *{{item.t64portalapphelppage}}* |
| {%tr endfor %} | | |

Table 65- Log setting

|  |  |  |
| --- | --- | --- |
| **Name** | **Appearance** | |
| {%tr for item in t65%} | | |
| GlobalProtect\_Portal | *Log Successful SSL Handshake*  *Log Unsuccessful SSL Handshake* | *{{item.t65logsuccessfulSSLHandshake}}*  *{{item.t65logunsuccessfulSSLHandshake}}* |
| {%tr endfor %} | | |

###### Authentication

**Client Authentication**

Table 66- Client authentication

|  |  |  |  |
| --- | --- | --- | --- |
| **OS** | **Name** | **Auth Profile** | **Allow Authentication with User Credentials or Client Certificate** |
| {%tr for item in t66%} | | | |
| *{{item. t66os}}* | *{{item. t66name}}* | *{{item. t66authprofile}}* | *{{item. t66clientCertificate}}* |
| {%tr endfor %} | | | |

Table 67- Portal Data Collection

|  |  |
| --- | --- |
| **Portal Data Collection** | |
| {%tr for item in t67%} | |
| **Certificate Profile for Configuration Selection** | *{{item. t67certificateprofileforconfigurationselection}}* |
| **Certificate Profile** | *{{item. t67certificateprofile}}* |
| {%tr endfor %} | |

Table 68- Customs Checks for Windows

|  |  |
| --- | --- |
| **Custom Checks - Windows** | |
| {%tr for item in t68%} | |
| **Registry Key** | *{{item. t68registrykey}}* |
| **Registry Value** | *{{item. t68registryvalue}}* |
| {%tr endfor %} | |

Table 69- Customs Checks for Mac

|  |  |
| --- | --- |
| **Custom Checks - Mac** | |
| {%tr for item in t69%} | |
| **Plist** | *{{item. t69plist}}* |
| **Key** | *{{item. t69key}}* |
| {%tr endfor %} | |

###### Agent

Table 70- Customs Checks for Mac

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Configs** | **User/User Group** | **OS** | **External Gateways** | **Internal Gateways** |
| {%tr for item in t70%} | | | | |
| *{{item. t70Configs}}* | *{{item. t70user}}* | *{{item. t70os}}* | *{{item. t70extgw}}* | *{{item. t70intgw}}* |
| {%tr endfor %} | | | | |

###### Clientless VPN

##### Gateway

### Mobile Users – Explicit Proxy

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prisma-access-for-users/secure-mobile-users-with-an-explicit-proxy.html#id622034b4-64a0-4924-b32a-14a6c2915cc3>

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/secure-mobile-users-with-prisma-access/explicit-proxy.html#id236be938-50d5-4244-9b9b-16393ad99ec0>

#### General Settings

##### Settings

##### Group Mapping Settings

##### Authentication Settings

#### Explicit Proxy Connection Setup

##### Settings

##### Locations

### Remote Networks

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prisma-access-for-networks.html>

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/secure-remote-networks-with-prisma-access.html>

#### General Settings

##### Settings

##### DNS Proxy

##### Group Mapping Settings

#### Zone Mapping

#### Aggregate Bandwidth

#### Remote Networks Onboarding

#### Inbound Access Remote Networks Onboarding

### Service Connections

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prepare-the-prisma-access-infrastructure/create-a-service-connection.html>

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prepare-the-prisma-access-infrastructure/create-a-service-connection-to-enable-access-between-users-and-networks.html>

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/prisma-access-service-connections.html>

#### Onboarding

### Traffic Steering

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prepare-the-prisma-access-infrastructure/use-traffic-forwarding-rules-with-service-connections.html>

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/prisma-access-service-connections/traffic-forwarding.html>

#### General Settings

#### Target Service Connections for Traffic Steering

#### Traffic Steering Rules

## Retrieve IP Addresses for Prisma Access

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prisma-access-overview/retrieve-ip-addresses-for-prisma-access.html>

*Retrieve the IPs that are active and reserved for Mobile Users and Remote Networks in Prisma Access. Delete the tables that are not in use/in scope.*

The API key can be used to interact with Prisma Access to obtain information about the service or set IP reservations.

Table 71- **Mobile Users - GlobalProtect Portal**

|  |  |  |  |
| --- | --- | --- | --- |
| **Locations** | **Active IPs** | **Reserved IPs** | |
| {%tr for item in t71%} | | |
| *{{item.t71locations}}* | *{{item.t71activeips}}* | *{{item.t71reservedips}}* |
| {%tr endfor %} | | |

Table 72- **Mobile Users - GlobalProtect Gateways**

|  |  |  |  |
| --- | --- | --- | --- |
| **Locations** | **Active IPs** | **Reserved IPs** | |
| {%tr for item in t72%} | | |
| *{{item.t72locations}}* | *{{item.t72activeips}}* | *{{item.t72reservedips}}* |
| {%tr endfor %} | | |

Table 73- **Mobile Users - Explicit Proxy**

|  |  |  |  |
| --- | --- | --- | --- |
| **Locations** | **Active IPs** | **Reserved IPs** | |
| {%tr for item in t72%} | | |
| *{{item.t73locations}}* | *{{item.t73activeips}}* | *{{item.t73reservedips}}* |
| {%tr endfor %} | | |

Table 74 Remote Networks

|  |  |
| --- | --- |
| **Remote Networks** | |
| {%tr for item in t74%} | |
| **Locations** | *{{item.t74locations}}* |
| **Active IPs** | *{{item.t74activeips}}* |
| {%tr endfor %} | |

## 

## HIP

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/redistribute-hip-information-and-run-hip-reports.html>

## Autonomous Digital Experience Management (ADEM)

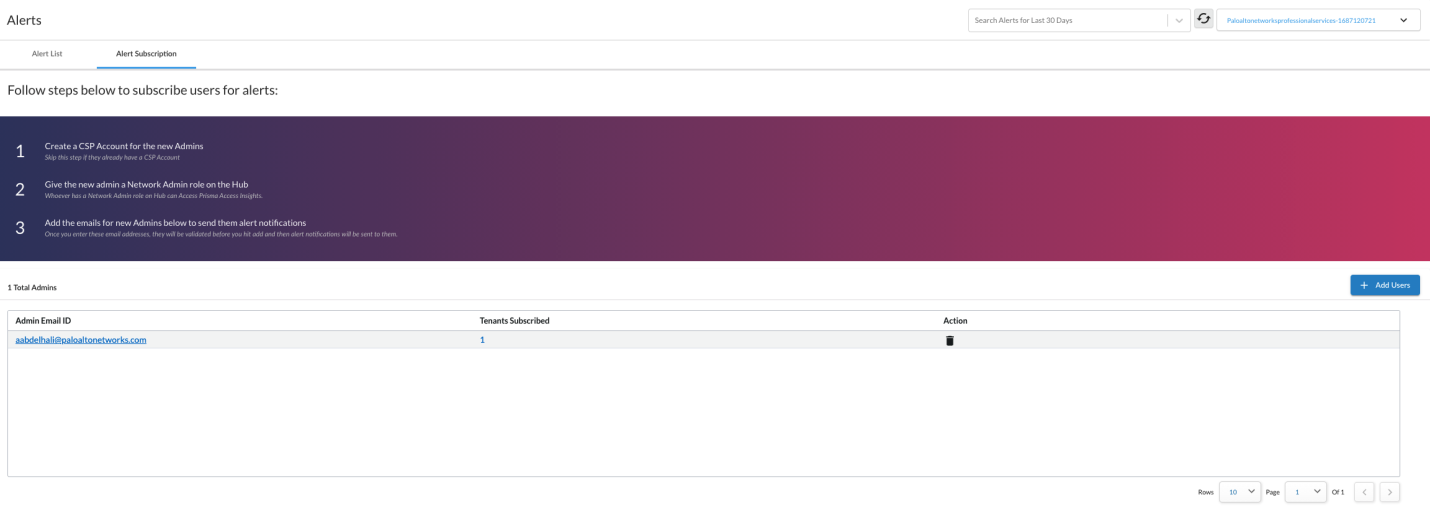
<https://docs.paloaltonetworks.com/autonomous-dem/autonomous-dem-in-prisma-access/autonomous-dem.html>

## Prisma Access Insights

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-insights/insights>

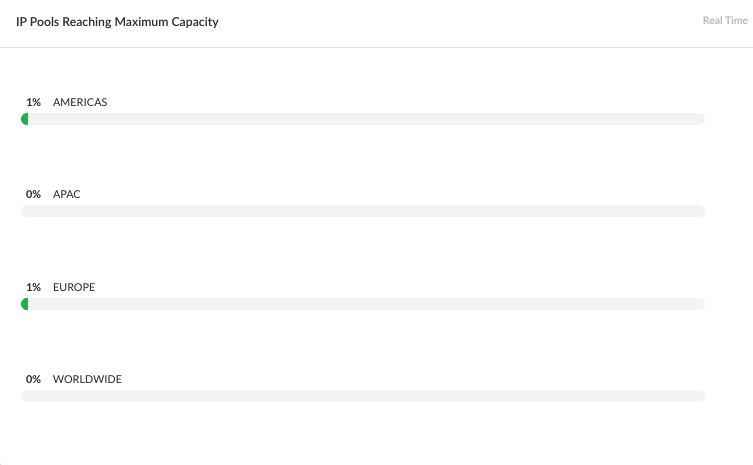
*Document the following Prisma Access fields as demonstrated here for Prisma Access.*

### Alert Subscription



*Figure 1 - Insights Alert Subscription*

### Mobile User IP Pool



*Figure 2 - Insights Mobile User IP Pools Utilization*

# Panorama

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

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

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin.html>

<https://docs.paloaltonetworks.com/panorama/10-0/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 24shows 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

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

[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)

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/manage-templates-and-template-stacks.html>

<https://docs.paloaltonetworks.com/panorama/10-0/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 25shows 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

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

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

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/manage-device-groups.html>

<https://docs.paloaltonetworks.com/panorama/10-0/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 %} | | | | | |

## Log Forwarding

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

[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)

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-log-collection/configure-log-forwarding-to-panorama.html>

<https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/manage-log-collection/configure-log-forwarding-to-panorama.html>

{{Customer}}has a single VM-Series Panorama deployed in Panorama mode. This allows 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 sends all traffic, threat, URL, Data, and WildFire logs to Panorama and the 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** |
| {%tr for item in t27%} | | | | | | |
| *{{item.t27devicename}}* | *{{item.t27profilename}}* | *{{item.t27logtype}}* | *{{item.t27panorama}}* | *{{item.t27snmp}}* | *{{item.t27email}}* | *{{item.t27syslog}}* |
| {%tr endfor %} | | | | | | |

## Security Profiles

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

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

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention.html>

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/threat-prevention.html>

*Describe each security profile that the customer has configured and 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** |
| {%tr for item in t28%} | | | | |
| *{{item.t28devicename}}* | *{{item.t28avprofilename}}* | *{{item.t28decoders}}* | *{{item.t28actions}}* | *{{item.t28wfactions}}* |
| {%tr endfor %} | | | | |

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

Table 29– Anti-Spyware Profile

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device Name** | **Profile Name** | **Severity** | **Action** | **DNS Sinkhole?** |
| {%tr for item in t29%} | | | | |
| *{{item.t29devicename}}* | *{{item.t29asprofilename}}* | *{{item.t29severity}}* | *{{item.t29actions}}* | *{{item.t29dnssink}}* |
| {%tr endfor %} | | | | |

The Vulnerability profile details are shown in Table 30.

Table 30– Vulnerability Profiles

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device Name** | **Profile Name** | **Rule Name** | **Severity** | **Action** |
| {%tr for item in t30%} | | | | |
| *{{item.t30devicename}}* | *{{item.t30vprofilename}}* | *{{item.t30rulename}}* | *{{item.t30severity}}* | *{{item.t30action}}* |
| {%tr endfor %} | | | | |

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** |
| {%tr for item in t31%} | | | | | | | |
| *{{item.t31devicename}}* | *{{item.t31profilename}}* | *{{item.t31blocked}}* | *{{item.t31allow}}* | *{{item.t31alert}}* | *{{item.t31continue}}* | *{{item.t31override}}* | *{{item.t31credential}}* |
| {%tr endfor %} | | | | | | | |

The WildFire profile details are shown in Table 32.

Table 32–WildFire Profile Details

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Device Name** | **Profile Name** | **Applications** | **File Types** | **Direction** | **Analysis** |
| {%tr for item in t32%} | | | | | |
| *{{item.t32devicename}}* | *{{item.t32profilename}}* | *{{item.t32applications}}* | *{{item.t32filetypes}}* | *{{item.t32direction}}* | *{{item.t32analysis}}* |
| {%tr endfor %} | | | | | |

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** |
| {%tr for item in t33%} | | | | | |
| *{{item.t33devicename}}* | *{{item.t33rulename}}* | *{{item.t33applications}}* | *{{item.t33filetypes}}* | *{{item.t33direction}}* | *{{item.t33action}}* |
| {%tr endfor %} | | | | | |

Data pattern object details are shown in Table 34.

Table 34– Data Pattern Objects

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Device Name** | **Profile Name** | **Pattern Type** | **Name** | **File Types** | **Pattern** |
| {%tr for item in t34%} | | | | | |
| *{{item.t34devicename}}* | *{{item.t34profilename}}* | *{{item.t34patterntype}}* | *{{item.t34name}}* | *{{item.t34filetypes}}* | *{{item.t34pattern}}* |
| {%tr endfor %} | | | | | |

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** |
| {%tr for item in t35%} | | | | | | | |
| *{{item.t35devicename}}* | *{{item.t35rulename}}* | *{{item.t35apps}}* | *{{item.t35filetype}}* | *{{item.t35patterns}}* | *{{item.t35direction}}* | *{{item.t35alert}}* | *{{item.t35block}}* |
| {%tr endfor %} | | | | | | | |

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)** |
| {%tr for item in t36%} | | | | | | | | |
| *{{item.t36devicename}}* | *{{item.t36profilename}}* | *{{item.t36type}}* | *{{item.t36syn}}* | *{{item.t36udp}}* | *{{item.t36icmp}}* | *{{item.t36icmp6}}* | *{{item.t36flood}}* | *{{item.t36rps}}* |
| {%tr endfor %} | | | | | | | | |

## 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** |
| {%tr for item in t37%} | | | | | | | | |
| *{{item.t37devicename}}* | *{{item.t37groupname}}* | *{{item.t37av}}* | *{{item.t37as}}* | *{{item.t37vp}}* | *{{item.t37fb}}* | *{{item.t37df}}* | *{{item.t37wf}}* | *{{item.t37url}}* |
| {%tr endfor %} | | | | | | | | |

## {{Customer}}Security Profiles Configuration

*Describe the customers use of security profiles onSecurity 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

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

[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)

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/software-and-content-updates/dynamic-content-updates.html>

<https://docs.paloaltonetworks.com/pan-os/10-0/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** |
| {%tr for item in t38%} | | | | | |
| *{{item.t38devicename}}* | *{{item.t38type}}* | *{{item.t38recurrence}}* | *{{item.t38time}}* | *{{item.t38action}}* | *{{item.t38threshold}}* |
| {%tr endfor %} | | | | | |

# User-ID

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

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

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id.html>

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/user-id.html>

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/configure-user-based-policies-with-prisma-access.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** |
| {%tr for item in t39%} | | | | | |
| *{{item.t39devicename}}* | *{{item.t39source}}* | *{{item.t39type}}* | *{{item.t39ipaddress}}* | *{{item.t39port}}* | *{{item.t39interface}}* |
| {%tr endfor %} | | | | | |

## LDAP 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** |
| {%tr for item in t40%} | | | | | | |
| *{{item.t40devicename}}* | *{{item.t40serverprofile}}* | *{{item.t40domain}}* | *{{item.t40group}}* | *{{item.t40user}}* | *{{item.t40attributes}}* | *{{item.t40includelist}}* |
| {%tr endfor %} | | | | | | |

## Cloud Identity Engine Group Mapping

<https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/configure-user-based-policies-with-prisma-access/collect-user-and-group-information-using-the-cloud-identity-engine>

# SNMP

*Delete the PAN-OS document links that are not related to the Customer’s environment.*

[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)

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/snmp-monitoring-and-traps.html>

<https://docs.paloaltonetworks.com/pan-os/10-0/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 |
| {%tr for item in t41%} | | | | |
| *{{item.t41devicename}}* | *{{item.t41profilename}}* | *{{item.t41managername}}* | *{{item.t41managerip}}* | *{{item.t41communitystring}}* |
| {%tr endfor %} | | | | |

## SNMPv2 Settings

SNMPv2 settings are shown in Table 42.

Table 42– SNMPv2 Settings

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device Name | Physical Location | Contact | Version | Community String |
| {%tr for item in t42%} | | | | |
| *{{item.t42devicename}}* | *{{item.t42location}}* | *{{item.t42contact}}* | *{{item.t42version}}* | *{{item.t42community}}* |
| {%tr endfor %} | | | | |

## SNMPv3 Settings

SNMPv3 settings are shown in Table 43 and Table 44.

Table 43– Views

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device Name | Name | View | OID | Option | Mask |
| {%tr for item in t43%} | | | | | |
| *{{item.t43devicename}}* | *{{item.t43name}}* | *{{item.t43view}}* | *{{item.t43oid}}* | *{{item.t43option}}* | *{{item.t43mask}}* |
| {%tr endfor %} | | | | | |

Table 44– Users

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device Name | Users | View | Auth Password | Priv Password |
| {%tr for item in t44%} |  |  |  |  |
| *{{item.t44devicename}}* | *{{item.t44users}}* | *{{item.t44view}}* |  |  |
| *{%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. >*

## Cloud Services Plug-In

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

## Prisma Public Cloud

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

## SaaS Security API/In-Line

*< 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. >*

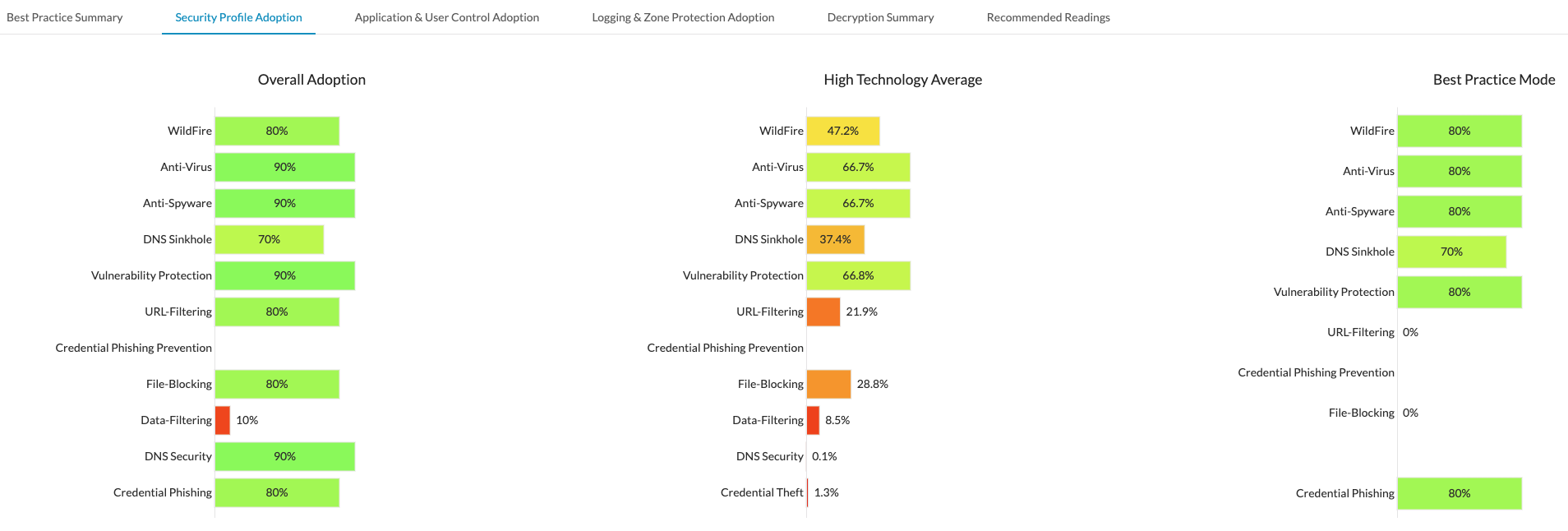
# Best Practice Assessment (BPA)

*Document the following BPA field as demonstrated here for Firewalls, Panorama, or Prisma Access.*

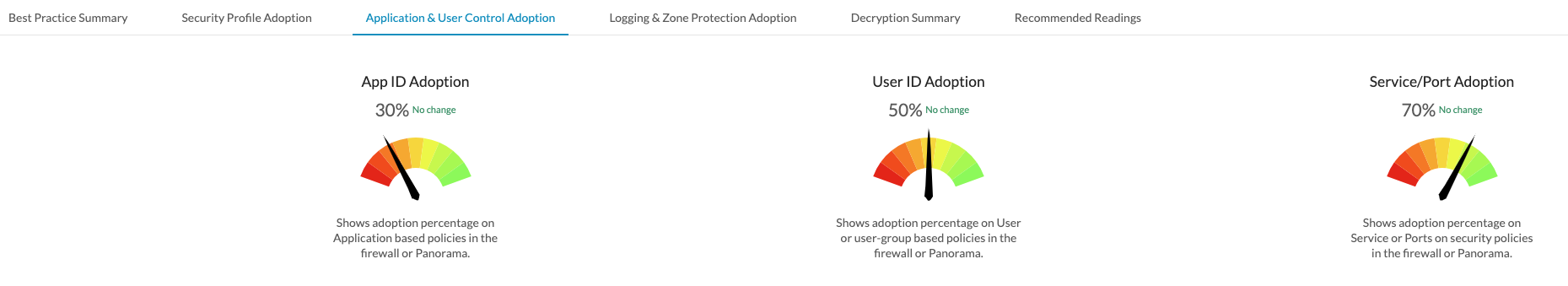
## BPA Report



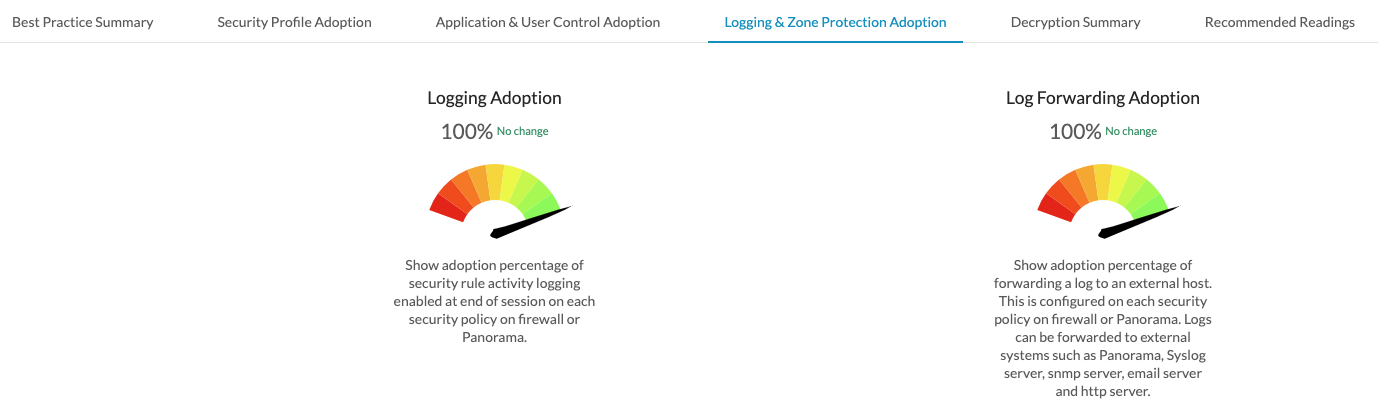
*Figure 3 - BPA Capability and Control Category*



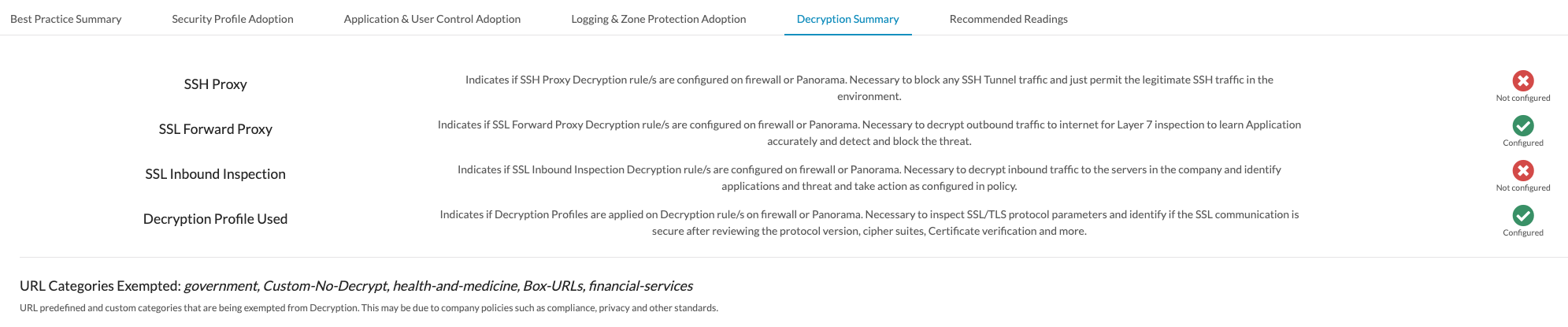
*Figure 4 - BPA Security Profile Adoption*



*Figure 5 - BPA Application and User Control Adoption*



*Figure 6 - BPA Logging Adoption*



*Figure 7 - BPA Decryption Summary*

## Best Practices Guides

* [Starting Best Practices with the BPA and Security Assurance (Version 10.0)](https://docs.paloaltonetworks.com/best-practices/10-0/best-practices-getting-started.html)
* [Best Practices for Securing Administrative Access (Version 10.0)](https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/getting-started/best-practices-for-securing-administrative-access.html)
* [Best Practices Implementing Zero Trust With Palo Alto Networks (Version 10.0)](https://docs.paloaltonetworks.com/best-practices/10-0/zero-trust-best-practices.html)
* [Internet Gateway Best Practice Security Policy (Version 10.0)](https://docs.paloaltonetworks.com/best-practices/10-0/internet-gateway-best-practices.html)
* [Decryption Best Practices (Version 10.0)](https://docs.paloaltonetworks.com/best-practices/10-0/decryption-best-practices.html)
* [Best Practices for Migrating to Application-Based Policy (Version 10.0)](https://docs.paloaltonetworks.com/best-practices/10-0/best-practices-for-migrating-to-application-based-policy.html)
* [Autonomous DEM in Prisma Access](https://docs.paloaltonetworks.com/autonomous-dem/autonomous-dem-in-prisma-access.html)

# Third Party Integrations

*This section is devoted to the documentation of any third-party tools integrated into the Palo Alto Networks deployed solution. This can include 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* |