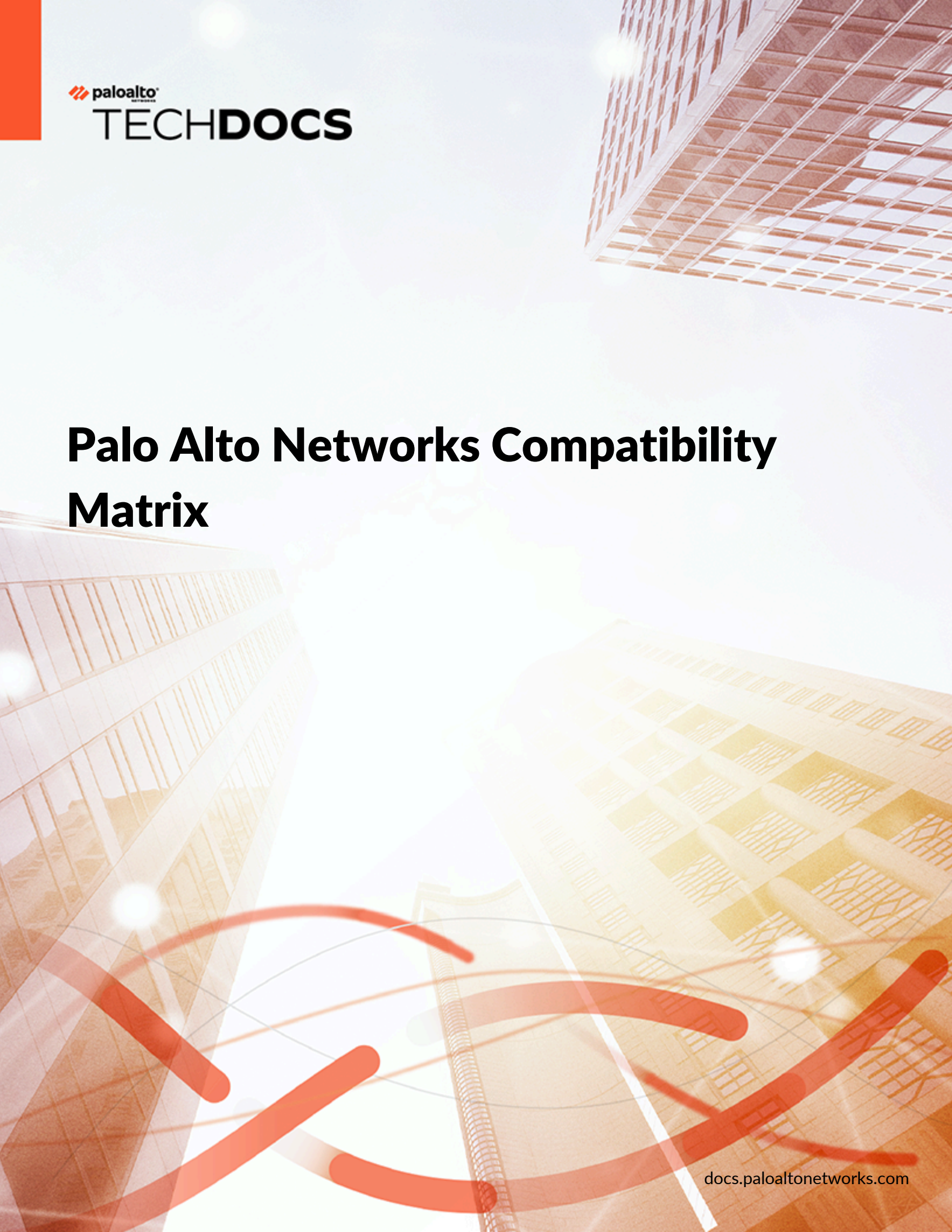
paloalto TECHDOCS

Palo Alto Networks Compatibility Matrix



docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

August 22, 2025

Table of Contents

Supported OS Releases by Model

Use the tables throughout this Palo Alto Networks Compatibility Matrix to determine support for Palo Alto Networks Next-Generation Firewalls, appliances, and agents. Additionally, refer to the product comparison tool for detailed information about Palo Alto Networks firewalls by model, including specifications for throughput, maximum number of sessions, rules, objects, tunnels, and zones.

For supported operating systems on firewalls and appliances and for high-availability (HA) port and processor support on firewalls, review the following topics:

- Palo Alto Networks Next-Generation Firewalls
- Palo Alto Networks Appliances
- WF-500 Appliance Analysis Environment Support
- Palo Alto Networks PA-7000 Series Firewall Cards
- HA Port and Processor Support
- Breakout Port Support

Palo Alto Networks Next-Generation Firewalls

The following table shows the PAN-OS® releases supported for each of the Palo Alto Networks Next-Generation Firewall hardware, VM-Series, and CN-Series models. You can also review PAN-OS support for PA-7000 Series cards and PA-5450 firewall cards as well as for Palo Alto Networks appliances.

Palo Alto Networks Firewall Model	PAN-OS 9.1	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
Hardware Firewalls						
PA-220 Firewall	√	√	√	—	—	—
PA-220R Firewall	√	√	√	—	—	—
PA-410 Firewall	—	√ 10.1.2 & later	√	√	√	√
PA-410R Firewall	—	—	—	—	√ 11.1.3 & later	√
PA-410R-5G Firewall	—	—	—	—	√ 11.1.4 & later	√
PA-415-5G Firewall	—	—	—	—	√	√
PA-415 and PA-445 Firewalls	—	—	—	√	√	√
PA-440, PA-450, and PA-460 Firewalls	—	√	√	√	√	√
PA-450R Firewall	—	—	—	—	√	√
PA-450R-5G	—	—	—	—	√	√
PA-455 Firewall	—	—	—	—	√	√
PA-455-5G	—	—	—	—	—	√

Palo Alto Networks Firewall Model	PAN-OS 9.1	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
						11.2.3 & later
PA-800 Series Firewalls	√	√	√	√	√	–
PA-1400 Series Firewalls	–	–	–	√	√	√
PA-3200 Series Firewalls	√	√	√	√	√	–
PA-3400 Series Firewalls	–	–	√	√	√	√
PA-5200 Series Firewalls	√	√	√	√	√	√
PA-5410, PA-5420, and PA-5430 Firewalls	–	–	√	√	√	√
PA-5440 Firewall	–	–	–	√	√	√
PA-5445 Firewall	–	–	–	–	√	√
PA-5450 Firewall	–	√	√	√	√	√
PA-7000 Series Firewalls	√	√	√	√	√	√
PA-7500 Firewall	–	–	–	–	√	–
VM-Series Firewalls						
Flexible vCPU Firewalls (Up to 32 cores)	–	√	√	√	√	√
Flexible vCPU Firewalls (Up to 64 cores)	–	–	√	√	√	√
VM-50 Firewall	√	√	√	√	√	√

Palo Alto Networks Firewall Model	PAN-OS 9.1	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
VM-100 Firewall	√	√	√	√	√	√
VM-200 Firewall	√	√	√	√	√	√
VM-300 Firewall	√	√	√	√	√	√
VM-500 Firewall	√	√	√	√	√	√
VM-700 Firewall	√	√	√	√	√	√
VM-1000-HV Firewall	√	√	√	√	√	√
CN-Series Firewall						
CN-Series Small CN-MGMT Mem: 2GB CN-NGFW Mem: 2 to 2.5GB	—	√	√	√	√	√
CN-Series Medium CN-MGMT Mem: 2GB CN-NGFW Mem: 6GB	—	√	√	√	√	√
CN-Series Large CN-MGMT Mem: 4GB CN-NGFW Mem: 48GB	—	√	√	√	√	√

* You should also review the hardware EoL information for more specific information about firewalls and appliances that have reached end-of-sale (EoS) status.

Palo Alto Networks Appliances

The following table shows PAN-OS® release support for each Palo Alto Networks (non-firewall) appliance. You can also review PAN-OS release support for Palo Alto Networks Next-Generation Firewalls.

Palo Alto Networks Appliance	Release 9.1*	Release 10.1	Release 10.2	Release 11.0	Release 11.1	Release 11.2
Panorama Virtual Appliance	√	√	√	√	√	√
M-200 Appliance	√	√	√	√	√	√
M-300 Appliance	—	—	√	√	√	√
M-500 Appliance (EoL)	√	√	—	—	—	—
M-600 Appliance	√	√	√	√	√	√
M-700 Appliance	—	—	√	√	√	√
WF-500 Appliance(*)	√	√	√ 10.2.2 & later	√	√	√
WF-500-B Appliance(*)	—	—	√ 10.2.2 & later	√	√	√

* WF-500 appliances have optional guest VM images that provide support for additional analysis environments. For information about which VMs are available for a specific PAN-OS® (WildFire®) release, refer to WF-500 Appliance Analysis Environment Support.

** For more specific information about firewalls and appliances that have reached end-of-sale (EoS) status, review our hardware EoL web page.

WF-500 Appliance Analysis Environment Support

We support the following WildFire® guest VM images (analysis environments) in PAN-OS® (WildFire) releases. When ready, upgrade your WF-500 appliances to the appropriate image.

Make sure to download and install the correct WildFire VM image for your WF-500 appliances. Installing a WildFire VM image that the PAN-OS (WildFire) release running on your appliance does not support will produce error messages, fail to process samples, and won't detect malware as expected.

WF-500 Appliance Analysis Environment	VM ID	WF-500 Appliance Guest VM Filename	Minimum Compatible PAN-OS Version
Windows XP (Adobe Reader 11, Flash 11, Office 2010)	vm-3	WFWinXpAddon3_m-1.0.1.xpaddon3	10.2.2 and later
		WFWinXpAddon3_m-1.0.0.xpaddon3*	10.1 and earlier
Windows 7 x64 SP1 (Adobe Reader 11, Flash 11, Office 2010)	vm-5	WFWin7_64Addon1_m-1.0.1.7_64addon1	10.2.2 and later
		WFWin7_64Addon1_m-1.0.0.7_64addon1	10.1 and earlier
		WFWin7_64Base_m-1.0.0.7_64base *This is a required base VM image package for the proper function of the Windows 7 analysis environment.*	10.1 and earlier
Windows XP (Internet Explorer 8, Flash 11, Elink analysis support)	vm-6*	WFWinXpGf_m-1.0.0.xpgf	10.1 and earlier
		WFWinXpGf_m-1.0.1.xpgf	10.2.2 and later
Windows 10 x64 (Adobe Reader 11, Flash 11, Office 2010)	vm-7	WFWin10Base_m-1.0.1.10base	10.2.2 and later
		WFWin10Base_m-1.0.0-c2.10base	10.1 and earlier

** You cannot select this WF-500 appliance analysis environment through the WF-500 appliance CLI.*

Palo Alto Networks PA-7000 Series Cards

The following table shows the PAN-OS® releases supported for each of the system cards and for each of the network and data processing cards available for PA-7000 Series firewalls. You can also review PAN-OS support for each Palo Alto Networks Next-Generation Firewall, for all other Palo Alto Networks appliances, and for the data processing cards for the PA-5450 firewall or the PA-7500 firewall.

PA-7000 Series Firewall Cards	PAN-OS 9.1	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
Network and Data Processing Cards						
PAN-PA-7000-20GXM-NPC	√	√	—	—	—	—
PAN-PA-7000-20GQXM-NPC	√	√	—	—	—	—
PAN-PA-7000-100G-NPC-A	√	√	√	√	√	√
PAN-PA-7000-DPC-A	—	√	√	√	√	√
System Cards						
PAN-PA-7050-SMC	√	√* (*until February 28, 2026)	—	—	—	—
PAN-PA-7050-SMC (v2)	√	√* (*until February 28, 2026)	—	—	—	—
PAN-PA-7050-SMC-B	√	√	√	√	√	√
PAN-PA-7080-SMC	√	√* (*until February 28, 2026)	—	—	—	—

PA-7000 Series Firewall Cards	PAN-OS 9.1	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
PAN-PA-7080-SMC (v2)	√	√* (*until February 28, 2026)	—	—	—	—
PAN-PA-7080-SMC-B	√	√	√	√	√	√
PAN-PA-7000-LPC	√	√* (*until February 28, 2026)	—	—	—	—
PAN-PA-7000-LFC-A	√	√	√	√	√	√

Palo Alto Networks PA-5450 Cards

The following table shows the PAN-OS® releases supported for each of the system, network, and data processing cards available for the PA-5450 firewall. You can also review PAN-OS support for each Palo Alto Networks Next-Generation Firewall, each of our other Palo Alto Networks appliances, and for the data processing cards for the PA-7000 Series firewalls or the PA-7500 firewall.

PA-5450 Firewall Cards	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
Network and Data Processing Cards					
PAN-PA-5400-NC-A	√	√	√	√	√
PAN-PA-5400-DPC-A	√	√	√	√	√
System Cards					
PAN-PA-5400-BC-A	√	√	√	√	√
PAN-PA-5400-MPC-A	√	√	√	√	√

Palo Alto Networks PA-7500 Cards

The following table shows the PAN-OS® releases supported for each of the system, network, and data processing cards available for the PA-7500 firewall. You can also review PAN-OS support for each Palo Alto Networks Next-Generation Firewall, each of our other Palo Alto Networks appliances, and for the data processing cards for the PA-7000 Series firewalls or the PA-5450 firewall.

PA-7500 Firewall Cards	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1
Network and Data Processing Cards				
PAN-PA-7500-NPC-A	—	—	—	√
PAN-PA-7500-DPC-A	—	—	—	√
System Cards				
PAN-PA-7500-MPC-A	—	—	—	√
PAN-PA-7500-SFC-A	—	—	—	√

HA Port and Processor Support

The following table identifies which Palo Alto Networks Next-Generation Firewall (NGFW) can support the HA ports and processor functionality you require in your network.

Additionally, some firewall models and PA-7000 Series firewall cards include an offload processor—a Content Engine (CE) for accelerating signature matches or a Crypto Accelerator (CA) for accelerating SSL processing; some firewalls support either one but none can support both simultaneously.

Palo Alto Networks Firewall Model	Separate Mgmt Plane Processor	Network Processor	Offload Processor	First Packet Processor	HA1 Port	HA2 Port	HSCI Port
Firewalls							
PA-220 (EoS)*	—	—	—	—	—	—	—
PA-220R (EoS)*	—	—	—	—	—	—	—
PA-410	—	—	—	—	—	—	—
PA-415	—	—	—	—	—	—	—
PA-415-5G	—	—	—	—	—	—	—
PA-440	—	—	—	—	—	—	—
PA-445	—	—	—	—	—	—	—
PA-450	—	—	—	—	—	—	—
PA-450R	—	—	—	—	—	—	—
PA-455	—	—	—	—	—	—	—
PA-455-5G	—	—	—	—	—	—	—
PA-460	—	—	—	—	—	—	—
PA-820*	—	—	—	—	√	√	—
PA-850*	—	—	—	—	√	√	—
PA-1410	—	—	—	—	√ (x2)	—	√

Palo Alto Networks Firewall Model	Separate Mgmt Plane Processor	Network Processor	Offload Processor	First Packet Processor	HA1 Port	HA2 Port	HSCI Port
PA-1420	—	—	—	—	√ (x2)	—	√
PA-3220 (EoS)*	√	√	—	—	√ (x2)	—	√
PA-3250 (EoS)*	√	√	√ (CE)	—	√ (x2)	—	√
PA-3260 (EoS)*	√	√	√ (CE)	—	√ (x2)	—	√
PA-3410	√	√	—	—	√ (x2)	—	√
PA-3420	√	√	—	—	√ (x2)	—	√
PA-3430	√	√	—	—	√ (x2)	—	√
PA-3440	√	√	—	—	√ (x2)	—	√
PA-5220 (EoS)*	√	√	√ (CE or CA)	√	√ (x2)	—	√
PA-5250 (EoS)*	√	√	√ (CE or CA)	√	√ (x2)	—	√
PA-5260 (EoS)*	√	√	√ (CE or CA)	√	√ (x2)	—	√
PA-5280 (EoS)*	√	√	√	√	√	—	√

Palo Alto Networks Firewall Model	Separate Mgmt Plane Processor	Network Processor	Offload Processor	First Packet Processor	HA1 Port	HA2 Port	HSCI Port
			(CE or CA)		(x2)		
PA-5410	—	—	—	—	√ (x2)	—	√
PA-5420	—	—	—	—	√ (x2)	—	√
PA-5430	—	—	—	—	√ (x2)	—	√
PA-5440	—	—	—	—	√ (x2)	—	√
PA-5445	—	—	—	—	√ (x2)	—	√
PA-5450	√	√	√ (CE or CA)	√	√ (x2)	—	√ (x2)
PA-7050	√	√	√ (CE or CA)	√	√ (x2)	—	√ (x2)
PA-7080	√	√	√ (CE or CA)	√	√ (x2)	—	√ (x2)
PA-7500	√	√	√ (CE or CA)	√	—	—	√ (x2)
PA-7000 Series Firewall Cards							
PA-7050-SMC (EoS)*	√	—	—	√	√ (x2)	—	√ (x2)

Palo Alto Networks Firewall Model	Separate Mgmt Plane Processor	Network Processor	Offload Processor	First Packet Processor	HA1 Port	HA2 Port	HSCI Port
PA-7080-SMC (EoS)*	√	—	—	√	√ (x2)	—	√ (x2)
PA-7050-SMC-B	√	—	—	√	√ (x2)	—	√ (x2)
PA-7080-SMC-B	√	—	—	√	√ (x2)	—	√ (x2)
PA-7000-20GXM-NPC (EoS)*	—	√	√ (CE x2)	—	—	—	—
PA-7000-20GQXM-NPC (EoS)*	—	√	√ (CE x2)	—	—	—	—
PA-7000-100G-NPC-A	—	√	√ (CE or CA)	—	—	—	—
PA-7000-DPC-A	—	—	√ (CA x2)	—	—	—	—

* Some of the firewalls and firewall cards in this table have reached end-of-sale (EoS), are not supported in newer versions of PAN-OS software, or both. Be sure to review the specific information for your firewalls, firewall cards, and appliances on the hardware EoL web page.

Breakout Port Support

The following table identifies which Palo Alto Networks Next-Generation Firewalls (NGFWs) support the breakout feature of the QSFP+/QSFP28 ports. When a port is broken out using a breakout cable, the port functions as four new independent interfaces whose speeds are a quarter of the speed of the broken out port. This allows you to split your network connections into additional, lower speed channels that link to multiple network switches or devices.

Palo Alto Networks Firewall Model	Breakout Support	Breakout Ports	Breakout Speed
PA-220	—	—	—
PA-220R	—	—	—
PA-410	—	—	—
PA-410R	—	—	—
PA-410R-5G	—	—	—
PA-415	—	—	—
PA-415-5G	—	—	—
PA-440	—	—	—
PA-445	—	—	—
PA-450	—	—	—
PA-450R	—	—	—
PA-450R-5G	—	—	—
PA-455	—	—	—
PA-455-5G	—	—	—
PA-460	—	—	—
PA-820	—	—	—
PA-850	—	—	—
PA-1410	—	—	—

Palo Alto Networks Firewall Model	Breakout Support	Breakout Ports	Breakout Speed
PA-1420	—	—	—
PA-3220	—	—	—
PA-3250	—	—	—
PA-3260	—	—	—
PA-3410	—	—	—
PA-3420	—	—	—
PA-3430	√	• Port 35 — Ports 27, 28, 29, and 30 • Port 36 — Ports 31, 32, 33, and 34	10Gbps/25Gbps
PA-3440	√	• Port 35 — Ports 27, 28, 29, and 30 • Port 36 — Ports 31, 32, 33, and 34	10Gbps/25Gbps
PA-5220	—	—	—
PA-5250	—	—	—
PA-5260	—	—	—
PA-5280	—	—	—
PA-5410	√	• Port 41 — Ports 25, 26, 27, and 28 • Port 42 — Ports 29, 30, 31, and 32 • Port 43 — Ports 33, 34, 35, and 36 • Port 44 — Ports 37, 38, 39, and 40	10Gbps/25Gbps
PA-5420	√	• Port 41 — Ports 25, 26, 27, and 28 • Port 42 — Ports 29, 30, 31, and 32	10Gbps/25Gbps

Palo Alto Networks Firewall Model	Breakout Support	Breakout Ports	Breakout Speed
		• Port 43 — Ports 33, 34, 35, and 36 • Port 44 — Ports 37, 38, 39, and 40	
PA-5430	√	• Port 41 — Ports 25, 26, 27, and 28 • Port 42 — Ports 29, 30, 31, and 32 • Port 43 — Ports 33, 34, 35, and 36 • Port 44 — Ports 37, 38, 39, and 40	10Gbps/25Gbps
PA-5440	√	• Port 41 — Ports 25, 26, 27, and 28 • Port 42 — Ports 29, 30, 31, and 32 • Port 43 — Ports 33, 34, 35, and 36 • Port 44 — Ports 37, 38, 39, and 40	10Gbps/25Gbps
PA-5445	√	• Port 41 — Ports 25, 26, 27, and 28 • Port 42 — Ports 29, 30, 31, and 32 • Port 43 — Ports 33, 34, 35, and 36 • Port 44 — Ports 37, 38, 39, and 40	10Gbps/25Gbps
PA-5450 (PA-5400 NC-A)	√	• Port 25 — Ports 5, 6, 7, and 8 • Port 26 — Ports 9, 10, 11, and 12	10Gbps/25Gbps
PA-7050 (PA-7000 100G-NPC)	√ PAN-OS 10.2 & later	• Port 25 — Ports 9, 10, 11, and 12 • Port 26 — Ports 13, 14, 15, and 16 • Port 27 — Ports 17, 18, 19, and 20	10Gbps/25Gbps

Palo Alto Networks Firewall Model	Breakout Support	Breakout Ports	Breakout Speed
		• Port 28 — Ports 21, 22, 23, and 24	
PA-7050 (PA-7000 LFC)	√ PAN-OS 10.2 & later	• Port 9 — Ports 1, 2, 3, and 4 • Port 10 — Ports 5, 6, 7, and 8	10Gbps
PA-7080 (PA-7000 100G-NPC)	√ PAN-OS 10.2 & later	• Port 25 — Ports 9, 10, 11, and 12 • Port 26 — Ports 13, 14, 15, and 16 • Port 27 — Ports 17, 18, 19, and 20 • Port 28 — Ports 21, 22, 23, and 24	10Gbps/25Gbps
PA-7080 (PA-7000 LFC)	√ PAN-OS 10.2 & later	• Port 9 — Ports 1, 2, 3, and 4 • Port 10 — Ports 5, 6, 7, and 8	10Gbps
PA-7500 (PA-7500 NPC)	√	• Port 1 — Ports 21, 22, 23, and 24 • Port 2 — Ports 25, 26, 27, and 28 • Port 3 — Ports 29, 30, 31, and 32 • Port 4 — Ports 33, 34, 35, and 36 • Port 11 — Ports 37, 38, 39, and 40 • Port 12 — Ports 41, 42, 43, and 44 • Port 13 — Ports 45, 46, 47, and 48 • Port 14 — Ports 49, 50, 51, and 52	10Gbps/25Gbps/100Gbps

VM-Series Firewalls

The hypervisors and the public cloud regions in which you can deploy the VM-Series firewalls:

- VM-Series Firewall Hypervisor Support
- PacketMMAP and DPDK Drivers on VM-Series Firewalls
- Partner Interoperability for VM-Series Firewalls
- VM-Series Plugin
- AWS and AWS Gov Cloud Regions
- Azure Regions
- Google Cloud Regions
- OCI Cloud Regions
- Alibaba Cloud Regions
- AWS CFT Amazon Machine Images (AMI) List

For the best instance types for optimal VM-Series capacity and performance, review the VM-Series Capacity & Performance document.

VM-Series Firewall OpenShift Virtualization and Hypervisor Support

VM-Series Firewall OpenShift Virtualization Support

PAN-OS Version Support (Minimum)	OpenShift Version Support	Notes
PAN-OS 11.2.x (11.2.5)	4.17	OpenShift virtualization allows running VM-Series firewalls.

VM-Series Firewall Hypervisor Support

Palo Alto Networks offers hypervisor version support on VM-Series firewalls for the following deployments:

- Private Cloud Deployments
- Public Cloud Deployments

Private Cloud Deployments

The following Private Clouds require a PAN-OS for VM-Series base image from the Palo Alto Networks Support Portal:

- VM-Series for VMware vSphere Hypervisor (ESXi)
- VM-Series for VMware NSX-V
- VM-Series for VMware NSX (Formerly NSX-T)
- VM-Series for KVM
- VM-Series for Nutanix
- VM-Series for Hyper-V
- VM-Series for OpenStack
- Cisco ACI: Hardware and VM-Series Firewalls in Cisco ACI

In the compatibility matrix below, the PAN-OS Version Support column displays the range of versions and the (Minimum) version in parentheses. For example, if the PAN-OS Version Support column displays **PAN-OS 11.1.x (11.1.3)**, it indicates that the integration supports PAN-OS 11.1 versions beginning with PAN-OS 11.1.3.

Further I/O Enhancement support is detailed in the list of PacketMMAP and DPDK Drivers on VM-Series Firewalls.

VM-Series for VMware vSphere Hypervisor (ESXi)

This ESXi version support list does not include NSX. For NSX, see VM-Series for VMware NSX-V or VM-Series for VMware NSX (Formerly NSX-T).

You can download base images from the Palo Alto Networks Support Portal.

Access mode with SR-IOV on VMware ESXi is supported on PAN-OS 9.1.5 and later PAN-OS 9.1 versions and all later PAN-OS versions but only with VM-Series plugin 2.0.5 and later plugin versions. However, you must enable VLAN access mode for ESXi where needed.

VMware ESXi Version Support	VMware Virtual Machine Hardware Version	PAN-OS Version Support (Minimum)	I/O Enhancement Support	Base Image
8.0	• vmx-10 • vmx-15	PAN-OS 11.2.x (11.2.6)	SR-IOV, DPDK	**PA-VM-ESX-11.2.6.ova**
	• vmx-15	PAN-OS 11.1.x (11.1.6-h4) PAN-OS 11.2.x (11.2.6)	SR-IOV, DPDK	**PA-VM-ESX-11.1.6-h4.ova** **PA-VM-ESX-11.2.6.ova**
6.7, 7.0, 8.0	• vmx-10 • vmx-15	PAN-OS 11.1.x (11.1.0)	SR-IOV, DPDK	**PA-VM-ESX-11.1.6-h4.ova**
6.7, 7.0, 8.0	vmx-10	PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0)	SR-IOV, DPDK	**PA-VM-ESX-10.2.3.ova** **PA-VM-ESX-11.0.0.ova**
6.7, 7.0	vmx-10	PAN-OS 9.1.x (9.1.0) PAN-OS 10.1.x (10.1.0)	SR-IOV, DPDK	**PA-VM-ESX-9.1.0.ova** **PA-VM-ESX-10.1.0.ova**
6.5, 6.7	vmx-10	PAN-OS 9.1.x (9.1.0)	SR-IOV, DPDK	**PA-VM-ESX-9.1.0.ova**

VM-Series for VMware NSX-V

vSphere with VMware NSX is available on all VM-Series firewalls except the VM-50 and VM-700 firewalls.

Palo Alto Networks approves the vSphere with VMware NSX and Panorama combinations listed below with the following criteria. You can download base images from the Palo Alto Networks Support Portal.

For versions of PAN-OS certified by VMware, see the VMware Compatibility Guide.

- Panorama management servers running PAN-OS 9.1 and later versions require the VMware NSX plugin. For more plugin version information, see Panorama Plugins for VMware NSX.
- VMware has announced EoS for NSX-V and Palo Alto Networks will continue to support the VM-Series on NSX-V running PAN-OS 9.1 when managed by Panorama management servers running PAN-OS 10.1 or PAN-OS 10.2 software.
  - Palo Alto Networks does not support VMware NSX-V on Panorama management servers running PAN-OS 11.0 or later versions.
  - There aren't any VM-Series for VMware NSX-V base images for PAN-OS 10.1 or later PAN-OS versions.
  - You cannot upgrade the VM-Series firewall for NSX-V to PAN-OS 10.1 or later PAN-OS versions.
  - The Panorama management server running PAN-OS 10.1 or PAN-OS 10.2 supports PAN-OS 9.1 base images until June 30, 2024.

See the Palo Alto Networks End-of-Life Summary for more information about the PAN-OS EoL schedule.

Supported Panorama Versions	PAN-OS Version Support	Panorama Plugin for NSX	VMware NSX-V Manager	vSphere	VMware Virtual Machine Hardware Version	Minimum Base Image	I/O Enhancement Support
10.2.x	9.1.0 to 9.1.6	5.0.0 and later	6.4.1 to 6.4.7	• 6.5 • 6.7	vmx-10	**PA-VM-NSX-9.1.0.zip**	LRO
• 9.1.x • 10.1.x	9.1.7 to latest 9.1.x	3.2.0 to latest 4.0.x	6.4.8 and later	• 6.5 • 6.7 • 7.0	vmx-10	**PA-VM-NSX-9.1.9.zip**	LRO
• 9.1.x • 10.1.x	9.1.0 to 9.1.6	3.2.0 to latest 4.0.x	6.4.1 to 6.4.7	• 6.5 • 6.7	vmx-10	**PA-VM-NSX-9.1.0.zip**	LRO

VM-Series for VMware NSX (Formerly NSX-T)

Palo Alto Networks approves the VMware NSX-T and Panorama combinations listed below. You can download base images from the Palo Alto Networks Support Portal.

For versions of PAN-OS certified by VMware, see the VMware Compatibility Guide.

VMware NSX 4.0.x Service Deployments for partner Service Virtual Machines (SVM) sometimes experience a known traffic redirect issue. Contact VMware NSX Technical Support for details.

Panorama Version Support	Panorama Plugin for NSX	VMware NSX-T Version Support	VMware Virtual Machine Hardware Version	PAN-OS Version Support (Minimum)	Latest Base Image
11.2.x	5.0.2 and later	3.2.x, 4.0.x, 4.1.x	vmx-15	PAN-OS 10.1.x (10.1.0) PAN-OS 10.2.x (10.2.4) PAN-OS 10.2.x (10.2.9) PAN-OS 11.0.x (11.0.0) PAN-OS 11.1.x (11.1.0) PAN-OS 11.2.x (11.2.0)	**PA-VM-NST-11.2.0.zip** **PA-VM-NST-11.1.0.zip** **PA-VM-NST-11.0.2.zip** **PA-VM-NST-10.2.9-h1-vmwaresigned.zip** **PA-VM-NST-10.2.4-vmwaresigned.zip** **PA-VM-NST-10.1.9-h1-vmwaresigned.zip**
11.1.x	5.0.2 and later	3.2.x, 4.0.x, 4.1.x, 4.2.x	vmx-15	PAN-OS 10.1.x (10.1.0) PAN-OS 10.2.x (10.2.4) PAN-OS 10.2.x (10.2.9) PAN-OS 11.0.x (11.0.0) PAN-OS 11.1.x (11.1.0)	**PA-VM-NST-11.1.0.zip** **PA-VM-NST-11.0.2.zip** **PA-VM-NST-10.2.9-h1-vmwaresigned.zip** **PA-VM-NST-10.2.4-vmwaresigned.zip** **PA-VM-NST-10.1.9-h1-vmwaresigned.zip**
11.0.x	5.0.1 and later	3.2.x, 4.0.x,	vmx-15	PAN-OS 10.1.x (10.1.0)	**PA-VM-NST-11.0.2.zip**

Panorama Version Support	Panorama Plugin for NSX	VMware NSX-T Version Support	VMware Virtual Machine Hardware Version	PAN-OS Version Support (Minimum)	Latest Base Image
		4.1.x, 4.2.x		PAN-OS 10.2.x (10.2.4) PAN-OS 10.2.x (10.2.9) PAN-OS 11.0.x (11.0.0)	**PA-VM-NST-10.2.9-h1-vmwaresigned.zip** **PA-VM-NST-10.2.4-vmwaresigned.zip** **PA-VM-NST-10.1.9-h1-vmwaresigned.zip**
10.2.x	5.0.0 and later *NSX 4.1.x with PAN-OS 10.2 requires NSX plugin 5.0.1 or later.*	3.2.x, 4.0.x, 4.1.x, 4.2.x	vmx-10	PAN-OS 10.1.x (10.1.0) PAN-OS 10.2.x (10.2.4) PAN-OS 10.2.x (10.2.9)	**PA-VM-NST-10.2.9-h1-vmwaresigned.zip** **PA-VM-NST-10.2.4-vmwaresigned.zip** **PA-VM-NST-10.1.9-h1-vmwaresigned.zip**
10.1.x	3.2.0 to 4.0.x	2.5.x, 3.0.x, 3.1.x, 3.2.x	vmx-10	PAN-OS 10.1.x (10.1.0)	**PA-VM-NST-10.1.9-h1-vmwaresigned.zip** **PA-VM-NST-9.1.9-vmwaresigned.zip**
	4.0.x	4.0.x	vmx-10	PAN-OS 10.1.x (10.1.9-h1)	**PA-VM-NST-10.1.9-h1-vmwaresigned.zip**
9.1.x	3.2.0 to 4.0.x	2.5.x, 3.0.x, 3.1.x	vmx-10	PAN-OS 9.1.x (9.1.0)	**PA-VM-NST-9.1.9.zip**

VM-Series for KVM

You can download base images from the Palo Alto Networks Support Portal.

PAN-OS Version Support (Minimum)	VM-Series for KVM Version Support (Minimum)	I/O Enhancement Support	PAN-OS for VM-Series KVM Base Images
PAN-OS 11.1.4 (11.1.4)	Oracle Linux 8.10	DPDK Virtio	**PA-VM-KVM-11.1.4-h7.qcow2**
PAN-OS 11.2.5 (11.2.5 and later)	RHEL 9.5	DPDK with SR-IOV	**PA-VM-KVM-11.2.5.qcow2**
PAN-OS 11.1.6 (11.1.6) and later PAN-OS 10.2.x (10.2.5) PAN-OS 10.1.x (10.1.11)	RHEL 9.4 RHEL 9.2	• DPDK with SR-IOV • DPDK with Virtio	**PA-VM-KVM-11.1.6.qcow2** **PA-VM-KVM-10.2.5-h1.qcow2** **PA-VM-KVM-10.1.11-h1.qcow2**
PAN-OS 11.1.x (11.1.0)	Ubuntu 20.04	• DPDK with SR-IOV • DPDK with Virtio	**PA-VM-KVM-11.1.0.qcow2 for ARM** **PA-VM-KVM-11.1.x.qcow2 for x86**
PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0)	Ubuntu 22.04	• DPDK with SR-IOV • DPDK with Virtio	**PA-VM-KVM-10.2.x.qcow2** **PA-VM-KVM-11.0.0.qcow2**
PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0)	CentOS/Red Hat Enterprise Linux 9.1.x (9.1.x)	• DPDK with SR-IOV • DPDK with Virtio	**PA-VM-KVM-10.2.x.qcow2** **PA-VM-KVM-11.0.0.qcow2**
PAN-OS 10.1.x (10.1.0) PAN-OS 10.2.x (10.2.0)	CentOS/Red Hat Enterprise Linux: • 7.x.x (7.6.x) • 8.x.x (8.0.x)	• DPDK with SR-IOV • DPDK with Virtio	**PA-VM-KVM-10.1.x.qcow2** **PA-VM-KVM-10.2.x.qcow2**

PAN-OS Version Support (Minimum)	VM-Series for KVM Version Support (Minimum)	I/O Enhancement Support	PAN-OS for VM-Series KVM Base Images
PAN-OS 11.0.x (11.0.0)	• 9.0.x (9.0.x)		**PA-VM-KVM-11.0.0.qcow2**
PAN-OS 10.1.x (10.1.0)	Ubuntu 20.04	• DPDK with SR-IOV • DPDK with Virtio	**PA-VM-KVM-10.1.x.qcow2**
PAN-OS 10.1.x (10.1.0)	SUSE Enterprise Server 15 with QEMU 3.1.1	• MacVTap • Virtio	**PA-VM-KVM-10.1.x.qcow2**
PAN-OS 9.1.x (9.1.0) PAN-OS 10.1.x (10.1.0)	Ubuntu 18.04	• DPDK with SR-IOV • DPDK with Virtio	**PA-VM-KVM-9.1.x.qcow2** **PA-VM-KVM-10.1.x.qcow2**
PAN-OS 9.1.x (9.1.0)	CentOS/Red Hat Enterprise Linux: • 7.x.x (7.6.x) • 8.x.x (8.0.x)	• DPDK with SR-IOV • DPDK with Virtio	**PA-VM-KVM-9.1.x.qcow2**

VM-Series for Nutanix

You can download base images from the Palo Alto Networks Support Portal.

The VM-Series firewall for Nutanix uses the VM-Series firewall for KVM base image (qcow2).

PAN-OS Version Support (Minimum)	VM-Series for Nutanix Version Support (Minimum)	I/O Enhancement Support	VM-Series for KVM Base Image
PAN-OS 11.2.x (11.2.0) PAN-OS 11.1.x (11.1.0)	Nutanix AOS Version 7.0 Nutanix AHV v10.0	DPDK supported	**PA-VM-KVM-11.2.x.qcow2** **PA-VM-KVM-11.1.x.qcow2**
PAN-OS 10.1.x (10.1.0) PAN-OS 10.2.x (10.2.0)	Nutanix AOS Version 5.20	DPDK supported	**PA-VM-KVM-10.1.x.qcow2** **PA-VM-KVM-10.2.x.qcow2**

PAN-OS Version Support (Minimum)	VM-Series for Nutanix Version Support (Minimum)	I/O Enhancement Support	VM-Series for KVM Base Image
Layer 3 deployments, and virtual wire deployments with Service Chaining.	Nutanix AHV Release 20201105.2030		
PAN-OS 10.1.x (10.1.0) Layer 3 deployments, and virtual wire deployments with Service Chaining.	Nutanix AOS 6.5 version 6.0.5 in VPC mode	L3 mode only	**PA-VM-KVM-10.1.x.qcow2**
PAN-OS 9.1.x (9.1.0) PAN-OS 10.1.x (10.1.0) Layer 3 deployments, and virtual wire deployments with Service Chaining.	Nutanix AOS Version 5.10, 5.15 Nutanix AHV Release 20170830.185	DPDK supported	**PA-VM-KVM-9.1.0.qcow2** **PA-VM-KVM-10.1.x.qcow2**

VM-Series for Hyper-V

You can download base images from the Palo Alto Networks Support Portal.

PAN-OS Version Support (Minimum)	VM-Series for Hyper-V Version Support (Minimum)	I/O Enhancement Support	Base Image
PAN-OS 11.2.x (11.2.3)	Windows Server 2025 with Hyper-V role or Hyper-V 2025	• DPDK with SR-IOV supported • Packet MMAP with Virtio supported • Packet MMAP with SR-IOV supported	**PA-VM HPV-11.2.3.vhdx**

PAN-OS Version Support (Minimum)	VM-Series for Hyper-V Version Support (Minimum)	I/O Enhancement Support	Base Image
PAN-OS 11.2.x (11.2.0)	Windows Server 2022 with Hyper-V role or Hyper-V 2022	• DPDK with SR-IOV supported • Packet MMAP with Virtio supported • Packet MMAP with SR-IOV supported	**PA-VM HPV-11.2.0.vhdx**
PAN-OS 10.1.x (10.1.0) PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0)	• Windows Server 2012 R2 with Hyper-V role or Hyper-V 2012 R2 • Windows Server 2016 with Hyper-V role or Hyper-V 2016 • Windows Server 2019 with Hyper-V role or Hyper-V 2019	• DPDK with SR-IOV supported • Packet MMAP with Virtio supported • Packet MMAP with SR-IOV supported	**PA-VM-HPV-10.1.0.vhdx** **PA-VM-HPV-10.2.0.vhdx** **PA-VM-HPV-11.0.0.vhdx**
PAN-OS 9.1.x (9.1.0)	• Windows Server 2012 R2 with Hyper-V role or Hyper-V 2012 R2 • Windows Server 2016 with Hyper-V role or Hyper-V 2016 • Windows Server 2019 with Hyper-V role or Hyper-V 2019	• Packet MMAP supported • DPDK not supported	**PA-VM-HPV-9.1.0.vhdx**

VM-Series for OpenStack

You can download base images from the Palo Alto Networks Support Portal.

PAN-OS Version Support (Minimum)	VM-Series for OpenStack Version Support (Minimum)	I/O Enhancement Support	Base Image
PAN-OS 11.2.x (11.2.0) PAN-OS 11.1.x (11.1.4)	Redhat OpenStack 17.1	DPDK with Virtio Packet MMAP with Virtio	**PA-VM-KVM-11.2.0-h9.qcow2** **PA-VM-KVM-11.1.4-h13.qcow2**

PAN-OS Version Support (Minimum)	VM-Series for OpenStack Version Support (Minimum)	I/O Enhancement Support	Base Image
PAN-OS 10.2.x (10.2.10)			**PA-VM-KVM-10.2.10-h9.qcow2**
PAN-OS 10.1.x (10.1.3)	Redhat OpenStack Train 16	• DPDK with Virtio • DPDK with SR-IOV • Packet MMAP with Virtio • Packet MMAP with SR-IOV	**PA-VM-KVM-10.1.3.qcow2**
PAN-OS 9.1.x (9.1.5) PAN-OS 10.1.x (10.1.0)	Redhat OpenStack Queens 13	• DPDK with Virtio • DPDK with SR-IOV • Packet MMAP with Virtio • Packet MMAP with SR-IOV	**PA-VM-KVM-9.1.5.qcow2** **PA-VM-KVM-10.1.0.qcow2**

Cisco ACI: Hardware and VM-Series Firewalls in Cisco ACI

Review the Cisco ACI plugins information for supported PAN-OS, Panorama, and Cisco ACI plugin versions.

You can download base images from the Palo Alto Networks Support Portal.

Public Cloud Deployments

Palo Alto Networks supports the following public cloud deployments:

- Public Cloud Deployments Available from a Marketplace—AWS, Azure, GCP, Oracle, IBM, and Tencent Cloud China
- Public Cloud Deployments Requiring a Base Image—Alibaba, Oracle, vCloud Air
- VM-Series Firewall for VMware Cloud on AWS

Public Cloud Deployments Available from a Marketplace—AWS, Azure, GCP, Oracle, IBM, and Tencent Cloud China

Public Cloud Deployment	PAN-OS Version Support (Minimum)	I/O Enhancement Support
VM-Series on AWS List of supported AWS Regions. Support for AWS Outposts on PAN-OS 9.1 and later.	PAN-OS 9.1.x (9.1.0) PAN-OS 10.1.x (10.1.0) PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0) PAN-OS 11.1.x (11.1.0)	In PAN-OS 11.1.x (11.1.0) and later, ARM support is available on **AWS Graviton 3** and **AWS Graviton 2** instances.
VM-Series on Azure List of supported Azure Regions.	PAN-OS 9.1.x (9.1.0) PAN-OS 10.1.x (10.1.0) PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0) **Azure Stack Edge:** PAN-OS 10.1.x (10.1.5)	DPDK is supported in PAN-OS 9.1 and later PAN-OS releases.
VM-Series on Google Cloud List of supported Google Cloud Regions	PAN-OS 9.1.x (9.1.0) PAN-OS 10.1.x (10.1.0) PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0)	DPDK is supported and enabled by default.
VM-Series on Oracle Cloud Infrastructure	PAN-OS 9.1.x (9.1.0) PAN-OS 10.1.x (10.1.0) PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0) PAN-OS 11.2.x (11.2.0)	• DPDK is supported and enabled by default. • SR-IOV and MMAP mode is supported with jumbo and non-jumbo frames on PAN-OS 9.1.x and PAN-OS 10.1.x and later with VM-Series plugin 2.1.0 and later. • VM.STANDARD.E4.FLEX (AMD) instance type is supported on PAN-OS 11.2.0 (11.2.0 and above).
VM-Series on Oracle Cloud Infrastructure	**Oracle Gov Cloud:** PAN-OS 9.1.x (9.1.3) PAN-OS 10.1.x (10.1.2)	• DPDK is supported and enabled by default. • SR-IOV and MMAP mode is supported with jumbo and non-

Public Cloud Deployment	PAN-OS Version Support (Minimum)	I/O Enhancement Support
	PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0)	jumbo frames on PAN-OS 9.1.x and PAN-OS 10.1.x and later with VM-Series plugin 2.1.0 and later.
VM-Series on IBM Cloud	PAN-OS 10.1.x (10.1.0)	—
VM-Series on Tencent Cloud China	PAN-OS 10.2.10(10.2.10)	—

Further I/O Enhancement support is detailed in PacketMMAP and DPDK Drivers on VM-Series Firewalls.

To view the hypervisor support for Panorama versions, see Panorama Hypervisor Support. To view the Panorama plugin requirements for public clouds, see Public Cloud-AWS, Azure, GCP.

Public Cloud Deployments Requiring a Base Image—Alibaba, Oracle, vCloud Air

The following Public Clouds require a PAN-OS for VM-Series base image from the Palo Alto Networks Support Portal.

Public Cloud Deployment	PAN-OS Version Support (Minimum)	I/O Enhancement Support	Base Image
VM-Series on Alibaba Cloud	PAN-OS 9.1.x (9.1.0)	DPDK and Packet MMAP are supported. DPDK is enabled by default.	**PA-VM-KVM-9.1.0.qcow2**

Further I/O Enhancement support is detailed in the list of PacketMMAP and DPDK Drivers on VM-Series Firewalls.

VM-Series Firewall for VMware Cloud on AWS

You can deploy the VM-Series firewall on VMware Cloud on AWS. Set Up a VM-Series Firewall on an ESXi Server to deploy the VM-Series firewall. Review also the supported VMware ESXi versions for the VM-Series for VMware vSphere Hypervisor (ESXi).

VMware Cloud on AWS does not support the VM-Series firewall on VMware NSX-V or NSX-T.

PAN-OS Version Support	I/0 Enhancement Support	Documentation
PAN-OS 9.1.x (9.1.0)	DPDK and SR-IOV	• VMware Cloud on AWS Documentation

PAN-OS Version Support	I/O Enhancement Support	Documentation
		• VM-Series Firewall on VMware ESXi

PacketMMAP and DPDK Drivers on VM-Series Firewalls

The VM-Series firewall supports the PacketMMAP and Data Plane Development Kit (DPDK) drivers listed in the tables below. VM-Series firewalls use their own drivers to communicate with the drivers on the host. You should install host-driver versions that are equal to or later than the driver versions on your VM-Series firewall.

To choose host drivers for SR-IOV:

- **KVM**—On your KVM host, install a physical function (PF) driver version that is equal to or later than the virtual function (VF) native driver version listed below.
- **ESXi**—Refer to the VMware Compatibility Matrix and install the latest driver for the firmware version (PF=i40e, VF=i40evf).

For more information about communication between VF drivers on the VM-Series firewall and PF drivers on the host (the hypervisor), review the list of PacketMMAP and DPDK Drivers on VM-Series Firewalls in the VM-Series Deployment Guide.

- SR-IOV Access Mode
- PacketMMAP Driver Versions
- DPDK Driver Versions

SR-IOV Access Mode

VM-Series firewalls support SR-IOV Access Mode on KVM and ESXi hypervisors. To enable single root I/O virtualization (SR-IOV) access mode, you can include the bootstrap parameter file: `plugin-op-commands=sriov-access-mode-on` in the `initcfg.txt`

- **KVM**—Requires PAN-OS 9.1.5 or a later PAN-OS version with VM-Series plugin 2.0.1 or a later plugin version.
- **ESXi**—Requires PAN-OS 9.1.5 or a later PAN-OS 9.1 version or PAN-OS 10.1 or a later PAN-OS version with VM-Series plugin 2.0.5 or a later plugin version.

PacketMMAP Driver Versions

VM-Series firewalls use their virtual function (VF) drivers to communicate with the host's physical function (PF) drivers during SR-IOV. For example, i40e is a PF driver and i40evf is a VF driver.

PAN-OS Version	Driver Filename	ARM Driver Filename	Virtual Firewall Native Drivers (Linux Version)	Comment
11.2	bnx2x	mlx5	1.713.36-0	
	i40e	i40e	2.14.13	
	iavf		4.0.2	

PAN-OS Version	Driver Filename	ARM Driver Filename	Virtual Firewall Native Drivers (Linux Version)	Comment
	igb		5.6.0	
	igbvf		2.4.0	
	ixgbe		5.1.0	The minimum version for multiple queues is 4.2.5
	ixgbevf		4.1.0	
	mlnx-en		4.9	
11.1	bnx2x	mlx5	1.713.36-0	
	i40e	i40e	2.14.13	
	iavf		4.0.2	
	igb		5.6.0	
	igbvf		2.4.0	
	ixgbe		5.1.0	The minimum version for multiple queues is 4.2.5
	ixgbevf		4.1.0	
	mlnx-en		4.9	
11.0	bnx2x		1.713.36-0	
	i40e		2.14.13	
	iavf		4.0.2	
	igb		5.6.0	
	igbvf		2.4.0	
	ixgbe		5.1.0	The minimum version for multiple queues is 4.2.5
	ixgbevf		4.1.0	
	mlnx-en		4.9	
10.2	bnx2x		1.712.30-0	

PAN-OS Version	Driver Filename	ARM Driver Filename	Virtual Firewall Native Drivers (Linux Version)	Comment
	i40e		2.13.10	
	iavf		3.2.3	i40evf renamed to iavf; still compatible with i40en host driver.
	igb		5.4.0	
	igbvf		2.4.0	
	ixgbe		5.1.0	The minimum version for multiple queues is 4.2.5
	ixgbevf		4.1.0	
	mlnx-en		4.9	
10.1	bnx2x		1.712.30-0	
	i40e		2.13.10	
	iavf		3.2.3	i40evf renamed to iavf; still compatible with i40en host driver.
	igb		5.4.0	
	igbvf		2.4.0	
	ixgbe		5.1.0	The minimum version for multiple queues is 4.2.5
	ixgbevf		4.1.0	
	mlnx-en		4.9	
9.1	bnx2x		1.713.36-0	
	i40e		2.3.2	
	i40evf		3.2.2	Compatible with i40en host driver.
	igb		5.4.0	
	igbvf		2.4.0	

PAN-OS Version	Driver Filename	ARM Driver Filename	Virtual Firewall Native Drivers (Linux Version)	Comment
	ixgbe		5.1.0	The minimum version for multiple queues is 4.2.5
	ixgbevf		4.1.0	

DPDK Driver Versions

When the firewall is in DPDK mode, it uses DPDK drivers. Please check the official DPDK release notes for more information.

By default DPDK is enabled on VM-Series firewalls as stated below. If the VM-Series firewall detects an unsupported driver, the firewall reverts to PacketMMap mode.

Hypervisor	Virtual Driver	NIC Drivers
KVM	virtio	ixgbe, ixgbevf, i40e, i40evf, and mlnx-en (PAN-OS 10.1 and later)
ESXi	VMXNET3	ixgbe, ixgbevf, i40e, i40evf
ARM KVM	virtio	I40e and mlx5 (PAN_OS 11.1 and later)

See VM-Series for KVM and VM-Series for VMWare vSphere Hypervisor (ESXi) for PAN-OS versions that support DPDK, DPDK with SR-IOV, or DPDK with Virtio.

PAN-OS Version	DPDK Version	Comment
12.1	23.11.0	
11.2	22.11.1	
11.1	22.11.1	
11.0	20.11.1	
10.2	20.11.1	
10.1	19.11.3	
9.1	18.11	

Partner Interoperability for VM-Series Firewalls

Palo Alto Networks offers two tiers of support for third-party partner platforms for the VM-Series next-generation firewall: Palo Alto Networks Certified and Partner-Qualified. The VM-Series firewall provides the same security features and functionality regardless of support tier but the types of issues that we can help you resolve are different for each.

- **Partner Qualified**—Palo Alto Networks customer support helps you with any issue related directly to VM-Series firewalls. A VM-Series firewall issue is defined as an issue that occurs after a packet enters the firewall. This level of support does not include issues related to a partner platform.

  VM-Series issues include:

  - An issue with your PAN-OS configuration
  - An issue with VM-Series upgrades
  - An issue with VM-Series licensing
  - An issue with VM-Series documentation
- **Palo Alto Networks Certified**—Palo Alto Networks customer support helps you with all VM-Series firewall issues as well as any issues related to an approved partner platform. A platform issue is defined as an issue that involves a packet that is outside of the VM-Series firewall, such as before it arrives at or after it leaves the firewall or hypervisor. Palo Alto Networks Certified support also includes support for your hardware configuration.

  Partner platform issues include:

  - A network interface that is not recognized by the VM-Series firewall
  - The VM-Series firewall is not booting
  - A platform configuration issue
  - An issue with bootstrapping the VM-Series firewall
  - An issue that prevents the connection to other networking devices
  - Issues related to high availability (HA) functionality
  - I/O Acceleration (DPDK, SR-IOV, and PCI passthrough)

For a complete list of the partner platforms supported in each tier, review the integration information:

- Palo Alto Networks Certified Integrations
- Partner-Qualified Integrations

Palo Alto Networks Certified Integrations

Review these lists to see the Palo Alto Networks certified partner products with which VM-Series firewalls can interoperate. The tables include details about hardware platforms and software versions on which you can deploy a VM-Series firewall.

*The partner software version and the PAN-OS® version columns display the range of versions and the minimum version in parentheses. For example, if the PAN-OS Version column displays **PAN-OS 10.1.x (10.1.4)**, then integration support begins with PAN-OS 10.1 but not until PAN-OS 10.1.4. and later PAN-OS versions.*

- Ciena
- Cisco Cloud Services Platform
- Cisco Enterprise Computer System (ENCS)
- Citrix SD-WAN
- Juniper NFX Network Services Platform
- NSX SD-WAN by VeloCloud
- Nuage Networks
- Versa Networks
- Vyatta

Ciena

The following table shows the Ciena products with which VM-Series firewalls interoperate.

Hardware	Hypervi	SAOS Supported Software Version (Minimum)	SAOS Tested Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
3906mvi and 3926mvi	KVM	18.x.x (18.06.00)	18.06.x (18.06.00)	9.1.x (9.1.0)	Layer 3 mode on the VM-50, VM-100, and VM-300 VirtIO and DPDK mode.	Ciena documentation

Cisco Cloud Services Platform

The following table shows the Cisco Cloud Services Platform (CSP) products with which VM-Series firewalls interoperate.

Hardware	Hypervi	CSP Supported Software Version (Minimum)	CSP Tested Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
CSP 5228	Megaport (KVM)	2.6.x (2.6.1)	2.6.x (2.6.1)	10.2.x (10.2.0)	Layer 3 VM-Series Firewalls in an HA configuration SR-IOV, Packet MMAP, and DPDK mode	Set Up the VM-Series Firewall on Cisco CSP (PAN-OS 10.2) Megaport Documentation
CSP 5200 Series	KVM	2.6.x (2.6.1)	2.6.x (2.6.1)	10.2.x (10.2.0)	Layer 2, Layer3, Virtual wire deployments on all VM-Series models except VM-50 VM-Series Firewalls in an HA configuration SR-IOV, Packet MMAP, and DPDK mode	Set Up the VM-Series Firewall on Cisco CSP (PAN-OS 10.2)
CSP 5400 Series		4.6.x (4.6)	4.6.x (4.6.1-FC1)	10.1.x (10.1.0)		Set Up the VM-Series Firewall on Cisco CSP (PAN-OS 10.1)
CSP 5400 Series CSP 2100 Series		2.x.x (2.4.0)	2.4.x (2.4.0)	9.1.x (9.1.0)		Set Up the VM-Series Firewall on Cisco CSP (PAN-OS 9.1)

Cisco Enterprise Computer System (ENCS)

The following table shows the Cisco Enterprise Computer System (ENCS) products with which VM-Series firewalls interoperate.

Hardware	Hypervi	NFVIS Supported Software Version (Minimum)	Tested NFVIS Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
Cisco 5400 Series	KVM	4.12.x (4.12)	4.12.x (4.12)	11.1.x (11.1.0)	• Layer 2, Layer3, Virtual wire deployments • Firewalls in HA • Virtio with DPDK mode enabled by default	VM-Series on Cisco ENCS
		4.12.x (4.12)	4.12.x (4.12)	10.2.x (10.2.0)		
		4.6.x (4.6)	4.6.x (4.6.1-FC1)	10.1.x (10.1.0)		
		3.x.x (3.8) 4.6.x (4.6.1-FC1)	3.10.x (3.10.1) 3.12.x (3.12.1) 4.6.x (4.6.1-FC1)	9.1.x (9.1.0)		

For PAN-OS 11.1.x, you must use the NFVIS CLI to upload the PAN-OS image. The PAN-OS file size exceeds the file size limit of the ENCS UI.

Citrix SD-WAN

The following table shows the Citrix SD-WAN products with which VM-Series firewalls interoperate.

Hardware	Hypervi	Supported Software Version (Minimum)	Tested Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
Citrix SD-WAN 1100 Appliance	KVM	11.x.x (11.0.1)	11.0.x (11.0.1)	9.1.x (9.1.0)	Virtual wire deployments VirtIO with packet MMAP mode support only; so you must disable DPDK with **op-**	• Citrix SD-WAN Deployment Guide • Citrix SD-WAN Solution Brief

Hardware	Hypervi	Supported Software Version (Minimum)	Tested Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
					`cmd-dpdk-pkt-io=off` in the `init-cfg.txt` file used for bootstrapping or use the CLI command **`set system setting dpdk-pkt-io off`**	
				9.1.x (9.1.0)	Virtual wire DPDK Mode	

Juniper NFX Network Services Platform

The following table shows the Juniper NFX Network Services Platform products with which VM-Series firewalls interoperate.

Hardware	Hypervi	Junos Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
NFX 250	KVM	15.1X53-D470.x (15.1X53-D470.5)	9.1.x (9.1.0)	Layer 2, Layer 3, Virtual Wire DPDK mode	Juniper NFX documentation

NSX SD-WAN by VeloCloud

The following table shows the NSX SD-WAN by VeloCloud products with which VM-Series firewalls interoperate.

Hardware	Hypervi	VCE Supported Software Version (Minimum)	Tested VCE Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
Edge 520v Edge 840	KVM	3.x.x (3.2.0)	3.3.x (3.3.1)	9.1.x (9.1.0)	Virtual wire deployments DPDK	NSX SD-WAN by VeloCloud documentation

Nuage Networks

The following table shows the Nuage Networks products with which VM-Series firewalls interoperate.

Hardware	Hypervi	VSP Supported Software Version (Minimum)	Tested VSP Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
Nuage NSG-X series	—	5.x.x (5.3.3U3)	5.3.x (5.3.3U3)	TBD	Virtual wire deployments on VM-50 and VM-100 models VirtIO with packet MMAP mode support only DPDK must be disabled: If you bootstrap, include **`op-cmd-dpdk-pkt-io=off`** in the `init-cfg.txt` file, or, on the VM Series firewall, use the CLI command **`set system setting dpdk-pkt-io off`**	Nuage Networks documentation

Versa Networks

The following table shows the Versa Networks products with which VM-Series firewalls interoperate.

Hardware	Hypervi	Supported Versa FlexVNF Software Version (Minimum)	Tested Versa FlexVNF Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
Versa 930 (Dell VEP4600)	KVM	21.x.x (21.1.2)	21.1.x (21.1.2)	9.1.x (9.1.0)	Virtual wire, L3 deployments with DPDK	Versa Documentation

Vyatta

The following table shows the Vyatta products with which VM-Series firewalls interoperate.

Platform	Hypervi	Vyatta Software Version	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
AT&T vRouter 5600	KVM	19.x (1903f)	9.1.x (9.1.0)	Virtual wire, L2, L3 deployments with DPDK VM-50, VM-100, and VM-300	—

Partner-Qualified Integrations

Review these lists of partner-qualified products with which VM-Series firewalls interoperate. The tables include details about hardware platforms and software versions on which you can deploy VM-Series firewalls.

*The partner software version and PAN-OS® version columns display the range of versions and the minimum version in parentheses. For example, if the PAN-OS Version column displays **PAN-OS 10.1.x (10.1.4)**, then integration support begins with PAN-OS 10.1 but not until PAN-OS 10.1.4. and later PAN-OS versions.*

- ADVA
- Aryaka
- Corsa

- iS5Com
- Megaport
- SEL
- Siemens
- Stratus
- ZPE
- Zededa

ADVA

The following table shows the ADVA products with which VM-Series firewalls interoperate.

Hardware	Supported ADVA Ensemble Connector Version	PAN-OS Version	I/O Acceleration	Documentation
FSP 150-XG304u	19.1.1.33	10.1.x (10.1.0)	DPDK mode with SR-IOV	ADVA Documentation

Aryaka

The following table shows the Aryaka products with which VM-Series firewalls interoperate.

Hardware	Supported Aryaka Software Versions	PAN-OS Version	I/O Acceleration	Documentation
2600 3000 10000	• 5.0.0 • 5.2.0	• 10.2.x (10.2.0) • 11.0.x (11.0.0) • 11.1.x (11.1.0)	• DPDK and Virtio • Virtio and Packet MMAP mode	Aryaka Documentation

Corsa

The following table shows the Corsa products with which VM-Series firewalls interoperate.

Hardware	Supported Software Version	PAN-OS Version	I/O Acceleration	Documentation
Corsa Security Platform	2.x.x	10.1.x (10.1.4)	SR-IOV with Packet MMAP	Corsa Documentation

Hardware	Supported Software Version	PAN-OS Version	I/O Acceleration	Documentation
	1.x.x	9.1.x (9.1.0)	SR-IOV with Packet MMAP	

iS5Com

The following table shows the iS5Com products with which VM-Series firewalls interoperate.

Hardware	Supported Software Version	PAN-OS Version	Mode	I/O Acceleration	Documentation
iS5Com iROC Can be equipped in RAPTOR or MicroRAPTOR Series Platforms	ESX 7.0 Update 3	11.0.x (11.0.2)	L2, L3	PCI Passthrough (disabled by default)	iS5Com Documentation

Megaport

The following table shows the Megaport products with which VM-Series firewalls interoperate.

Hardware	Hypervisor	Mode	PAN-OS Version	I/O Acceleration	Documentation
Megaport Virtual Edge • 2vCPU/8GB • 4vCPU/16GB • 8vCPU/32GB • 12vCPU/48GB	KVM	MVE provides Virtual Cross Connect (VXC) private network paths provisioned as a layer-2 802.1q VLANs.	10.2.x (10.2.0)	SR-IOV	Megaport Documentation

SEL

The following table shows the SEL products with which VM-Series firewalls interoperate.

Hardware	Supported Software Version	PAN-OS Version	I/O Acceleration	Documentation
SEL-3350	AlmaLinux 8.6 RHEL 8.5	10.2.x (10.2.0)	None	SEL Documentation
SEL-3355	AlmaLinux 8.6 RHEL 8.5	10.2.x (10.2.0)	SR-IOV supported on SEL-3355 onboard ports	

Siemens

The following table shows the Siemens products with which VM-Series firewalls interoperate.

Hardware	Supported Software Version	PAN-OS Version	I/O Acceleration	Documentation
RUGGEDCOM APE 1808	Ubuntu 20.04 KVM	11.1.x (11.1.0) 10.1.x (10.1.0) 9.1.x (9.1.4)	L3 mode Virtio with DPDK	Siemens Support Siemens Technology Partners RUGGEDCOM ROX II v.2.14 CLI Configuration Manual RUGGEDCOM ROX II v.2.14 WebUI Configuration Manual RUGGEDCOM APE1808 Configuration Manual

Stratus

The following table shows the Stratus products with which VM-Series firewalls interoperate.

Hardware	Hypervisor	Supported Software Version	PAN-OS Version	I/O Acceleratio	Documentatio
ztC Edge 250i(ft)	KVM	Stratus Redundant Linux 2.3.3 and 3.0	11.0.x 10.2.x	—	Stratus ztC Edge 250i(ft) Documentation

Hardware	Hypervisor	Supported Software Version	PAN-OS Version	I/O Acceleration	Documentation
		Contact Stratus support to use version 2.3.3 with PAN-OS.			

ZPE

The following table shows the ZPE products with which VM-Series firewalls interoperate.

Hardware	Supported Nodegrid Software Version	PAN-OS Version	I/O Acceleration	Documentation
Gate SR NSR	4.1.x	9.1.x (9.1.0)	Virtio with DPDK	ZPE Documentation

Zededa

The following table shows the Zededa products with which VM-Series firewalls interoperate.

Bootstrapping is not supported for the VM-Series firewall deployed on Zededa.

EVE Version	PAN-OS Version	Mode	I/O Acceleration	Documentation
8.5.4	11.0.x 11.0.0	L3 Mode only IPv4 only	VirtIO	Zededa Documentation

VM-Series Plugin

The VM-Series plugin is built in to the VM-Series firewalls. You can configure this plugin directly on the VM-Series firewall or install it on a Panorama™ M-Series or virtual appliance.

To manage the VM-Series plugin configuration on your managed firewalls from Panorama, you must manually install the VM-Series plugin on Panorama. Refer to Panorama Plugins. You can also compare VM-Series Plugin and Panorama Plugins.

The following table briefly describes the features introduced in each version of the VM-Series plugin. For additional information about each version, refer to the VM-Series plugin release notes.

VM-Series Plugin 5.1.x

VM-Series plugin 5.1 versions are compatible with PAN-OS 11.1 releases. The following table describes new features or changes introduced in each plugin version and the VM-Series PAN-OS base image that includes each version of the plugin.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
5.1.9	11.2.8	Includes new fixes to improve your experience with the VM-Series firewall.
5.1.7	11.2.6	Includes new fixes to improve your experience with the VM-Series firewall.
5.1.6	11.2.5	Includes new fixes to improve your experience with the VM-Series firewall.
5.1.4	11.1.5	Includes new fixes to improve your experience with the VM-Series firewall.
5.1.3	—	Includes new fixes to improve your experience with the VM-Series firewall.
5.1.1	11.2.0	Includes new fixes to improve your experience with the VM-Series firewall.
5.1.0	11.2.0	Introduces reduced maximum session count on the VM-Series firewall. *This is the minimum required plugin version for the VM-Series on PAN-OS 11.2.0.*

VM-Series Plugin 5.0.x

VM-Series plugin 5.0 versions are compatible with PAN-OS 11.1 releases. The following table describes new features or changes introduced in each plugin version and the VM-Series PAN-OS base image that includes each version of the plugin.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
5.0.7		Includes fix to a known issue.
5.0.6		Includes fixes to known issues.
5.0.2	—	Introduces changes in the maximum session count on the VM-Series firewall and fixes to internally identified issues.
5.0.1	—	Introduces reduced maximum session count on the VM-Series firewall.
5.0.0	11.1.0	Includes fixes to known issues.

VM-Series Plugin 4.0.x

VM-Series plugin 4.0 versions are compatible with PAN-OS 11.0 releases. The following table describes new features or changes introduced in each plugin version and the VM-Series PAN-OS base image that includes each version of the plugin.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
4.0.8	11.0.5	Includes fixes to known issues.
4.0.7	—	Includes fixes to known issues.
4.0.5	—	Introduces improvements to Google Cloud Platform IPS, powered by Palo Alto Networks.
4.0.4	—	Introduces reduced maximum session count on the VM-Series firewall and improvements to Google Cloud Platform IPS, powered by Palo Alto Networks.
4.0.3-h1	—	Includes a fix to one issue.
4.0.3	—	Includes fixes to known issues.
4.0.2	11.0.2	Includes fixes to known issues.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
4.0.1	11.0.1	Includes fixes to known issues.
4.0.0	11.0.0	Introduces support for Advanced Routing on the VM-Series firewall.

VM-Series Plugin 3.0.x

VM-Series plugin 3.0 versions are compatible with PAN-OS 10.2 releases. The following table describes new features or changes introduced in each plugin version and the VM-Series PAN-OS base image that includes each version of the plugin.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
3.0.13	10.2.14	Addresses known issues.
3.0.12	10.2.14	Addresses known issues.
3.0.11	10.2.14	Addresses known issues.
3.0.10	10.2.13	Addresses known issues.
3.0.9	10.2.11	Addresses known issues.
3.0.8	10.2.10	Addresses known issues.
3.0.6	10.2.8	Addresses known issues.
3.0.5-h1	—	Introduces reduced maximum session count on the VM-Series firewall.
3.0.5	10.2.5	Addresses known issues.
3.0.4	10.2.4	Addresses known issues.
3.0.3	10.2.3	Addresses known issues and introduces two new features—Configuring OCI CloudWatch monitoring and Publishing custom metrics in the OCI console.
3.0.2	10.2.2	Addresses known issues.
3.0.1	10.2.1	Introduces one new feature—PAYG License Support for VM-Series on AWS, OCI, GCP and Azure.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
3.0.0	10.2.0	Addresses known issues.

VM-Series Plugin 2.1.x

VM-Series plugin 2.1 versions are compatible with PAN-OS 10.1 releases. The following table describes new features or changes introduced in each plugin version and the VM-Series PAN-OS base image that includes each version of the plugin.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
2.1.17	10.1.14	Introduces fixes for issues.
2.1.16	—	Introduces fixes for issues.
2.1.15	—	Introduces fixes for issues.
2.1.14	10.1.11	Introduces fixes for issues.
2.1.13	10.1.10	Introduces fixes for issues.
2.1.12	—	Introduces fixes for issues.
2.1.11	—	Introduces two new features—Full Bootstrap Support for the VM-Series on OCI and HA Support for the VM-Series on OCI in FIPS mode.
2.1.10	10.1.9-h1	Introduces fixes for issues.
2.1.9	10.1.9	Introduces fixes for issues.
2.1.8	—	Addresses known issues and introduces two new features—Configuring OCI CloudWatch monitoring and Publishing custom metrics in the OCI console.
2.1.7	10.1.7	Introduces fixes for issues.
2.1.6	10.1.6	Introduces fixes for issues.
2.1.5	10.1.5	Introduces fixes for issues.
2.1.4	10.1.4	Introduces one new feature—Limit the number of vCPUs licensed and used by a VM-Series firewall.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
2.1.3	10.1.3	Addresses a known issue.
2.1.2	10.1.2	Introduces two new features—Bootstrapping support for NUMA Performance Optimization and Azure Stack API Endpoint Access.
2.1.1	10.1.1	Introduces two new features—NUMA Performance Optimization and Six-Core Support for Intelligent Traffic Offload.
2.1.0	10.1.0	Default VM-Series plugin for PAN-OS 10.1.0.

VM-Series Plugin 2.0.x

VM-Series plugin 2.0 versions are compatible only with PAN-OS 9.1. The following table describes new features or changes introduced in each plugin version and the VM-Series PAN-OS base image that includes each version of the plugin.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
2.0.7	9.1.10 10.0.6*	Introduces management interface swap support for the VM-Series on VMware ESXi and KVM and addresses known issues.
2.0.6	9.1.9 10.0.5*	Addresses a known issue.
2.0.5	—	Addresses known issues and adds 1500 MTU for Google Cloud Platform and SR-IOV access mode on ESXi with PAN-OS 9.1.5 and later or 10.0.1 and later.
2.0.4	10.0.4*	Addresses known issues and adds licensing support for future PAN-OS releases.
2.0.3	10.0.3*	• Introduces custom image creation for the VM-Series firewall on Microsoft Azure. • Introduces Pay-As-You-Go license support for the VM-Series on Oracle Cloud Infrastructure. • Introduces enhancements for the VM-Series firewall on Alibaba Cloud. • Addresses known issues.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
2.0.2	9.1.6 9.1.7 9.1.8 10.0.2*	• Introduces shared storage on AWS, Azure and GCP. Supports subdirectories within cloud storage, enabling you to store multiple bootstrap files in one storage bucket. • Introduces support for secure bootstrap on AWS. • Change in default behavior: VM-Series plugin now uses HTTPS to communicate with the AWS CloudWatch endpoint. • Addresses known issues.
2.0.1	10.0.1*	• Introduces AWS active-passive high availability using a secondary IP address. • Change in default behavior: In new VM-Series deployments on AWS, the default Packet IO mode is DPDK. • Introduces bootstrapping with user data on AWS, Azure, and GCP. • Introduces bootstrapping VLAN access mode on SR-IOV for VM-Series firewall on KVM only. Requires PAN-OS 9.1.5 and later, or 10.0.1 and later. • Addresses known issues.
2.0.0	10.0.0*	Addresses known issues.

*PAN-OS 10.0 reached end-of-life (EoL) status on July 16, 2022.

VM-Series Plugin 1.0.x

VM-Series plugin 1.0 versions are compatible with PAN-OS 9.0 and PAN-OS 9.1 releases. The following table describes new features or changes introduced in each plugin versions and the VM-Series PAN-OS base image that includes each version of the plugin.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
1.0.13	9.0.14 9.0.13 9.0.12 9.0.11	Addresses known issues.
1.0.12	9.1.4	• Additional PAN-OS custom metrics for AWS, Azure, and GCP public clouds (panSessionConnectionsPerSecond,

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
	9.1.5	panSessionThroughputKbps, and panSessionThroughputPps). • New system startup updates, system health periodic updates, and live health failure updates for AWS CloudWatch. • Addresses known issues.
1.0.11	9.0.8 9.0.9 9.0.10 9.1.2 9.1.3	Introduces Deeper Visibility with AWS CloudWatch Enhancement and addresses known issues.
1.0.10	—	Addresses known issues on AWS.
1.0.9	—	Introduces support for Oracle Cloud Infrastructure marketplace deployment and high availability for the VM-Series firewall, and addresses known issues. PAN-OS 9.1.1 is required to use these OCI features.
1.0.8	9.1.0 9.1.1	Addresses known issues. Default VM-Series plugin version for PAN-OS 9.1.
1.0.7	—	Addresses known issues, including bug fixes and support for high availability (HA) on Azure Government for the VM-Series on Azure. Earliest version on which you can enable (HA) on Azure Government for the VM-Series on Azure.
1.0.6	—	Introduces support for the VM-Series firewall on NSX-T (North-South) and addresses known issues.
1.0.5	—	Introduces the PAN-OS accelerated feature releases (images with .xfr in the filename*) for only VM-Series firewalls to enable support for new features and bug fixes; also addresses known issues. PAN-OS 9.0.4 requires plugin 1.0.5 or later. *All PAN-OS 9.0-xfr releases are end-of-life (EoL) as of September 19, 2020.*

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
1.0.4	—	Addresses known issues.
1.0.3	—	Addresses known issues.  *If you want to enable management interface swap on GCP or AWS platforms and you are running PAN-OS 9.0.2, you must install VM-Series plugin 1.0.3 or later.*
1.0.2	—	Addresses known issues.
1.0.0	—	Enables publishing metrics for supported public clouds: AWS, Azure, and Google Cloud Platform. Default VM-Series plugin version for PAN-OS 9.0.

AWS Regions

The AWS regions—public, GovCloud, and AWS Outposts—in which you can deploy the VM-Series firewall from the AWS Marketplace.

AWS Regions	Region ID
US East (N. Virginia)	us-east-1
US East (Ohio)	us-east-2
US West (N.California)	us-west-1
US West (Oregon)	us-west-2
Asia Pacific (Hong Kong)	ap-east-1
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Jakarta)	ap-southeast-3
Asia Pacific (Melbourne)	ap-southeast-4
Asia Pacific (Malaysia)	ap-southeast-5
Asia Pacific (Tokyo)	ap-northeast-1
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Osaka) Available in BYOL as a Shared AMI. You can find the AMI for the VM-Series firewall on the EC2 console (**Instances** > **Launch Instance** > **Community AMIs**) using the AMI ID (ami-0d326a4c332ce4726) or by searching for **`Palo Alto Networks`**.	ap-northeast-3
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Hyderabad)	ap-south-2
Canada Central	ca-canada-1
Canada (Calgary)	ca-west-1

AWS Regions	Region ID
EU (Frankfurt)	eu-central-1
EU (Zurich)	eu-central-2
EU (Ireland)	eu-west-1
EU (London)	eu-west-2
EU (Paris)	eu-west-3
EU (Stockholm)	eu-north-1
EU (Milan)	eu-south-1
EU (Spain)	eu-south-2
Israel (Tel Aviv)	il-central-1
South America (Sao Paulo)	sa-east-1
Middle East (Bahrain)	me-south-1
Middle East (UAE)	me-central-1
Mexico	mx-central-1
Thailand	ap-southeast-7
Africa (Cape Town)	af-south-1
AWS Gov Cloud (US)	us-gov-west
	us-gov-east
AWS Outposts	On all regions listed above, where AWS Outposts is supported.

Azure Regions

The VM-Series firewall is available on the Azure public and the Azure Government Marketplace.

Locations	VM-Series Next-Generation Firewall Bundle 1*	VM-Series Next-Generation Firewall Bundle 2*	VM-Series Next-Generation Firewall (BYOL and ELA)**
All geographies (except China)	✓	✓	✓
Azure China	—	—	Only BYOL for PAN-OS 8.1
Azure Government (US)	✓	✓	✓
Azure Israel	✓	✓	✓
Azure DoD	✓	✓	✓

Refer to Azure geography for the list of regions.

Google Cloud Regions

You can deploy the VM-Series firewall with any supported PAN-OS® release in all Google Cloud Platform regions.

OCI Cloud Regions

You can deploy the VM-Series firewall with any supported PAN-OS® release in all Oracle Cloud Infrastructure public cloud regions and government cloud regions.

*VM-Series firewall on **OCI Gov cloud** regions is supported only with PAN-OS version 11.2.8 or above for FIPS and non-FIPS mode.*

Alibaba Cloud Regions

You can deploy the VM-Series firewall with PAN-OS® 8.1.3 and later PAN-OS 8.1 releases (where supported) or later supported PAN-OS releases in all Alibaba Cloud regions.

VM-Series Firewall Amazon Machine Images (AMI)

The two most recent versions—2.0 and 2.1—of the CFT for auto scaling the VM-Series firewall on AWS and the VM-Series Auto Scale Template are supported on all supported PAN-OS releases.

Please use the AWS CLI to find the AMI IDs for automating your deployment of VM-Series firewalls. (For convenience, we captured the list of PAN-OS Images for AWS GovCloud.)

PAN-OS Images for AWS GovCloud

Because AWS GovCloud had restricted access owing to specific U.S. regulatory requirements, the AMI IDs for the VM-Series firewall on AWS GovCloud are listed below for your convenience.

AMI IDs for VM-Series Firewalls on AWS GovCloud

Bring Your Own License (BYOL)

	us-gov-west-1 Cloned AMI ID	us-gov-east-1 Cloned AMI ID
PAN-OS 10.1.3	ami-0b0fb1dc91f1a5b9a	ami-0d1efc973806198d3
PAN-OS 10.1.1	ami-02f7ea8be900f9955	ami-0eeeec392d066b8ae
PAN-OS 9.1.9	ami-01686e0ff6dccff8c	ami-067d99132a54489a7
PAN-OS 9.1.8	ami-013219291e2bfe323	ami-07df5511d166c456e
PAN-OS 9.1.3	ami-019045558d9d46abe	

Pay-as-You-Go (PAYG) Bundle 1

	us-gov-west-1 Cloned AMI ID	us-gov-east-1 Cloned AMI ID
PAN-OS 10.1.3	ami-004b1a1777dcdfd9f	ami-016368ea5efba04e1
PAN-OS 10.1.1	ami-084ed91c50f9b4d96	ami-057662646115fdce4
PAN-OS 10.1.0	ami-0a5f5b771f7f8e5d3	ami-07ac1c7c5ce547d69
PAN-OS 9.1.15	ami-0e91c03870e1cd93c	ami-03437a1f70f52e166
PAN-OS 9.1.12-h3	ami-0b5bc9e573a08b041	ami-06749834defebd4e0
PAN-OS 9.1.10-c15	ami-0099471b6d15fbddb	ami-07797e48453a0682f
PAN-OS 9.1.10	ami-0709b58e478cab702	ami-0a098d4a886576dad

AMI IDs for VM-Series Firewalls on AWS GovCloud		
PAN-OS PAN-OS 9.1.3	ami-011be089674af6421	

Pay-as-You-Go (PAYG) Bundle 2

	us-gov-west-1 Cloned AMI ID	us-gov-east-1 Cloned AMI ID
PAN-OS 10.1.3	ami-0fb205aaef8ce2043	ami-0cb03b7f09207667b
PAN-OS 10.1.1	ami-0828cee4fb427a163	ami-0997795d86a05ede0
PAN-OS 10.1.0	ami-099a18de4da9ae98f	ami-0debf73b0bb9c2dbe
PAN-OS 9.1.15	ami-0a3050b051091a0eb	ami-0d67ea2069394aaba
PAN-OS 9.1.12-h3	ami-004abe9b7a57eed38	ami-068bf7a0c5746f727
PAN-OS 9.1.10-c15	ami-0a192fdfa754d6c40	ami-01df4c86af829b978
PAN-OS 9.1.10	ami-0fc65b7bb5280ec09	ami-050f8775e829afef7
PAN-OS 9.1.3	ami-06695afbfbca39f61	

CN-Series Firewalls

The CN-Series firewall is supported only in certain environments and is compatible with or requires a specific set of files to do so.

- CN-Series Supported Environments
- CN-Series Firewall Image and File Compatibility

CN-Series Supported Environments

You can deploy the CN-Series firewall in the following environments.

Product	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
Container runtime	Docker CRI-O Containers	Docker CRI-O Containers	Docker CRI-O Containers	Docker CRI-O Containers	Docker CRI-O Containers
Kubernetes version	1.17 through 1.27	1.17 through 1.31	1.17 through 1.31	1.17 through 1.31	1.17 through 1.31
Cloud provider managed Kubernetes	• AWS EKS (1.17 through 1.27 for CN-Series as a daemonset and CN-Series as a Service mode of deployment.) • EKS on AWS Outpost (1.17	• AWS EKS (1.17 through 1.31 for CN-Series as a daemonset and CN-Series as a Service mode of deployment.) • AWS EKS (1.17 through 1.31 for CN-Series	• AWS EKS (1.17 through 1.31 for CN-Series as a daemonset and CN-Series as a Service mode of deployment.) • AWS EKS (1.17 through 1.31 for CN-Series	• AWS EKS (1.17 through 1.31 for CN-Series as a daemonset and CN-Series as a Service mode of deployment.) • AWS EKS (1.17 through 1.31 for CN-Series	• AWS EKS (1.17 through 1.31 for CN-Series as a daemonset and CN-Series as a Service mode of deployment.) • AWS EKS (1.17 through 1.31 for CN-Series

Product	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
	through 1.22) *CN-Series for EKS on AWS Outpost does not support SR-IOV or Multus.* • Azure AKS (1.17 through 1.27) *In Azure AKS, the PAN-OS 10.1.10h1 is the minimum required version to support Kubernetes 1.25 and above.* • AliCloud ACK (1.26) • GCP GKE (1.17 through 1.27)	as a CNF mode of deployment.) • EKS on AWS Outpost (1.17 through 1.31) *CN-Series for EKS on AWS Outpost does not support SR-IOV or Multus.* • Azure AKS (1.17 through 1.31) *In Azure AKS, the PAN-OS 10.2.4h3 is the minimum required version to support Kubernetes 1.25 and above.*	as a CNF mode of deployment.) • EKS on AWS Outpost (1.17 through 1.31) *CN-Series for EKS on AWS Outpost does not support SR-IOV or Multus.* • Azure AKS (1.17 through 1.31) *In Azure AKS, the PAN-OS 11.0.2 is the minimum required version to support Kubernetes 1.25 and above.*	as a CNF mode of deployment.) • EKS on AWS Outpost (1.17 through 1.31) *CN-Series for EKS on AWS Outpost does not support SR-IOV or Multus.* • Azure AKS (1.17 through 1.31) *In Azure AKS, the PAN-OS 11.0.2 is the minimum required version to support Kubernetes 1.25 and above.*	as a CNF mode of deployment.) • EKS on AWS Outpost (1.17 through 1.31) *CN-Series for EKS on AWS Outpost does not support SR-IOV or Multus.* • Azure AKS (1.17 through 1.31) *In Azure AKS, the PAN-OS 11.0.2 is the minimum required version to support Kubernetes 1.25 and above.*

Product	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
		• GCP GKE (1.17 through 1.31)  *In GCP GKE, the PAN-OS 10.2.4h3 is the minimum required version to support Kubernetes 1.25 and above.* • Google Anthos 1.12.3 • OCI OKE (1.23)	• GCP GKE (1.17 through 1.31) • OCI OKE (1.23)	• GCP GKE (1.17 through 1.31) • OCI OKE (1.23)	• GCP GKE (1.17 through 1.31) • OCI OKE (1.23)
Customer-managed Kubernetes	On the public cloud or on-premises data center. Make sure that the Kubernetes version, CNI Types, and Host VM OS versions are included in this table. VMware TKG+ version 1.1.2	On the public cloud or on-premises data center. Make sure that the Kubernetes version, CNI Types, and Host VM OS versions are included in this table. VMware TKG+ version 1.1.2	On the public cloud or on-premises data center. Make sure that the Kubernetes version, CNI Types, and Host VM OS versions are included in this table. VMware TKG+ version 1.1.2	On the public cloud or on-premises data center. Make sure that the Kubernetes version, CNI Types, and Host VM OS versions are included in this table. VMware TKG+ version 1.1.2	On the public cloud or on-premises data center. Make sure that the Kubernetes version, CNI Types, and Host VM OS versions are included in this table. VMware TKG+ version 1.1.2

Product	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
	• Infrastructure Platform—vSphere 7.0 • Kubernetes Host VM OS—Photon OS	• Infrastructure Platform—vSphere 7.0 • Kubernetes Host VM OS—Photon OS	• Infrastructure Platform—vSphere 7.0 • Kubernetes Host VM OS—Photon OS	• Infrastructure Platform—vSphere 7.0 • Kubernetes Host VM OS—Photon OS	• Infrastructure Platform—vSphere 7.0 • Kubernetes Host VM OS—Photon OS
Kubernetes Host VM	Operating System: • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu-22.04 • RHEL/ CentOS 7.3 and later • CoreOS 21XX, 22XX • Container-Optimized OS	Operating System: • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu-22.04 • RHEL/ CentOS 7.3 and later • CoreOS 21XX, 22XX • Container-Optimized OS	Operating System: • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu-22.04 • RHEL/ CentOS 7.3 and later • CoreOS 21XX, 22XX • Container-Optimized OS	Operating System: • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu-22.04 • RHEL/ CentOS 7.3 and later • CoreOS 21XX, 22XX • Container-Optimized OS	Operating System: • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu-22.04 • RHEL/ CentOS 7.3 and later • CoreOS 21XX, 22XX • Container-Optimized OS
	Linux Kernel Netfilter: Iptables	Linux kernel version: • 4.18 or later (K8s Service Mode only) • 5.4 or later required to enable AF_XDP mode. See Editable Parameters in CN-Series Deployment YAML Files for more information.	Linux kernel version: • 4.18 or later (K8s Service Mode only) • 5.4 or later required to enable AF_XDP mode. See Editable Parameters in CN-Series Deployment YAML Files for more information.	Linux kernel version: • 4.18 or later (K8s Service Mode only) • 5.4 or later required to enable AF_XDP mode. See Editable Parameters in CN-Series Deployment YAML Files for more information.	Linux kernel version: • 4.18 or later (K8s Service Mode only) • 5.4 or later required to enable AF_XDP mode. See Editable Parameters in CN-Series Deployment YAML Files for more information.

Product	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
	Linux kernel version: • 4.18 or later (K8s Service Mode only) • 5.4 or later required to enable AF_XDP mode. See Editable Parameters in CN-Series Deployment YAML Files for more information.	Linux kernel Netfilter: Iptables	Linux kernel Netfilter: Iptables	Linux kernel Netfilter: Iptables	Linux kernel Netfilter: Iptables
CNI Plugins	CNI Spec 0.3 and later: • AWS-VPC • Azure • Calico • Flannel • Weave • For AliCloud, Terway • For Openshift, OpenshiftSDN • The following are supported on the CN-Series	CNI Spec 0.3 and later: • AWS-VPC • Azure • Calico • Flannel • Weave • For Openshift, OpenshiftSDN, OVN Kubernetes • The following are supported on the CN-Series	CNI Spec 0.3 and later: • AWS-VPC • Azure • Calico • Flannel • Weave • For Openshift, OpenshiftSDN, OVN Kubernetes • The following are supported on the CN-Series	CNI Spec 0.3 and later: • AWS-VPC • Azure • Calico • Flannel • Weave • For Openshift, OpenshiftSDN, OVN Kubernetes • The following are supported on the CN-Series	CNI Spec 0.3 and later: • AWS-VPC • Azure • Calico • Flannel • Weave • For Openshift, OpenshiftSDN, OVN Kubernetes • The following are supported on the CN-Series

Product	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
	firewall as a DaemonSet. • Multus • Bridge • SR-IOV • Macvlan	firewall as a DaemonSet. • Multus • Bridge • SR-IOV • Macvlan	firewall as a DaemonSet. • Multus • Bridge • SR-IOV • Macvlan	firewall as a DaemonSet. • Multus • Bridge • SR-IOV • Macvlan	firewall as a DaemonSet. • Multus • Bridge • SR-IOV • Macvlan
OpenShift	CN-Series as a DaemonSet: 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, and 4.13	• Version 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13,4.14,	• Version 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13,	• Version 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14, 4.15,	• Version 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14, 4.15,

Product	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
	CN-Series as a K8s Service: (PAN-OS 10.1.2 and later) 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14, and 4.15. *The PAN-OS 10.1.10h1 is the minimum required version to support 4.12 and above.*	4.15, 4.16, and 4.18 *OpenShift 4.7 is qualified on the CN-Series as a DaemonSet only.* *OpenShift 4.18 is qualified on the CN-Series as DaemonSet and K8s Service Mode only.* • OpenShift on AWS	4.14, 4.15, and 4.16 *OpenShift 4.7 is qualified on the CN-Series as a DaemonSet only.* *The PAN-OS 11.0.2 is the minimum required version to support 4.12 and above.* • OpenShift on AWS	4.16, and 4.18	4.16, and 4.18

Product	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
		The PAN-OS 10.2.4h3 is the minimum required version to support 4.12 and above.		*OpenShift 4.7 is qualified on the CN-Series as a DaemonSet only.* *OpenShift 4.18 is qualified on the CN-Series as DaemonSet and K8s Service Mode only.* *The PAN-OS 11.0.2 is the minimum required version to support 4.12 and above.* • OpenShift on AWS	*OpenShift 4.7 is qualified on the CN-Series as a DaemonSet only.* *OpenShift 4.18 is qualified on the CN-Series as DaemonSet and K8s Service Mode only.* *The PAN-OS 11.0.2 is the minimum required version to support 4.12 and above.* • OpenShift on AWS

CN-Series Firewall Image and File Compatibility

Deploying the CN-Series firewall requires a number of different of files. To help ensure a successful deployment, check the following information to make sure you download the correct combination of files for CN-Series firewall deployment.

PAN-OS Version	YAML Version	CNI Version	mgmt-init Version
PAN-OS 11.2.x PAN-OS 11.1.x PAN-OS 11.0.x PAN-OS 10.2.x PAN-OS 10.1.x	3.0.x	3.0.x	3.0.x

Panorama

This section includes information about Panorama™ and compatible versions for devices that Panorama can manage, as well as about plugins that are available for Panorama.

Panorama Plugins

The following tables describe the features and functionality introduced with the Panorama™ extensible plugin architecture.

- Cisco ACI
- Cisco TrustSec
- Panorama CloudConnector Plugin (Formerly, AIOps Plugin for Panorama)
- Cloud Services
- Enterprise Data Loss Prevention (DLP)
- Panorama Interconnect
- IPS Signature Converter
- Kubernetes
- Clustering Plugin
- Network Discovery
- Nutanix
- OpenConfig
- Panorama Software Firewall License Plugin
- Public Cloud—AWS, Azure, and GCP
- SD-WAN
- VMware NSX
- VMware vCenter
- Zero Touch Provisioning (ZTP)

For more information on Panorama plugin versions, refer to the VM-Series and Panorama Plugins Release Notes.

Plugins Bundled in Panorama 12.1.2

For PAN-OS 12.1, most plugins are bundled with the software package. The following plugins are part of the PAN-OS 12.1 package and available for installation from **Panorama** > **Plugins**.

Bundled Plugins	Version Released with PAN-OS 12.1.2
Advanced SD-WAN	3.4.0
AWS	6.0.1
Azure	6.0.1
Cisco ACI	4.0.0
Cisco TrustSec	3.0.0

Bundled Plugins	Version Released with PAN-OS 12.1.2
CloudConnector	2.1.1
Clustering	3.0.0
Enterprise Data Loss Prevention (DLP)	6.0.1
GCP	4.0.0
IPS Signature Converter	3.0.0
Kubernetes	5.0.1
Network Discovery	3.0.0
Nutanix	3.0.0
OpenConfig	2.1.4
Panorama Software Firewall License	1.2.1
Software Firewall Orchestration	1.0.1
VM-Series	6.1.0
VMware NSX	6.0.0
VMware VCenter	3.0.0
Zero Touch Provisioning	4.0.0
Cloud Services	6.0.0-h20

Cisco ACI

The following table shows the features introduced in each version of the Panorama™ plugin for Cisco ACI. The plugin uses device groups on Panorama to push the configuration to the managed firewalls.

End-of-life (EoL) software versions are included in this table. Review the Software End-of-Life Summary website to check whether we are still supporting your software version.

Plugin Version	Supported Cisco ACI Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
3.0.1	6.0.x, 6.1	10.2 (10.2.7)	Latest	Introduces support for Endpoint Security Group (ESG) tags and fixes to known issues.
	• 5.1.x, 5.2.x	10.2 (10.2.0)		
3.0.0	• 6.0.x	10.2 (10.2.4)	Latest	Introduces enhancements to increase reliability and robustness.
	• 5.2.x • 5.1.x	10.2 (10.2.0)		
2.0.3	• 6.0.x	10.1 (10.1.9)	Latest	Introduces a fix for a known issue.
	• 5.2.x • 5.1.x	10.1		

Plugin Version	Supported Cisco ACI Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
	• 5.0.x • 4.2.x • 4.1.x • 4.0.x • 3.2	9.1		*You can do a new deployment of Cisco ACI 2.0.3 on Panorama 9.0 or later. You can also upgrade from Cisco ACI 2.0.x to Cisco ACI 2.0.3. However, if you need to upgrade from Cisco ACI 1.0.0 or Cisco ACI 1.0.1, you will need to upgrade your Panorama to 10.0 or later, and then upgrade the ACI plugin to 2.0.3.*
2.0.2	• 5.1.x • 5.0.x • 4.2.x • 4.1.x	10.1 9.1	Latest	Introduces Cisco ACI 5.1 support and fixes for known issues.

Plugin Version	Supported Cisco ACI Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
	• 4.0.x • 3.2			*You can do a new deployment of Cisco ACI 2.0.2 on Panorama 9.0 or later. You can also upgrade from Cisco ACI 2.0.x to Cisco ACI 2.0.2. However, if you need to upgrade from Cisco ACI 1.0.0 or Cisco ACI 1.0.1, you will need to upgrade your Panorama to 10.0 or later, and then upgrade the ACI plugin to 2.0.2.*
2.0.1	• 5.0.x • 4.2.x • 4.1.x • 4.0.x	10.1 9.1	Latest	Introduces fixes for known issues.

Plugin Version	Supported Cisco ACI Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
	• 3.2			
2.0.0	• 5.0.x • 4.2.x • 4.1.x • 4.0.x • 3.2	10.1 9.1	Latest	Introduces the Panorama Plugin for Cisco ACI Dashboard and two new monitored attributes—L2 external endpoint groups and subnets under bridge domains.
1.0.1	• 5.0.x • 4.0.x • 3.2 • 3.1 • 2.3(1e)	9.1	9.1	Introduces support for multiple IP addresses per endpoint and Cisco ACI 4.0 and later.
1.0.0	• 5.0.x • 3.2 • 3.1 • 2.3(1e)	9.1	9.1	Enables support for Endpoint Monitoring from Panorama. Configure the Panorama plugin for Cisco ACI to monitor endpoints so that you can consistently enforce security policy that automatically adapts to changes within your ACI deployment.

Cisco TrustSec

The following table shows the features introduced in each version of Panorama™ plugin for Cisco TrustSec.

End-of-life (EoL) software versions are included in this table. Review the Software End-of-Life Summary website to check whether we are still supporting your software version.

Plugin Version	Minimum Panorama PAN-OS Version	Qualified Cisco ISE Versions	Features
2.0.2	10.2	• ISE 3.4 • ISE 3.3 • ISE 3.2 • ISE 3.1 • ISE 2.7	Introduces fixes for known issues.
2.0.1	10.2	• ISE 3.3 • ISE 3.2 • ISE 3.1 • ISE 2.7	Introduces fixes for known issues.
2.0.0	10.2	• ISE 3.2 • ISE 3.1 • ISE 2.7	Introduces support for Panorama 10.2.x. Introduces support for security group tags (SGT). Use these tags as match criteria for placing IP addresses in dynamic address groups.
1.0.3	9.1	• ISE 3.1 • ISE 2.7	Introduces a fix for one issue.
1.0.2	9.1	• ISE 2.4 • ISE2.6	Introduces the PubSub monitoring mode, which parses notifications directly from the server. The plugin enables PubSub mode when v1.0.2 is running on Panorama 10.0.0 and later. If v1.0.2 is running on a Panorama version earlier than 10.0.0, the monitoring mode is Bulk Sync.
1.0.1			• Lowers the minimum monitoring interval from 30 seconds to 10 seconds.

Plugin Version	Minimum Panorama PAN-OS Version	Qualified Cisco ISE Versions	Features
			• Combined Logs for the Panorama Plugin for Cisco TrustSec.
1.0.0			Enables support for endpoint monitoring from Panorama. Configure the Panorama plugin for Cisco TrustSec to monitor endpoints so that you can consistently enforce security policy that automatically adapts to changes within your TrustSec environment.

Panorama CloudConnector Plugin (Formerly, AIOps Plugin for Panorama)

The following table shows the features introduced in each version of the plugin for AIOps.

Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	New Features or Changes
2.1.0	10.2 (10.2.3)	Latest	Supports proxy configuration settings from Panorama.
2.0.1	10.2 (10.2.3)	Latest	Introduces enhancements for Cloud NGFW for AWS integration with Panorama.
2.0.0	10.2 (10.2.3)	Latest	Enables you to use the Panorama AWS plugin 5.0.0 to author and push device group based policies to Cloud NGFW for AWS resources.
1.1.0	10.2 (10.2.3)	Latest	Enables the policy analyzer feature that helps you to

Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	New Features or Changes
			check if a new security rule meets your intended purpose and that it does not duplicate, shadow, or conflict with your existing rules (pre-commit). You can also check for duplication and other anomalies across your current Security policy rulebase (post-commit).
1.0.0	10.2 (10.2.1)	Latest	Enables you to proactively enforce best practice checks by validating your commits and letting you know if a policy needs work before pushing it to your Panorama.

Cloud Services

You use the Cloud Services plugin to activate Panorama Managed Prisma Access and to retrieve logs from Panorama-managed firewalls using Strata Logging Service. Review the following table to see the minimum Panorama and plugin versions for your deployment type.

Deployment Type	Panorama and Plugin requirements
Panorama Managed Prisma Access	Dependent on plugin version. Review the Minimum Required Panorama Software Versions required for the plugin you are running. To find the plugin version you are running, select **Panorama** > **Cloud Services** > **Configuration** > **Service Setup** and find the plugin version in the **Plugin Alert** area.
Strata Logging Service log retrieval from Panorama-managed firewalls only	Strata Logging Service Software Compatibility has the minimum Panorama and plugin requirements.

Enterprise Data Loss Prevention (DLP)

The following table shows the features introduced in each version of the Panorama™ plugin for Enterprise Data Loss Prevention (DLP).

End-of-life (EoL) software versions are included in this table. Review the Software End-of-Life Summary website to check whether we are still supporting your software version.

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Cloud Services Plugin (Minimum)	Features
6.0.1	12.1.2	Latest	Cloud Services 6.0	Granular data profiles enhance Enterprise DLP detection capabilities by allow you to apply differentiated inline content inspection requirements and response actions with the same Security policy rule.
5.0.7	11.1.0	Latest 11.2	Cloud Services 5.0 Preferred	Minor bug and performance fixes.
5.0.6	11.1.0	Latest 11.2	Cloud Services 5.0 Preferred	Minor bug and performance fixes.
5.0.5	11.1.0	Latest 11.2	Cloud Services 5.0 Preferred	Minor bug and performance fixes.
5.0.4	11.1.0	Latest 11.2	Cloud Services 5.0 Preferred	Upgrade to Enterprise DLP plugin 5.0.4 to use AI Access Security for Prisma Access (Managed by Panorama). AI Access Security enables organizations to safely adopt GenAI applications by employees by mitigating the risks posed by inadvertent data leakage in prompts and malicious content in responses. Fine-grained data exfiltration and access control policies let you to control the data exposed to GenAI apps while simultaneously allowing

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Cloud Services Plugin (Minimum)	Features
				you to block access when necessary. A robust dashboard with detailed monitoring capabilities provides paralleled insights in to how GenAI apps are used across your organization.
5.0.3	11.1.0	Latest 11.2	Cloud Services 5.0 Preferred	Upgrade to Enterprise DLP plugin 5.0.3 to use AI Access Security for NGFW (Managed by Panorama). AI Access Security enables organizations to safely adopt GenAI applications by employees by mitigating the risks posed by inadvertent data leakage in prompts and malicious content in responses. Fine-grained data exfiltration and access control policies let you to control the data exposed to GenAI apps while simultaneously allowing you to block access when necessary. A robust dashboard with detailed monitoring capabilities provides paralleled insights in to how GenAI apps are used across your organization.
5.0.2	11.1.0	11.2.2	Cloud Services 5.0 Preferred	Minor bug and performance fixes.

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Cloud Services Plugin (Minimum)	Features
5.0.1	11.1.0	Latest 11.1 Release	Cloud Services 5.0 Preferred	Minor bug and performance fixes.
5.0.0	11.1.0	Latest 11.1 Release	Cloud Services 5.0 Preferred	You must upgrade to Enterprise DLP 5.0 plugin to upgrade to PAN-OS 11.1. Additionally, you must download the Enterprise DLP 5.0 plugin before you attempt to install PAN-OS 11.1.
4.0.4	11.0.3	Latest 11.0 Release	Cloud Services 4.0 Preferred	Minor bug and performance fixes.
4.0.3	11.0.3	Latest 11.0 Release	Cloud Services 4.0 Preferred	Minor bug and performance fixes.
4.0.2	11.0.3	Latest 11.0 Release	Cloud Services 4.0 Preferred	The data pattern character limit for a data profile is removed. Data profiles no longer limit the number of data pattern match criteria based on the number of alphanumeric characters in the data pattern name, description, regular expressions, and proximity keywords.
4.0.1	11.0.2	11.0.2	Cloud Services 4.0 Preferred	Enterprise Data Loss Prevention (E-DLP) now supports creating a file type include or exclude list for data filtering profiles configured for file-based inspection. This allows you to select one of two modes:

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Cloud Services Plugin (Minimum)	Features
				• **Inclusion Mode**—Allow only specified file types be scanned by Enterprise DLP. • **Exclusion Mode**—Allow all supported files to be scanned by Enterprise DLP by default but excluding the file types you specify. Exclusion Mode includes True File Type Support and does not rely on file extensions to determine file types.
4.0.0	11.0.0	11.0.1	Cloud Services 4.0 Preferred	You must upgrade to Enterprise DLP 4.0 plugin to upgrade to PAN-OS 11.0. Additionally, you must download the Enterprise DLP 4.0 plugin before you attempt to install PAN-OS 11.0.
3.0.10	10.2.8	Latest 10.2 Release	Cloud Services 3.1.0-h50 (PAN-OS 10.2.2-h1 and later releases)	Minor bug and performance fixes.
3.0.9	10.2.8	Latest 10.2 Release	Cloud Services 3.1.0-h50 (PAN-OS 10.2.2-h1 and later releases)	Minor bug and performance fixes.
3.0.8	10.2.4-h3	10.2.7	Cloud Services 3.1.0-h50	Minor bug and performance fixes.

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Cloud Services Plugin (Minimum)	Features
			(PAN-OS 10.2.2-h1 and later releases)	
3.0.8	10.2.4-h3	10.2.7	Cloud Services 3.1.0-h50 (PAN-OS 10.2.2-h1 and later releases)	Minor bug and performance fixes.
3.0.7	10.2.4-h3	10.2.7	Cloud Services 3.1.0-h50 (PAN-OS 10.2.2-h1 and later releases)	Minor bug and performance fixes.
3.0.6	10.2.4-h3	10.2.7	Cloud Services 3.1.0-h50 (PAN-OS 10.2.2-h1 and later releases)	The data pattern character limit for a data profile is removed. Data profiles no longer limit the number of data pattern match criteria based on the number of alphanumeric characters in the data pattern name, description, regular expressions, and proximity keywords.
3.0.5	10.2.4-h3	10.2.7	Cloud Services 3.1.0-h50 (PAN-OS 10.2.2-h1 and later releases)	Minor bug and performance fixes.
3.0.4	10.2.4	10.2.4-h3	Cloud Services 3.1.0-h50 (PAN-OS 10.2.2-h1 and later releases)	Enterprise DLP now supports new applications, expanded download support and large file inspection for many existing applications, and

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Cloud Services Plugin (Minimum)	Features
				FedRAMP High compliance.
3.0.3	10.2.3-h4	10.2.4	Prisma Access 3.1.0-h50 (PAN-OS 10.2.2-h1 and later releases)	Enterprise DLP now supports upload inspection of files up to 100MB in size for the Box Web App and Web Browsing applications.
3.0.2	10.2.3	Latest 10.2.3-h4	Cloud Services 3.1.0-h50 (PAN-OS 10.2.2-h1 and later releases)	Enterprise DLP now supports inspection of file and non-file based HTTP/2 traffic.
3.0.1	10.2.1	10.2.3	Cloud Services 3.1.0-h50 (PAN-OS 10.2.2-h1 and later releases)	The Panorama plugin for Enterprise DLP supports creating a data filtering profile to scan non-file based traffic for sensitive data.
3.0.0	10.2.0	10.2.1	Not Supported	Upgrade to the Enterprise DLP plugin to increase reliability. Enterprise DLP plugin 3.0 is required to upgrade to PAN-OS 10.2 and is supported only on PAN-OS 10.2 and later releases.
1.0.8	10.1.11	Latest 10.1 Release	Cloud Services 2.2	Minor bug and performance fixes.
1.0.7	10.1	Latest 10.1 Release	Cloud Services 2.2	Minor bug and performance fixes.
1.0.6	10.1	Latest 10.1 Release	Cloud Services 2.2	Minor bug and performance fixes.

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Cloud Services Plugin (Minimum)	Features
1.0.5	10.1	Latest 10.1 Release	Cloud Services 2.2	Minor bug and performance fixes.
1.0.4	10.1	Latest 10.1 Release	Cloud Services 2.2	Minor bug and performance fixes.
1.0.3	10.1	Latest 10.1 Release	Cloud Services 2.2	The Panorama plugin for DLP supports the integration of Enterprise DLP with Prisma Access.
1.0.2	10.1	Latest 10.1 Release	Not Supported	No new features were added for this release.
1.0.1	10.1	Latest 10.1 Release	Not Supported	Enables support for Enterprise DLP from Panorama. Configure the Panorama plugin for Enterprise DLP to protect against unauthorized access, misuse, extraction, and sharing of sensitive information and effectively filter network traffic to block or generate an alert before sensitive information leaves the network.

Panorama Interconnect

The following table shows the features introduced in each version of the Panorama™ Interconnect plugin.

End-of-life (EoL) software versions are included in this table. Review the Software End-of-Life Summary website to check whether we are still supporting your software version.

Plugin Version	Minimum PAN-OS Version	Maximum PAN-OS Version	New Features or Changes
2.0.0	10.2.4 (PAN-OS 10.2 release)	Latest 10.2 version (PAN-OS 10.2 release)	You must upgrade to Panorama Interconnect 2.0.0 plugin to upgrade to PAN-OS 10.2.
1.1.0	10.0.0	Latest 10.1 version	Enables you to selectively push device groups, template stacks, and some common Panorama configurations from the Panorama Controller to the Panorama Nodes to avoid pushing extraneous configurations to Panorama Nodes to minimize configuration bloat and operational delays across your Panorama Interconnect deployment.
1.0.2	9.1	Latest 10.1 version	Minor bug and performance fixes.
1.0.1			Minor bug and performance fixes.
1.0.0			First plugin introduced to support a two-tier Panorama deployment for a horizontal scale-out architecture.

IPS Signature Converter

The following table shows the features introduced in each version of the Panorama™ IPS Signature Converter plugin.

End-of-life (EoL) software versions are included in this table. Review the Software End-of-Life Summary website to check whether we are still supporting your software version.

Plugin Version	Minimum PAN-OS Version	Features
2.0.3	10.2	• Supports the Startswith and Endswith keywords. • Supports DNS protocol and the dns_query keyword.
2.0.2	10.2	Supports SMTP and FTP protocols.
2.0.1	10.2	Supports HTTP sticky buffers. Now converts Snort rules that have commas separating content patterns and their associated suboption.
2.0.0	10.2	Uses Python 3 for compatibility with PAN-OS 10.2.
1.0.7	10.1	• Supports the Startswith and Endswith keywords. • Supports DNS protocol and the dns_query keyword.
1.0.6	10.1	Supports SMTP and FTP protocols.
1.0.5	10.1	Supports HTTP sticky buffers. Now converts Snort rules that have commas separating content patterns and their associated suboption.
1.0.4	10.1	No significant changes in functionality.
1.0.3	10.1	Converts rules into SSL custom signatures if their port is **443**. Converts server-to-client HTTP rules without content modifiers into custom signatures with the **`http-rsp-status-line`** and **`http-rsp-headers`** contexts. Converts Suricata TLS rules into TLS custom signatures and supports additional TLS and file data sticky buffers.

Plugin Version	Minimum PAN-OS Version	Features
1.0.2	10.1	Converts rules that use the **smb** protocol or port **445**. Supports HTTP sticky buffer keywords in Suricata rules. Converts HTTP rules into HTTP custom signatures if either the port in the rule is **HTTP-_PORTS** or the protocol is **http**.
1.0.1	10.1	Identifies whether newly converted signatures are already included as part of your Palo Alto Networks Threat Prevention subscription.
1.0.0	10.1	Enables support for third-party IPS signature conversion from Panorama. Use the Panorama IPS Signature Converter plugin to gain immediate protection against newly discovered threats by converting third-party IPS rules into Palo Alto Networks custom threat signatures and distributing them to your Panorama-managed firewalls.

Kubernetes

The following table displays the features introduced in each version of the Panorama™ Kubernetes plugin.

End-of-life (EoL) software versions are included in this table. Review the Software End-of-Life Summary website to check whether we are still supporting your software version.

Plugin Version	Minimum Panorama PAN-OS Version	Maximum Panorama PAN-OS Version	Features
4.0.0	11.0	Latest	Introduces new features like CN-Series Hyperscale Security Fabric, (HSF), Tag Length Enhancement, Shared DAG Support, and Nested DAG Support.

Plugin Version	Minimum Panorama PAN-OS Version	Maximum Panorama PAN-OS Version	Features
3.0.3	10.2	Latest	Introduces fixes for known issues.
3.0.2	10.2	Latest	Introduces fixes for known issues.
3.0.1			Introduces support for shared dynamic address groups.
3.0.0			Introduces Retrieving IPv6 Addresses for Multus CNI Setup, Tag Pruning, Service Account Validation, and advanced Dashboard features.
2.0.2	10.1	10.1	K8s plugin 2.0.2 creates a new template on Panorama called **K8S-Network-Setup-V1-125**. This template creates 250 vwire interfaces and 125 vwires.
2.0.1			Introduces fixes for known issues.
2.0.0			Introduces Core-Based Licensing, Multiple Interface Support, and Custom Certificate Chaining.
1.0.5			Introduces fixes for known issues.
1.0.4			Introduces fixes for known issues.
1.0.3			Introduces fixes for known issues.
1.0.2			Introduces fixes for known issues.

Plugin Version	Minimum Panorama PAN-OS Version	Maximum Panorama PAN-OS Version	Features
1.0.1			Introduces the ability to disable the creation of service objects on Panorama, and support for offline licensing of CN-Series firewalls with Panorama.
1.0.0			Manages licenses for the CN-Series firewall and enables you to monitor clusters and leverage Kubernetes labels that you use to organize Kubernetes objects. The plugin communicates with the API server and retrieves metadata, which gives you visibility into applications running within a cluster.

Clustering Plugin

The following table shows the features introduced in Panorama Clustering plugin.

Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
2.0.0	11.1.5	Latest	Provides a migration process that allows you to migrate from a non-PA-7500 Series firewall with an existing Panorama non-clustering template to a PA-7500 Series firewall with a Panorama clustering template. The release also provides support for MACsec on the HSCI ports that connect the firewalls in the NGFW

Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
			cluster. MACsec provides data confidentiality and integrity between the two endpoints.
2.0.0	11.1.3	Latest	Provides visibility to the NGFW clusters (also known as PA-Series clusters) in PA-7500 Series firewalls.
1.0.0	11.0	Latest	Provides the visibility to the Hyper Scale Security Fabric (HSF) clusters in CN-Series.

Network Discovery

The following table shows the features introduced in each version of the Panorama™ plugin for Network Discovery.

Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
2.2.2	10.2.17 11.1	Latest 10.2. release Latest 11 release	Includes fixes for known issues.
2.2.1	10.2.14 11.1	Latest 10.2 release Latest 11 release	Includes fixes for known issues.
2.2.0	10.2.14 11.1	Latest 10.2 release Latest 11 release	Introduces new protocols for device polling.
2.1.2	10.2.14 11.1	Latest 10.2 release Latest 11 release	Includes fixes for known issues.
2.1.1	10.2.14 11.1	Latest 10.2 release Latest 11 release	Includes fixes for known issues.

Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
2.1.0	10.2.14 11.1	Latest 10.2 release Latest 11 release	Introduces support for multiple entry switches and multiple SNMP credentials. Supports site creation and site overwrite for existing subnets learned through SNMP crawling.
2.0.2	11.1	Latest 11 release	Introduces new protocols for device polling. Introduces new settings options for configuring SNMP network discovery and network data refreshment jobs. Includes a fix for a known issue.
2.0.1	11.1	Latest 11 release	Introduces debug logs and fixes for a known issue.
2.0.0	11.1	Latest 11 release	Introduces device polling using various protocols. Use polling to learn new device attributes to send to Device Security.
1.0.1	11.1	Latest 11 release	Introduces the capability to specify a network discovery protocol using the CLI.
1.0.0	11.1	Latest 11 release	Introduces SNMP querying for switches and network devices. Use SNMP querying to learn bindings and network data to send to Device Security.

Nutanix

The following table shows the features introduced in each version of the Panorama™ plugin for Nutanix.

End-of-life (EoL) software versions are included in this table. Review the Software End-of-Life Summary website to check whether we are still supporting your software version.

Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
2.0.2	10.2	Latest	Introduces fixes for known issues.
2.0.1	10.2	Latest	Introduces fixes for known issues.
2.0.0			Introduces enhancements to increase reliability and robustness.
1.0.0	9.0 (9.0.4)	Latest	Enables support for VM Monitoring from Panorama. Configure the Panorama plugin for Nutanix to monitor VM workloads so that you can consistently enforce security policy that automatically adapts to changes within your Nutanix environment.

OpenConfig

The following table shows the features introduced in each version of the OpenConfig plugin.

End-of-life (EoL) software versions are included in this table. Review the Software End-of-Life Summary website to check whether we are still supporting your software version.

Plugin Version	PAN-OS Version (Minimum)	New Features or Changes
2.1.2	10.2.11	A number of improvements and bug fixes.
2.1.1	10.2.11	Support for XML API and File-upload custom PAN-OS data models.
2.1.0	10.2.11	General improvements and bug fixes.
2.0.2	10.2.11	Plugin support for PAN-OS version 10.2.11 and later.
2.0.1	11.0.4	Plugin support for PAN-OS version 11.0.4 and later.
2.0	11.1	Enables Panorama suppport and telemetry streaming with PAN-OS custom data models for logging, PCAP, and config data. Starting with 2.0, the OpenConfig plugin also comes prepackaged with PAN-OS.
1.3 (Firewall Only)	10.1	Enables support for all streaming modes with the OpenConfig-routing-policy model.
1.2.0 (Firewall Only)		Enables support for protobuf and unbundling.
1.1.0 (Firewall Only)		Enables support for these standard OpenConfig models: • openconfig-ha • openconfig-zones • openconfig-network-instances • openconfig-routing-policy • openconfig-ospfv2
1.0.0 (Firewall Only)		Enables support for the OpenConfig plugin on PAN-OS firewalls so that you can use standard OpenConfig models to automate configuration and stream telemetry.

Panorama Software Firewall License Plugin

The following table shows the features introduced in each version of the Panorama™ Software Firewall License plugin.

End-of-life (EoL) software versions are included in this table. Review the Software End-of-Life Summary website to check whether we are still supporting your software version.

Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Minimum VM-Series Plugin Version	Features
1.2.0	10.0 (10.0.4)	Latest	2.0.4	Introduces fixes for known issues.
1.1.3	10.0 (10.0.4)	Latest	2.0.4	Introduces fixes for known issues.
1.1.2	10.0 (10.0.4)	Latest	2.0.4	Introduces fixes for known issues.
1.1.1	10.1	Latest	2.0.4	Introduces fixes for known issues.
1.1.0				Introduces fixes for known issues.
1.0.0				The Panorama Software Firewall License plugin allows you to automatically license a VM-Series firewall when it connects to Panorama.

Public Cloud—AWS, Azure, and GCP

The following table shows the features introduced in each version of the Panorama™ plugin for Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). The plugins use device groups and templates on Panorama to push the configuration to the managed firewalls.

End-of-life (EoL) software versions are included in this table. Review the Software End-of-Life Summary website to check whether we are still supporting your software version.

Public Cloud Platform	AWS Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	VM-Series Plugin Version (Minimum)	Features
AWS	5.4.1	10.2 (10.2.3)	Latest	3.0.0	Introduces fixes for known issues.
	5.3.4	10.2 (10.2.3)	Latest	3.0.0	Introduces fixes for known issues.
	5.3.2	10.2 (10.2.3)	Latest	3.0.0	Introduces fixes for known issues.
	5.3.1	10.2 (10.2.3)	Latest	3.0.0	Introduces fixes for known issues.
	5.3.0	10.2 (10.2.3)	Latest	3.0.0	Adds support for Egress NAT and Zone-based Policy Rules on the Cloud NGFW for AWS. Introduces fixes for known issues.
	5.2.2	10.2 (10.2.3)	Latest	3.0.0	Introduces fixes for known issues.
	5.2.1	10.2 (10.2.3)	Latest	3.0.0	Introduces fixes for known issues.
	5.1.3	10.2 (10.2.3)	Latest	3.0.0	Introduces fixes for known issues.
	5.1.2	10.2 (10.2.3)	Latest	3.0.0	Introduces fixes for known issues.
	5.1.1	10.2 (10.2.3)	Latest	3.0.0	Introduces enhancements for Cloud NGFW for AWS integration with Panorama.
	5.0.1	10.2 (10.2.3)	Latest	3.0.0	Introduces enhancements for Cloud NGFW for AWS integration with Panorama.

Public Cloud Platform	AWS Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	VM-Series Plugin Version (Minimum)	Features
	5.0.0	10.2 (10.2.3)	Latest	3.0.0	Introduces support for Panorama integration with Cloud NGFW for AWS.
	4.1.0	10.2	Latest	3.0.0	Introduces support for nested dynamic address groups and tag pruning.
	4.0.0	10.2	Latest	3.0.0	Introduces enhancements to increase reliability and robustness.
	3.0.3	10.1	10.1	2.0.6	Introduces shared dynamic address groups support and bug fixes.
	3.0.2	10.1	10.1	2.0.6	Introduces proxy support and bug fixes.
	3.0.1	10.1	10.1	2.0.6	Introduces enhancements and bug fixes.
	3.0.0	10.1	10.1	2.0.6	Introduces Panorama Orchestration and new monitoring parameters.
	2.0.2	10.1	10.1	2.0.2	Introduces fixes for known issues.
		9.1 (9.1.2)		1.0.8	
	2.0.1			1.0.4	Introduces a fix for a known issue.

Public Cloud Platform	AWS Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	VM-Series Plugin Version (Minimum)	Features
	2.0.0	9.1 (9.1.2)	10.1	1.0.8	Enables support for: • VM Monitoring • Secure Kubernetes Services in an EKS Cluster

Public Cloud Platform	Azure Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	VM-Series Plugin Version (Minimum)	Features
Azure	5.2.2	10.2.4	Latest	4.0.0	Adds support for Strata Logging Service. Introduces fixes for known issues.
	5.2.1	10.2.4	Latest	4.0.0	Adds permission validation for private endpoint read access. Introduces new tags used for monitoring. Introduces fixes for known issues.
	5.2.0	10.2.4	Latest	4.0.0	Introduces an automated workflow for maintaining the life cycle of the VM auth key.
	5.1.2	10.2.4	Latest	4.0.0	Introduces loopback zone support and DNS proxy support on

Public Cloud Platform	Azure Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	VM-Series Plugin Version (Minimum)	Features
					Cloud NGFW for Azure.
	5.1.1	10.2.4	Latest	4.0.0	Introduces tag pruning feature to increase the scalability and the number of tags collected by the Azure plugin.
	5.0.0	10.2.4	Latest	4.0.0	Introduces support for Panorama integration with Cloud NGFW for Azure.
	4.2.0	10.2 (10.2.3)	Latest	3.0.1	Introduces support for Azure Workspace-based Application Insights.
	4.1.0	10.2	Latest	Latest	Increased the number of front-end applications per VM-Series for Azure deployment.
	4.0.0	10.2	Latest	Latest	Introduces enhancements to increase reliability and robustness.
	3.2.2	10.1	10.1	2.1.0 2.0.1	Introduces fixes for a known issue.
	3.2.1	10.1	10.1	2.1.0 2.0.1	Introduces fixes for known issues.

Public Cloud Platform	Azure Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	VM-Series Plugin Version (Minimum)	Features
	3.2.0	10.1	10.1	2.1.0 2.0.1	Introduces proxy support and fix for a known issue.
	3.1.0	10.1	10.1	2.1.0 2.0.1	Introduces fixes for a known issue.
	3.0.1	10.1	10.1	2.1.0 2.0.1	Introduces fixes for known issues.
	3.0.0 (Upgrade from 2.0.0 to 3.0.0 is not supported.)	10.1	10.1	2.1.0 2.0.1	Introduces Panorama Orchestration.
	2.0.3	10.1	10.1	2.1.0 2.0.0	Introduces a fix for a known issue.
		9.1 (9.1.2)		1.0.8	
		9.1		1.0.4	
	2.0.2	9.1	10.1	1.0.4	Introduces fixes for known issues.
	2.0.1	9.1	10.1	1.0.4	Introduces fixes for known issues.
	2.0.0	9.1	10.1	1.0.4	Enables support for: • Auto Scaling—Template v1.0 • Azure Kubernetes Service (AKS)

Public Cloud Platform	Azure Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	VM-Series Plugin Version (Minimum)	Features
					Cluster—Template v1.0

Public Cloud Platform	GCP Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	VM-Series Plugin Version	Features
GCP	3.1.2	10.2	Latest	3.0.0	Addresses a known issue.
	3.1.1	10.2	Latest	3.0.0	Introduces performance and status enhancements in monitoring definitions.
	3.1.0	10.2	Latest	3.0.0	Introduces monitoring of shared VPC deployments.
	3.0.0	10.2	Latest	3.0.0	Introduces enhancements to increase reliability and robustness.
	2.0.0 (Upgrade from 1.0.0 to 2.0.0 is not supported.)	9.1	Latest	1.0.4	Enables you to monitor and secure VMs or GKE clusters deployed in GCP. • Deploy auto scaling for VM instance groups or GKE clusters using auto

Public Cloud Platform	GCP Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	VM-Series Plugin Version	Features
					scaling templates for both firewall and application deployments. • VM Monitoring for GCP assets.

SD-WAN

The following table shows the features introduced in each version of the Panorama™ plugin for SD-WAN.

End-of-life (EoL) software versions are included in this table. Review the Software End-of-Life Summary website to check whether we are still supporting your software version.

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Features
3.4.0	12.1.2	Latest	*(PAN-OS 12.1.2 or later releases) Upgrading the SD-WAN plugin version manually is no longer required.* SD-WAN 3.4.0 and later plugin versions are managed by Panorama.

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Features
			To use the following feature or enhancements, you require PAN-OS 12.1.2 or later releases. • Configure HA peers simultaneously from a single window while adding the SD-WAN firewall branches and hubs, ensuring configuration consistency between the active and passive devices. • Bug fixes.
3.3.3-h1	11.2.5 or 11.2.4-h4	Latest	Bug fixes.
3.3.3	11.2.5	Latest	To use the following feature or enhancements, you require PAN-OS 11.2.5 or later 11.2 releases. • Configure Post-Quantum IKEv2 VPNs with RFC 8784 PPKs. • Bug fixes.
3.3.2	11.2.4	Latest	To use the following feature or enhancements, you require PAN-OS 11.2.4 or later 11.2 releases. • Prisma Access Hub Support for SD-WAN enabled Cellular Interfaces (4G/5G). • Improvements and bug fixes.
3.3.1	11.2.3	Latest	To use the following feature or enhancements, you

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Features
			require PAN-OS 11.2.3 or later 11.2 releases. • Support for multiple virtual routers on the SD-WAN branches to have overlapping IP subnet addresses on both hub and branch devices. • Support for SD-WAN capability to the 5G cellular interface. • Bug fixes.
3.3.0	11.2	Latest	To use the following feature or enhancements, you require PAN-OS 11.2.0 or later releases. • Supports monitoring the **bandwidth** of a tunnel and a physical interface for a selected site (by default) in addition to existing **jitter**, **latency**, and **packet loss** performance measures. • Supports multiple virtual routers on the SD-WAN hubs that enable you to have overlapping IP subnet addresses on branch devices connecting to the same SD-WAN hub. • Additional SD-WAN hubs supported for VPN cluster. • Additional private link types supported for

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Features
			SD-WAN interface profile. • Bug and performance fixes.
3.2.4	11.1.8 (11.1.8)	Latest	To use the following feature or enhancements, you require PAN-OS 11.1.8 or later 11.1 releases. • Supports dedicated tunnel to Panorama for establishing a persistent and dedicated IPSec tunnels from your branch devices to Panorama through designated termination devices using DIA interfaces. • Bug fixes.
3.2.3-h2	11.1.8 (11.1.8)	Latest	Bug fixes.
3.2.3	11.1.8 (11.1.8)	Latest	To use the following feature or enhancements, you require PAN-OS 11.1.8 or later 11.1 releases. • Configure Post-Quantum IKEv2 VPNs with RFC 8784 PPKs. • Bug fixes.
3.2.2-h1	11.1.5 (11.1.5)	Latest	Bug fixes.
3.2.2	11.1.5 (11.1.5)	Latest	To use the following feature or enhancements, you require PAN-OS 11.1.5 or later releases.

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Features
			• Supports monitoring the **bandwidth** of a tunnel and a physical interface for a selected site (by default) in addition to existing **jitter**, **latency**, and **packet loss** performance measures. • Supports MongoDB related HA peer synchronization CLI commands. • SD-WAN plugin improvements. • Bug fixes.
3.2.1	11.1 (11.1.3)	Latest	To use the following feature or enhancements, you require PAN-OS 11.1.3 or later 11.1 releases. • Supports multiple virtual routers on the SD-WAN hubs that enable you to have overlapping IP subnet addresses on branch devices connecting to the same SD-WAN hub. • Additional SD-WAN hubs supported for VPN cluster. • Additional private link types supported for SD-WAN interface profile. • Bug fixes.
3.2.0	11.1	Latest	• SD-WAN IKEv2 certificate-based

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Features
			authentication support. • Public cloud SD-WAN high availability support. • Enable SD-WAN on IPv6 interfaces and IPv6 tunnel support. • Bug and performance fixes.
3.1.3	11.0 (11.0.4)	Latest	To use the following feature or enhancements, you require PAN-OS 11.0.4 or later 11.0 releases. • Additional SD-WAN hubs supported for VPN cluster. • Additional private link types supported for SD-WAN interface profile. • Bug and performance fixes.
3.1.2	11.0 (11.0.2)	Latest	Bug and performance fixes.
3.1.1	11.0 (11.0.2)	Latest	SD-WAN IPv6 basic connectivity
3.0.1-h6	11.0 (11.0.1)	Latest	Bug and performance fixes.
3.1.0-h6	11.0 (11.0.1)	Latest	Enables Advanced Routing Engine support.
3.0.8-h2	10.2.11	Latest	Bug fixes.
3.0.8	10.2.11	Latest	Improvements and bug fixes

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Features
3.0.7	10.2 (10.2.8)	Latest	To use the following feature or enhancements, you require PAN-OS 10.2.8 or later releases. • Supports multiple virtual routers on the SD-WAN hubs that enable you to have overlapping IP subnet addresses on branch devices connecting to the same SD-WAN hub. • Bug fixes.
3.0.6	10.2 (10.2.7)	Latest	Bug fixes.
3.0.6	10.2 (10.2.6)	Latest	Bug fixes.
3.0.5	10.2 (10.2.5)	Latest	Bug and performance fixes.
3.0.4	10.2 (10.2.4)	Latest	Bug and performance fixes.
3.0.3	10.2 (10.2.1)	Latest	Bug and performance fixes.
3.0.2	10.2 (10.2.1)	Latest	Bug and performance fixes.
3.0.1	10.2 (10.2.1)	Latest	Copy ToS Header Support.
3.0.0	10.2	Latest	Upgrade to the SD-WAN plugin to increase reliability. SD-WAN plugin 3.0 is required to upgrade to PAN-OS 10.2 and is supported only on PAN-OS 10.2 and later releases.
2.2.7-h5	10.1.14-h2	Latest	Bug fixes.

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Features
2.2.7	10.1.3-h1	Latest	Improvements and bug fixes
2.2.6	10.1 (10.1.11)	Latest	Bug and performance fixes.
2.2.5	10.1 (10.1.11)	Latest	Bug and performance fixes.
2.2.4	10.1 (10.1.10)	Latest	Bug and performance fixes.
2.2.3	10.1 (10.1.9)	Latest	Bug and performance fixes.
2.2.2	10.1 (10.1.5-h1)	Latest	Bug and performance fixes.
2.2.1	10.1 (10.1.5-h1)	Latest	Copy ToS Header support.
2.2.0	10.1 (10.1.4)	Latest	Prisma Access Hub support.
2.1.1	10.1	Latest	Minor bug and performance fixes.
2.1.0	10.1	Latest	SD-WAN supports Aggregated Ethernet (AE) interfaces with or without subinterfaces for link redundancy. AE interfaces allow you to tag for different ISP services to achieve end-to-end traffic segmentation. SD-WAN also supports Layer 3 subinterfaces for end-to-end traffic segmentation.
2.0.3	10.1	Latest	Minor bug and performance fixes.
2.0.2	10.1	Latest	Includes support so you can control whether

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Features
			Auto VPN configuration enables or disables the **Remove Private AS** setting for all BGP peer groups on a branch or hub.
2.0.1	10.1	Latest	Includes support for full mesh VPN cluster with DDNS service, auto-VPN configuration with branch behind NAT, and Direct Internet Access (DIA) AnyPath.
2.0.0	10.1	Latest	Maintain high-quality application experience by leveraging Forward Error Correction (FEC) and packet duplication and by accurately measuring SaaS and Cloud applications when you have an SD-WAN firewall with Direct Internet Access (DIA) links.
1.0.6	9.1 (9.1.4)	Latest	Minor bug and performance fixes.
1.0.5	9.1 (9.1.4)	Latest	Minor bug and performance fixes.
1.0.4	9.1 (9.1.4)	Latest	In an SD-WAN VPN cluster that has more than one hub, you must assign a priority to each hub, which determines the primary hub and hub failover order. Panorama maps the priority to a BGP local preference and pushes the local preference

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Features
			to the branches in the cluster.
1.0.3	9.1 (9.1.3)	9,1	When the SD-WAN hub is behind a NAT device, the plugin supports an upstream NAT IP address or FQDN for Auto VPN configuration to use as a tunnel endpoint.
1.0.2	9.1 (9.1.2-h1)	9.1.3	Improves ease of use, such as an automatic Security policy rule to allow BGP between branches and hubs, ability to refresh the IKE preshared key for VPN cluster members, specifying VPN tunnel IP address ranges, and more.
1.0.1	9.1 (9.1.1)	9.1.2	Improves monitoring experience and search filtering, and adds an option to display HA peers consecutively.
1.0.0	9.1	9.1.2	Enables support for SD-WAN from Panorama. Configure the Panorama plugin for SD-WAN to provide intelligent and dynamic path selection on top of the industry-leading security that PAN-OS software already delivers. Provide the optimal end user experience by leveraging multiple ISP links to ensure application performance and scale capacity.

VMware NSX

The following table shows the features introduced in each version of the VM-Series firewall VMware NSX plugin. For additional information about each plugin, see the release notes on the Customer Support Portal.

End-of-life (EoL) software versions are included in this table. Review the Software End-of-Life Summary website to check whether we are still supporting your software version.

Plugin Version	Panorama Version (Minimum)	Panorama Version (Maximum)	Managed VM-Series PAN-OS Version (Minimum)	New Features or Changes
5.0.1	• NSX-V: 10.2 (10.2.2) • NSX-T N/S: 10.2 (10.2.2) • NSX-T E/W: 10.2 (10.2.2)	• NSX-V: 10.2 • NSX-T N/S: 10.2 • NSX-T E/W: 10.2	• NSX-V: 9.1 • NSX-T N/S: 9.1 • NSX-T E/W: 9.1	Introduces support for PAN-OS and Panorama 10.2.x.
5.0.0				Introduces support for PAN-OS and Panorama 10.2.x.
4.0.3	• NSX-V: 10.1 • NSX-T N/S: 10.1 • NSX-T E/W: 10.1	• NSX-V: 10.1 • NSX-T N/S: 10.1 • NSX-T E/W: 10.1	• NSX-V: 9.1 • NSX-T N/S: 9.1 • NSX-T E/W: 9.1	Introduces fixes for known issues.
4.0.2				Introduces fixes for known issues.
4.0.1				Introduces fixes for known issues.
4.0.0				Introduces Security-Centric Deployment Workflow (East-West) for the VM-Series on VMware NSX-T.

Plugin Version	Panorama Version (Minimum)	Panorama Version (Maximum)	Managed VM-Series PAN-OS Version (Minimum)	New Features or Changes
3.2.4	• NSX-V: 10.1 • NSX-T N/S: 10.1 • NSX-T E/W: 10.1	• NSX-V: 10.1 • NSX-T N/S: 10.1 • NSX-T E/W: 10.1	• NSX-V: 9.1 • NSX-T N/S: 9.1 • NSX-T E/W: 9.1	Introduces fixes for known issues.
3.2.3				Introduces fixes for known issues.
3.2.1	• NSX-V: 9.1 • NSX-T N/S: 9.1 • NSX-T E/W: 9.1			Introduces fixes for known issues.
3.2.0	• NSX-V: 9.1 • NSX-T N/S: 9.1 • NSX-T E/W: 9.1	• NSX-V: 10.1 • NSX-T N/S: 10.1 • NSX-T E/W: 10.1	• NSX-V: 9.1 • NSX-T N/S: 9.1 • NSX-T E/W: 9.1	Introduces Security Policy Extension Between NSX-V and NSX-T and Device Certificate Support on the VM-Series for NSX. The following VM-Series firewall for NSX OVFs require that you enable device certificates. • 10.1 or later • 9.1.5 or later
3.1.0	9.1	• NSX-V: 10.1 • NSX-T N/S: 10.2 • NSX-T E/W: 10.2	• NSX-V: 9.1 • NSX-T N/S: 9.1 • NSX-T E/W: 9.1	Introduces the VM-Series firewall on VMware NSX-T for East-West traffic protection.

VMware vCenter

The following table shows the features introduced in each version of the Panorama™ plugin for VMware vCenter.

End-of-life (EoL) software versions are included in this table. Review the Software End-of-Life Summary website to check whether we are still supporting your software version.

Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
2.1.0	10.2	Latest	Introduces fixes for known issues.
2.0.0			Introduces enhancements to increase reliability and robustness.
1.0.0	9.1	Latest	Enables support for VM Monitoring from Panorama. Configure the Panorama plugin for VMware vCenter to monitor VM workloads so that you can consistently enforce security policy that automatically adapts to changes within your vCenter environment.

Zero Touch Provisioning (ZTP)

The following table shows the features introduced in each version of the Panorama™ plugin for Zero Touch Provisioning (ZTP).

End-of-life (EoL) software versions are included in this table. Review the Software End-of-Life Summary website to check whether we are still supporting your software version.

Plugin Version	PAN-OS Version Minimum	Maximum PAN-OS Version	Features
3.0.1	11.2.0	Latest	Minor bug and performance fixes.
3.0.0	11.2.0	Latest	ZTP 3.0 introduces enhancements to

Plugin Version	PAN-OS Version Minimum	Maximum PAN-OS Version	Features
			the ZTP onboarding experience by allowing you to activate applicable licenses and install the latest content updates when the firewall first connects to Panorama.
2.0.4	11.0.1 10.2.4	Latest	Minor bug and performance fixes.
2.0.3	11.0.1 10.2.4	Latest	Minor bug and performance fixes.
2.0.2	10.2.0	10.2.3	Minor bug and performance fixes.
2.0.1	10.2.0	10.2.3	Minor bug and performance fixes.
2.0.0	10.2.0	10.2.3	Upgrade to the ZTP plugin to increase reliability. ZTP plugin 2.0 is required to upgrade to PAN-OS 10.2 and is supported only on PAN-OS 10.2 and later releases.
1.0.2	10.1.0	Latest 10.1 release	Minor bug and performance fixes.
1.0.1	10.1.0	Latest 10.1 release	Minor bug and performance fixes.
1.0.0	9.1.4	Latest 9.1 release	Enables support for ZTP from Panorama. Configure the Panorama plugin for ZTP to simplify and streamline initial firewall deployment by automating the new managed firewall on-boarding without the need for network

Plugin Version	PAN-OS Version Minimum	Maximum PAN-OS Version	Features
			administrators to manually provision the firewall.

Compatible Plugin Versions for PAN-OS 10.2

To increase reliability and robustness, we enhanced PAN-OS® software starting in PAN-OS 10.2 with upgraded Panorama™ plugins and by installing the VM-Series plugin by default. However, we did not introduce support for all plugins with the initial release of PAN-OS 10.2. Use the following table to determine the minimum plugin versions for use with PAN-OS 10.2 software and, where applicable, the first PAN-OS 10.2 version that supports each plugin. (If no PAN-OS 10.2 version is specified, then the minimum version of the plugin is supported in all PAN-OS 10.2 versions.)

For more information about plugins compatible with PAN-OS 10.2 and all other supported PAN-OS releases, refer to the Panorama Plugins page.

Plugin Name	Minimum Compatible Plugin Version with PAN-OS 10.2
AWS plugin	4.0.0
AIOps for NGFW plugin	1.0.0
Azure plugin	4.0.0
Cloud Services plugin (for use with Strata™ Logging Service only)	3.1 (Compatible with PAN-OS 10.2.1 and later PAN-OS 10.2 versions)
Cloud Services plugin (for use with Panorama Managed Prisma Access)	• 3.2 (compatible with PAN-OS 10.2.3 and later PAN-OS 10.2 versions) • 3.1 starting with version 3.1.0-h50 (compatible with PAN-OS 10.2.2-h1 and later PAN-OS 10.2 versions) IMPORTANT: Review the PAN-OS and Prisma Access Known Issues that are applicable to Panorama deployments running PAN-OS 10.2.2 with Prisma Access 3.1.
Kubernetes plugin	3.0.0
SW FW Licensing plugin (VM licensing plugin is not a Python-based plugin and the previous version is supported)	1.0.0
Panorama VM-Series plugin	3.0.0
SD-WAN plugin	3.0.0
IPS Signature Converter plugin	2.0.0

Plugin Name	Minimum Compatible Plugin Version with PAN-OS 10.2
ZTP plugin	2.0.0
DLP plugin	3.0.0
OpenConfig plugin	1.1.0
GCP plugin	3.0.0
Cisco ACI plugin	3.0.0
VCenter plugin	2.0.0
Nutanix plugin	2.0.0
Cisco TrustSec plugin	2.0.0
Network Discovery plugin	2.1.0 and later 2.x versions

Important considerations for upgrading your plugins

- *The plugin versions listed in the above table are the only plugins compatible with PAN-OS 10.2 and later PAN-OS 10.2 versions. If you use any other plugins, you should not upgrade to PAN-OS 10.2 until you upgrade all of your plugins to the minimum supported version for PAN-OS 10.2.*
- *Starting with PAN-OS 10.2, the VM-Series plugin is installed by default. This option is currently available only in PAN-OS 10.2, which means that Panorama software requires that you download a compatible version of the VM-Series plugin if you downgrade your firewall from PAN-OS 10.2 to a PAN-OS 10.1 or earlier version.*

Each upgraded Panorama plugin supports any supported PAN-OS release in addition to PAN-OS 10.2.

Supported Migration Paths for Plugins

Plugin Name	Upgrade/ Downgrade	Base PAN-OS Version	Base Plugin Version	Target PAN-OS Version	Target Plugin Version
AWS	Upgrade	10.1	3.0	10.2	4.0

Plugin Name	Upgrade/ Downgrade	Base PAN-OS Version	Base Plugin Version	Target PAN-OS Version	Target Plugin Version
			You should upgrade AWS plugin 2.x.x to 3.0.x in PAN-OS 10.1.x version before you upgrade to PAN-OS 10.2.		
	Downgrade	10.2	4.0	10.1	3.0
Azure plugin	Upgrade	10.1	3.1	10.2	4.0
	Downgrade	10.2	4.0	10.1	3.2
Kubernetes plugin	Upgrade	10.1	2.0	10.2	3.0
	Downgrade	10.2	3.0	10.1	2.0

Plugin Name	Upgrade/ Downgrade	Base PAN-OS Version	Base Plugin Version	Target PAN-OS Version	Target Plugin Version
					If you have a custom certificate size greater than 32k, the autocommit (which happens after downgrade) will fail. To avoid this, save the config file, add a dummy value in the custom certificate that is less than 16K, and then downgrade to 2.0.x (k8s plugin cannot contact the API server). Then upgrade the

Plugin Name	Upgrade/ Downgrade	Base PAN-OS Version	Base Plugin Version	Target PAN-OS Version	Target Plugin Version
GCP plugin	Upgrade	10.1	2.0	10.2	3.0
	Downgrade	10.2	3.0	10.1	2.0
Cisco ACI plugin	Upgrade	10.1	2.0	10.2	3.0
	Downgrade	10.2	3.0	10.1	2.0
VCenter plugin	Upgrade	10.1	1.0	10.2	2.0
	Downgrade	10.2	2.0	10.1	1.0
Nutanix plugin	Upgrade	10.1	1.0	10.2	2.0
	Downgrade	10.2	2.0	10.1	1.0

For more information, review how to:

- Upgrade your PAN-OS software.
- Upgrade your Panorama plugins.

Panorama Management Compatibility

Review the table below to understand which Palo Alto Networks Next-Generation Firewall, Dedicated Log Collector, and WildFire® appliances a Panorama™ management server can manage based on the installed PAN-OS version. Palo Alto Networks recommends management of currently supported Palo Alto Networks Next-Generation Firewalls, Dedicated Log collector, and WildFire appliance running a supported PAN-OS version.

(PAN-OS 10.2.6 and earlier releases) Panorama must be running the same or a later PAN-OS version than the firewall it manages.

Dedicated Log Collectors must be running the same or later PAN-OS version than managed firewalls from which logs are forwarded. Palo Alto Networks does not support forwarding logs from managed firewalls to a Dedicated Log Collector if the Dedicated Log Collector is running an earlier PAN-OS version than that installed on your managed firewalls. This may lead to log forwarding and ingestion issues.

(PAN-OS 10.2.7 and later releases) Dedicated Log Collectors can receive logs from firewalls running a higher version of PAN-OS within the same release train.

Panorama can manage a firewall running a higher version of PAN-OS within the same release train. For example, a Panorama appliance running PAN-OS 10.2.7 can manage a firewall running PAN-OS 10.2.8 or later 10.2 releases. Panorama does not support any new features, optimizations, or platforms introduced in the later versions of PAN-OS or installed plugins. For information on new features, see the PAN-OS or Plugin Release Notes. It is a best practice that Panorama runs the same or a later PAN-OS version than the firewall it is managing.

Dedicated Log Collectors can receive logs from firewalls running a higher version of PAN-OS within the same release train.

(PAN-OS 10.1.2 and earlier PAN-OS 10.1 releases) The device registration authentication key length is increased when you upgrade Panorama to PAN-OS 10.1.3 or later release:

- **Panorama running PAN-OS 10.1.2 or earlier PAN-OS 10.1 releases—** Supports onboarding firewalls, Dedicated Log Collectors, and WildFire appliances running PAN-OS 10.1.2 or earlier PAN-OS 10.1 release, or running PAN-OS 10.0 or earlier PAN-OS release.
- **Panorama running PAN-OS 10.1.3 or later releases—** Supports onboarding firewalls, Dedicated Log Collectors, and WildFire appliances running PAN-OS 10.1.3 or later release, or running PAN-OS 10.0 or earlier PAN-OS release.

Despite these onboarding requirements, Panorama supports managing firewalls, Dedicated Log Collectors, and WildFire appliances running the PAN-OS versions described below.

PAN-OS software versions that are End-of-Life (EoL) are not displayed. See the Palo Alto Networks End of Life Announcements for additional information. EoL PAN-OS versions are supported only for End-of-Sale (EoS) firewall models until they reach EoL.

Management of End-of-Life (EoL) PAN-OS versions may result in unexpected issues, particularly if there is a large gap between the PAN-OS version installed on Panorama and the one installed on the firewall. For example, you may run into unexpected or unknown issues if you attempt to manage a firewall running the EoL PAN-OS 7.1 release from a Panorama management server running PAN-OS 10.2 or a later version.

Panorama Version	Managed Device Version
11.2	11.2 11.1 11.0 10.2 10.1 9.1
11.1	11.1 11.0 10.2 10.1 9.1
11.0	11.0 10.2 10.1 9.1
10.2	10.2 10.1 9.1
10.1	10.1 9.1
9.1	9.1

Panorama Hypervisor Support

Before you deploy a Panorama™ virtual appliance, verify that the hypervisor meets the minimum version requirements to deploy Panorama.

*VMX-19 is supported on Panorama running **PAN-OS 11.1.5 or later** on VMWare ESXi 7.0. The supported base image for this configuration is Panorama-ESX-11.1.3.ova.*

Panorama Version	VMware ESXi Compatibility	KVM Compatibility	Hyper-V Compatibility	Nutanix AHV Compatibility	Public Cloud/ Partner Integra Compatibility
PAN-OS 11.2, 11.1	64-bit kernel-based VMware ESXi 6.0, 6.5, 6.7, 7.0, or 8.0. The supported version of the virtual hardware family type (also known as the VMware virtual hardware version) on the ESXi server is vmx-15. ESXi 6.0 and later versions supports one disk of up to 8TB. Earlier ESXi versions support one disk of up to 2TB.	• Ubuntu 18.04 • Ubuntu 16.04 • CentOS/ RHEL 7 • CentOS/ RHEL 8	• Windows Server 2019 with Hyper-V role or Hyper-V 2019 • Windows Server 2016 with Hyper-V role or Hyper-V 2016 • Windows Server 2022 with Hyper-V role or Hyper-V 2022	Nutanix AOS version 7.0 Nutanix AHV v10.0	• Alibaba Cloud • Amazon AWS • Microsoft Azure • Google Cloud Platform • Amazon AWS GovCloud • Oracle Cloud Infrastructure (OCI)
PAN-OS 11.0	64-bit kernel-based	• Ubuntu 18.04	• Windows Server	—	• Alibaba Cloud

Panorama Version	VMware ESXi Compatibility	KVM Compatibility	Hyper-V Compatibility	Nutanix AHV Compatibility	Public Cloud/ Partner Integra Compatibility
	VMware ESXi 6.0, 6.5, 6.7, 7.0, or 8.0. The supported version of the virtual hardware family type (also known as the VMware virtual hardware version) on the ESXi server is vmx-15. ESXi 6.0 and later versions supports one disk of up to 8TB. Earlier ESXi versions support one disk of up to 2TB.	• Ubuntu 16.04 • CentOS/ RHEL 7 • CentOS/ RHEL 8	2019 with Hyper-V role or Hyper-V 2019 • Windows Server 2016 with Hyper-V role or Hyper-V 2016 • Windows Server 2022 with Hyper-V role or Hyper-V 2022		• Amazon AWS • Microsoft Azure • Google Cloud Platform • Amazon AWS GovCloud • Oracle Cloud Infrastructure (OCI)
PAN-OS 10.2	64-bit kernel-based VMware ESXi 6.0, 6.5, 6.7, 7.0, or 8.0. The supported version of the virtual hardware family type (also known as the VMware	• Ubuntu 18.04 • Ubuntu 16.04 • CentOS/ RHEL 7 • CentOS/ RHEL 8	• Windows Server 2019 with Hyper-V role or Hyper-V 2019 • Windows Server 2016 with Hyper-V role or Hyper-V 2016	Nutanix AOS Version—5.10 and later Nutanix AHV Version—20170830.185 To manage VM-Series firewalls running supported	• Alibaba Cloud • Amazon AWS • Microsoft Azure • Google Cloud Platform • Amazon AWS GovCloud

Panorama Version	VMware ESXi Compatibility	KVM Compatibility	Hyper-V Compatibility	Nutanix AHV Compatibility	Public Cloud/ Partner Integra Compatibility
	virtual hardware version) on the ESXi server is vmx-15. ESXi 6.0 and later versions supports one disk of up to 8TB. Earlier ESXi versions support one disk of up to 2TB.		• Windows Server 2022 with Hyper-V role or Hyper-V 2022	versions of AHV. See VM-Series for Nutanix.	• Oracle Cloud Infrastructure (OCI)
PAN-OS 10.1	64-bit kernel-based VMware ESXi 6.0, 6.5, 6.7, or 7.0. The supported version of the virtual hardware family type (also known as the VMware virtual hardware version) on the ESXi server is vmx-10. ESXi 6.0 and later versions supports one disk of up to 8TB.	• Ubuntu 18.04 • Ubuntu 16.04 • CentOS/ RHEL 7 • CentOS/ RHEL 8	• Windows Server 2019 with Hyper-V role or Hyper-V 2019 • Windows Server 2016 with Hyper-V role or Hyper-V 2016	Nutanix AOS Version—5.10 and later Nutanix AHV Version—20170830.185 To manage VM-Series firewalls running supported versions of AHV. See VM-Series for Nutanix.	• Alibaba Cloud • Amazon AWS • Microsoft Azure • Google Cloud Platform • Amazon AWS GovCloud • Oracle Cloud Infrastructure (OCI)

Panorama Version	VMware ESXi Compatibility	KVM Compatibility	Hyper-V Compatibility	Nutanix AHV Compatibility	Public Cloud/ Partner Integra Compatibility
	Earlier ESXi versions support one disk of up to 2TB.				
PAN-OS 9.1	64-bit kernel-based VMware ESXi 6.0, 6.5, 6.7, or 7.0. The supported version of the virtual hardware family type (also known as the VMware virtual hardware version) on the ESXi server is vmx-10. ESXi 6.0 and later versions supports one disk of up to 8TB. Earlier ESXi versions support one disk of up to 2TB.	• Ubuntu 18.04 • Ubuntu 16.04 • CentOS/ RHEL 7 • CentOS/ RHEL 8	• Windows Server 2019 with Hyper-V role or Hyper-V 2019 • Windows Server 2016 with Hyper-V role or Hyper-V 2016	Nutanix AOS Version—5.10 and later Nutanix AHV Version—20170830.185 To manage VM-Series firewalls running supported versions of AHV. See VM-Series for Nutanix.	• Amazon AWS • Microsoft Azure • Google Cloud Platform • Amazon AWS GovCloud

Device Certificate for a Palo Alto Networks Cloud Service

A Palo Alto Networks cloud service is a cloud-hosted service maintained and operated by Palo Alto Networks.

You must install the appropriate device certificate on the firewalls, Panorama™ appliances, and WildFire® appliances that are using the cloud service that is running one of the following PAN-OS® versions:

- PAN-OS 11.2.0 or a later PAN-OS 11.2 version
- PAN-OS 11.1.0 or a later PAN-OS 11.1 version
- PAN-OS 11.0.2 or a later PAN-OS 11.0 version
- PAN-OS 10.2.5 or a later PAN-OS 10.2 version
- PAN-OS 10.1.10 or alater PAN-OS 10.1 version
- PAN-OS 9.1.8 or a later PAN-OS 9.1 version

Review the Palo Alto Networks cloud services listed below that require you to install a device certificate before it will function as expected. Panorama management of firewalls, Dedicated Log Collectors, and WildFire appliances or downloading content and software updates from the Palo Alto Networks update server does not require a device certificate. You also do not need to install a device certificate to establish communication between a firewall and a WildFire appliance.

Cloud Service	Firewall (Individual and Panorama-Managed)	Panorama
AIOps	Yes	Yes
App-ID Cloud Engine (ACE)	Yes	Yes
Cloud Services (Prisma® Access)	N/A	No
Strata™ Logging Service (Formerly Cortex® Data Lake)	Yes (PAN-OS 10.1 and later)	Yes (PAN-OS 10.1 and later)
Device Telemetry	Yes	Yes
Enterprise DLP	Yes	Yes
Advanced URL Categorization (PAN-DB)	Yes	No

Cloud Service	Firewall (Individual and Panorama-Managed)	Panorama
Also requires an Advanced URL Filtering license		
Inline Cloud Analysis Also requires an Advanced Threat Protection license	Yes	No
Internet of Things (IoT) Security	Yes	Yes
ZTP	Yes	Yes

MFA Vendor Support

Palo Alto Networks Next-Generation Firewalls and Panorama™ appliances can integrate with multi-factor authentication (MFA) vendors using RADIUS and SAML. Firewalls can additionally integrate with specific MFA vendors using the API to enforce MFA through Authentication policy.

Authentication Use Case	RADIUS (any vendor)	TACACS + (any vendor)	SAML (any vendor)	MFA Server Profile
Next-Generation Firewall and Panorama Administrator Web Interface	√	√	√	—
Next-Generation Firewall and Panorama Administrator CLI	√	√	—	—
GlobalProtect™ Portal and Gateway Authentication	√	√	√	—
Authentication Policy (Formerly Captive Portal Policy)	√	√	√	√ **Vendor / Min. Content Version** * • RSA SecurID Access / 752 • PingID / 655 • Okta Adaptive / 655 • Duo v2 / 655

* *Palo Alto Networks provides support for MFA vendors through Applications content updates, which means that if you use Panorama to push device group configurations to firewalls, you must install the same Applications release version on managed firewalls as you install on Panorama to avoid mismatches in vendor support.*

Supported Cipher Suites

Use this table in the Palo Alto Networks Compatibility Matrix to determine support for cipher suites according to function and PAN-OS® software release.

Cloud Identity Engine Cipher Suites

The following cipher suites are supported and required on the Cloud Identity Engine agent host for on-premises directories.

Feature or Function	Required Ciphers
Cloud Identity Engine agent	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Cipher Suites Supported in PAN-OS 11.2

The following topics list cipher suites that are supported on firewalls running a PAN-OS® 11.2 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.2 Cipher Suites Supported in FIPS-CC Mode.

The ciphers supported in normal operation mode are grouped according to feature or functionality in the following sections:

- PAN-OS 11.2 GlobalProtect Cipher Suites
- PAN-OS 11.2 IPSec Cipher Suites
- PAN-OS 11.2 IKE and Web Certificate Cipher Suites
- PAN-OS 11.2 Decryption Cipher Suites
- PAN-OS 11.2 HA1 SSH Cipher Suites
- PAN-OS 11.2 Administrative Session Cipher Suites
- PAN-OS 11.2 PAN-OS-to-Panorama Connection Cipher Suites

PAN-OS 11.2 GlobalProtect Cipher Suites

The following table lists cipher suites for GlobalProtect™ supported on firewalls running a PAN-OS® 11.2 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.2 Cipher Suites Supported in FIPS-CC Mode.

- GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal
- GlobalProtect App/Agent—IPSec mode
- GlobalProtect Portal—Browser Access

Feature or Function	Ciphers Supported in PAN-OS 11.2 Releases
GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal	• TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 11.2 Releases
	• RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-SEED-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA-1 • ECDHE-RSA-AES-128-SHA-1 • ECDHE-RSA-AES-256-SHA-1 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-128-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384 • TLS-AES-128-GCM-SHA256 • TLS-AES-256-GCM-SHA384 • TLS-CHACHA20-POLY1305-SHA256
GlobalProtect App/Agent—IPSec mode (Keys transported through SSL session with gateway)	• AES-128-CBC-HMAC-SHA-1 • AES-128-GCM-HMAC-SHA-1 • AES-256-GCM-HMAC-SHA-1
GlobalProtect Portal—Browser Access	• SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 11.2 Releases
	• DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA-1 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384

PAN-OS 11.2 IPSec Cipher Suites

The following table lists the cipher suites for IPSec that are supported on firewalls running a PAN-OS® 11.2 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.2 Cipher Suites Supported in FIPS-CC Mode.

- IPSec—Post-Quantum Cryptographic Suites (PQCs)
- IPSec—Encryption
- IPSec—Message Authentication
- IPSec—Key Exchange

Feature or Function	Ciphers Supported in PAN-OS 11.2 Releases

IPSec—Post-Quantum Cryptographic Suites (PQCs)	You can use these cipher suites to secure the rekey operations for your IPSec tunnels.
	• ML-KEM—512-bit, 768-bit, and 1024-bit keys
	• HQC—128-bit, 192-bit, and 256-bit keys
	• BIKE—bike-L1, bike-L3, & bike-L5
	• Classic McEliece—348,864-bit and 348,864f-bit
	• FrodoKEM:
	  • 640-AES, 976-AES, and 1344-AES
	  • 640-SHAKE, 976-SHAKE, and 1344-SHAKE
	• NTRU-Prime—sntrup761

IPSec—Encryption	• NULL • 3DES

Feature or Function	Ciphers Supported in PAN-OS 11.2 Releases
	• AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CCM • AES-128-GCM • AES-256-GCM
IPSec—Message Authentication	• NONE • HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IPSec—Key Exchange	Diffie-Hellman groups with or without perfect forward secrecy (PFS): • No PFS—This option specifies that the firewall reuses the same key for IKE phase 1 and phase 2 instead of renewing the key for phase 2. • Group 1 (768-bit keys) with PFS enabled • Group 2 (1024-bit keys) with PFS enabled • Group 5 (1536-bit keys) with PFS enabled • Group 14 (2048-bit keys) with PFS enabled • Group 15 (3072-bit modular exponential group) • Group 16 (4096-bit modular exponential group) • Group 19 (256-bit elliptic curve group) with PFS enabled • Group 20 (384-bit elliptic curve group) with PFS enabled • Group 21 (512-bit random elliptic curve group)

PAN-OS 11.2 IKE and Web Certificate Cipher Suites

The following table lists cipher suites for Internet Key Exchange (IKE) and PAN-OS® web certificates that are supported on firewalls running a PAN-OS 11.2 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.2 Cipher Suites Supported in FIPS-CC Mode.

- IKE—Post-Quantum Cryptographic Suites (PQCs)

- IKE Certificate Support
- IKE—Encryption
- IKE—Message Authentication
- IKE—Key Exchange
- PAN-OS Web Certificates

Feature or Function	Ciphers Supported in PAN-OS 11.2 Releases

IKE—Post-Quantum Cryptographic Suites (PQCs)	• ML-KEM—512-bit, 768-bit, and 1024-bit keys
	• HQC—128-bit, 192-bit, and 256-bit keys
	• BIKE—bike-L1, bike-L3, & bike-L5
	• Classic McEliece—348,864-bit and 348,864f-bit
	• FrodoKEM:
	  • 640-AES, 976-AES, and 1344-AES
	  • 640-SHAKE, 976-SHAKE, and 1344-SHAKE
	• NTRU-Prime—sntrup761

IKE Certificate Support	• RSA
	  • Keys—512-bit, 1024-bit, 2048-bit, and 3072-bit keys
	  • Digital signature algorithms—SHA-1, SHA-256, SHA-384, or SHA-512
	• ECDSA
	  • Keys—256-bit and 384-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

IKE—Encryption	• 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC **Starting with PAN-OS 10.0.3:** • AES-128-GCM • AES-256-GCM
IKE—Message Authentication	• HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 11.2 Releases
	• HMAC-SHA-512
IKE—Key Exchange	Diffie-Hellman groups • Group 1 (768-bit keys) • Group 2 (1024-bit keys) • Group 5 (1536-bit keys) • Group 14 (2048-bit keys) • Group 15 (3072-bit modular exponential group) • Group 16 (4096-bit modular exponential group) • Group 19 (256-bit elliptic curve group) • Group 20 (384-bit elliptic curve group) • Group 21 (512-bit random elliptic curve group)

PAN-OS Web Certificates	• RSA
	  • Keys—2048-bit, 3072-bit, and 4096-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512
	• ECDSA
	  • Keys—256-bit and 384-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

PAN-OS 11.2 Decryption Cipher Suites

The following table lists cipher suites for decryption that are supported on firewalls running a PAN-OS® 11.2 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.2 Cipher Suites Supported in FIPS-CC Mode.

- SSH Decryption—Host Key Algorithms
- SSH Decryption (SSHv2 only)—Encryption
- SSH Decryption (SSHv2 only)—Message Authentication
- SSL/TLS Decryption
- SSL/TLS Decryption—NIST-approved Elliptical Curves
- SSL/TLS Decryption—Perfect Forward Secrecy (PFS) Ciphers
- TLS 1.3 Decryption—Signature Algorithms

Feature or Function	Ciphers Supported in PAN-OS 11.2 Releases
SSH Decryption—Host Key Algorithms	• SSH-RSA (2048-bit) • SSH-DSS (2048-bit)
SSH Decryption (SSHv2 only)—Encryption	• AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR • AES-256-CTR
SSH Decryption (SSHv2 only)—Message Authentication	• HMAC-RIPEMD • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-1-96 • HMAC-RIPEMD-160 • HMAC-SHA-1
SSL/TLS Decryption	• SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3 cipher suites • RSA 512-bit, 1024-bit, 2048-bit, 3072-bit, 4096-bit, and 8192-bit keys *The firewall can authenticate certificates up to 8192-bit RSA keys from the destination server, however the firewall generated certificate to the client supports only up to 4096-bit RSA keys.* • RSA-RC4-128-MD5 • RSA-RC4-128-SHA-1 • RSA-3DES-EDE-CBC-SHA-1 • RSA-AES-128-CBC-SHA-1 • RSA-AES-256-CBC-SHA-1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • TLS_AES_256_GCM_SHA-384 • TLS_CHACHA20_POLY1305_SHA-256 • TLS_AES_128_GCM_SHA-256

Feature or Function	Ciphers Supported in PAN-OS 11.2 Releases
SSL/TLS Decryption—NIST-approved Elliptical Curves	• P-192 (secp192r1) • P-224 (secp224r1) • P-256 (secp256r1) • P-384 (secp384r1) • P-521 (secp521r1) • (TLS 1.3 only) X25519 • (TLS 1.3 only) X448
SSL/TLS Decryption—Perfect Forward Secrecy (PFS) Ciphers  *If you use the DHE or ECDHE key exchange algorithms to enable PFS support for SSL decryption, you can use a hardware security module (HSM) to store the private keys used for SSL Inbound Inspection.*	• DHE-RSA-3DES-EDE-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-1 • DHE-RSA-AES-256-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-256 • DHE-RSA-AES-256-CBC-SHA-256 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-CBC-SHA-1 • ECDHE-RSA-AES-256-CBC-SHA-1 • ECDHE-RSA-AES-128-CBC-SHA-256 • ECDHE-RSA-AES-256-CBC-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-CBC-SHA-1 • ECDHE-ECDSA-AES-256-CBC-SHA-1 • ECDHE-ECDSA-AES-128-CBC-SHA-256 • ECDHE-ECDSA-AES-256-CBC-SHA-384 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384 • (TLS 1.3 only) TLS_AES_128_GCM_SHA-256 • (TLS 1.3 only) TLS_AES_256_GCM_SHA-384 • (TLS 1.3 only) TLS_CHACHA20_POLY1305_SHA-256
TLS 1.3 Decryption—Signature Algorithms	• ECDSA-SECP256r1-SHA-256 • RSA-PSS-RSAE-SHA-256 • RSA-PKCS1-SHA-256 • ECDSA-SECP384r1-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 11.2 Releases
	• RSA-PSS-RSAE-SHA-384 • RSA-PKCS1-SHA-386 • RSA-PSS-RSAE-SHA-512 • RSA-PKCS1-SHA-512 • RSA-PKCS1-SHA-1

PAN-OS 11.2 Administrative Session Cipher Suites

The following table lists the cipher suites for administrative sessions that are supported on firewalls running a PAN-OS® 11.2 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.2 Cipher Suites Supported in FIPS-CC Mode.

- Administrative Sessions to Web Interface
- Administrative Sessions to CLI (SSH)—Encryption
- Administrative Sessions to CLI (SSH)—Message Authentication
- Administrative Sessions to CLI (SSH)—Server Host Key Types
- Administrative Sessions to CLI (SSH)—Key Exchange Algorithms

Feature or Function	Ciphers Supported in PAN-OS 11.2 Releases
Administrative Sessions to Web Interface	TLSv1.1, TLSv1.2, and TLSv1.3 cipher suites *TLSv1.3 cipher suites begin with "TLS".* • RSA-SEED-SHA1 • RSA-CAMELLIA-128-SHA1 • RSA-CAMELLIA-256-SHA1 • RSA-AES-128-SHA1 • RSA-AES-256-SHA1 • RSA-AES-256-CBC-SHA1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 11.2 Releases
	• ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA1 • ECDHE-ECDSA-AES-256-SHA1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384 • TLS-AES-128-CCM-SHA256 • TLS-AES-128-GCM-SHA256 • TLS-AES-256-GCM-SHA384 • TLS-CHACHA20-POLY1305-SHA256
Administrative Sessions to CLI (SSH)—Encryption	• AES-128-CTR • AES-192-CTR • AES-256-CTR • AES-128-GCM • AES-256-GCM • CHACHA20-POLY1305
Administrative Sessions to CLI (SSH)—Message Authentication	• UMAC-64 • UMAC-128 • HMAC-SHA1 • HMAC-SHA2-256 • HMAC-SHA-384 • HMAC-SHA2-512
Administrative Sessions to CLI (SSH)—Server Host Key Types	• RSA keys—2048-bit, 3072-bit, and 4096-bit keys • ECDSA keys—256-bit, 384-bit, and 521-bit keys
Administrative Sessions to CLI (SSH)—Key Exchange Algorithms	• curve25519-sha256 • diffie-hellman-group14-sha1 • diffie-hellman-group14-sha256 • diffie-hellman-group14-sha384 • diffie-hellman-group16-sha512 • diffie-hellman-group-exchange-sha256 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384

Feature or Function	Ciphers Supported in PAN-OS 11.2 Releases
	• ecdh-sha2-nistp521

PAN-OS 11.2 HA1 SSH Cipher Suites

The following table lists the cipher suites for HA1 control connections using SSH that are supported on firewalls running a PAN-OS® 11.2 release in normal (non-FIPS-CC) or FIPS-CC operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.2 Cipher Suites Supported in FIPS-CC Mode.

Feature or Function	Ciphers Supported in PAN-OS 11.2 Releases
HA1 SSH	• AES 128-bit cipher with Counter Mode • AES 128-bit cipher with GCM (Galois/Counter Mode) • AES 192-bit cipher with Counter Mode • AES 256-bit cipher with Counter Mode • AES 256-bit cipher with GCM • CHACHA20-POLY1305

PAN-OS 11.2 PAN-OS-to-Panorama Connection Cipher Suites

The following table lists the cipher suites for PAN-OS®-to-Panorama™ connections that are supported on firewalls running a PAN-OS 11.2 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.2 Cipher Suites Supported in FIPS-CC Mode.

Feature or Function	Ciphers Supported in PAN-OS 11.2 Releases
PAN-OS to Panorama Connection	• RSA-RC4-128-SHA-1 • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-1 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 11.2 Releases
	• DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1

PAN-OS 11.2 Cipher Suites Supported in FIPS-CC Mode

The following table lists cipher suites that are supported on firewalls running a PAN-OS® 11.2 release in FIPS-CC mode. The Cryptographic Algorithm Validation Program has additional details regarding the algorithm implementation.

If your firewall is running in normal (non-FIPS-CC) operational mode, see Cipher Suites Supported in PAN-OS 11.2

Functions	Standards	Certificates
Asymmetric key generation		
ECC key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	**Appliances:** <TBD> **VMs:** <TBD>
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	**Appliances:** <TBD> **VMs:** <TBD>
Cryptographic Key Generation (for IKE Peer Authentication)		
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	**Appliances:** <TBD> **VMs:** <TBD>
ECDSA key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	**Appliances:** <TBD> **VMs:** <TBD>
Cryptographic Key Establishment		

Functions	Standards	Certificates
ECC-based key establishment	SP 800-56A Revision 3	**Appliances:** <TBD> **VMs:** <TBD>
FFC-based key establishment	SP 800-56A Revision 3	**Appliances:** <TBD> **VMs:** <TBD>
AES Data Encryption/Decryption		
• AES CTR 128/192/256 • AES CBC 128/192/256 • AES GCM 128/256 • AES CCM 128	• AES as specified in ISO 18033-3 • CBC/CTR as specified in ISO 10116 • GCM as specified in ISO 19772 • NIST SP 800-38A/C/D/F • FIPS PUB 197	**Appliances:** <TBD> **VMs:** <TBD>
Signature Generation and Verification		
RSA (2048 bits or greater)	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSAPKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	**Appliances:** <TBD> **VMs:** <TBD>
ECDSA (NIST curves P-256, P-384, and P-521)	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing "NIST	**Appliances:** <TBD> **VMs:**

Functions	Standards	Certificates
	curves" P-256, P-384, P-521 ISO/IEC 14888-3, Section 6.4	<TBD>
Cryptographic hashing		
SHA-1, SHA-256, SHA-384 and SHA-512 (digest sizes 160, 256, 384 and 512 bits)	ISO/IEC 10118-3:2004 FIPS PUB 180-4	**Appliances:** <TBD> **VMs:** <TBD>
Keyed-hash message authentication		
• HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512	ISO/IEC 9797-2:2011 FIPS PUB 198-1	**Appliances:** <TBD> **VMs:** <TBD>
Random bit generation		
CTR_DRBG (AES-256)	ISO/IEC 18031:2011 NIST SP 800-90A	**Appliances:** <TBD> **VMs:** <TBD>

Cipher Suites Supported in PAN-OS 11.1

The following topics list cipher suites that are supported on firewalls running a PAN-OS® 11.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.1 Cipher Suites Supported in FIPS-CC Mode.

The ciphers supported in normal operation mode are grouped according to feature or functionality in the following sections:

- PAN-OS 11.1 GlobalProtect Cipher Suites
- PAN-OS 11.1 IPSec Cipher Suites
- PAN-OS 11.1 IKE and Web Certificate Cipher Suites
- PAN-OS 11.1 Decryption Cipher Suites
- PAN-OS 11.1 HA1 SSH Cipher Suites
- PAN-OS 11.1 Administrative Session Cipher Suites
- PAN-OS 11.1 PAN-OS-to-Panorama Connection Cipher Suites

PAN-OS 11.1 GlobalProtect Cipher Suites

The following table lists cipher suites for GlobalProtect™ supported on firewalls running a PAN-OS® 11.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.1 Cipher Suites Supported in FIPS-CC Mode.

- GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal
- GlobalProtect App/Agent—IPSec mode
- GlobalProtect Portal—Browser Access

Feature or Function	Ciphers Supported in PAN-OS 11.1 Releases
GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal	• TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 11.1 Releases
	• RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-SEED-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA-1 • ECDHE-RSA-AES-128-SHA-1 • ECDHE-RSA-AES-256-SHA-1 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-128-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384 • TLS-AES-128-GCM-SHA256 • TLS-AES-256-GCM-SHA384 • TLS-CHACHA20-POLY1305-SHA256
GlobalProtect App/Agent—IPSec mode (Keys transported through SSL session with gateway)	• AES-128-CBC-HMAC-SHA-1 • AES-128-GCM-HMAC-SHA-1 • AES-256-GCM-HMAC-SHA-1
GlobalProtect Portal—Browser Access	• SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 11.1 Releases
	• DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA-1 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384

PAN-OS 11.1 IPSec Cipher Suites

The following table lists the cipher suites for IPSec that are supported on firewalls running a PAN-OS® 11.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.1 Cipher Suites Supported in FIPS-CC Mode.

- IPSec—Encryption
- IPSec—Message Authentication
- IPSec—Key Exchange

Feature or Function	Ciphers Supported in PAN-OS 11.1 Releases
IPSec—Encryption	• NULL • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CCM • AES-128-GCM • AES-256-GCM
IPSec—Message Authentication	• NONE • HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 11.1 Releases
	• HMAC-SHA-512
IPSec—Key Exchange	Diffie-Hellman groups with or without perfect forward secrecy (PFS): • No PFS—This option specifies that the firewall reuses the same key for IKE phase 1 and phase 2 instead of renewing the key for phase 2. • Group 1 (768-bit keys) with PFS enabled • Group 2 (1024-bit keys) with PFS enabled • Group 5 (1536-bit keys) with PFS enabled • Group 14 (2048-bit keys) with PFS enabled • Group 15 (3072-bit modular exponential group) • Group 16 (4096-bit modular exponential group) • Group 19 (256-bit elliptic curve group) with PFS enabled • Group 20 (384-bit elliptic curve group) with PFS enabled • Group 21 (512-bit random elliptic curve group)

PAN-OS 11.1 IKE and Web Certificate Cipher Suites

The following table lists cipher suites for Internet Key Exchange (IKE) and PAN-OS® web certificates that are supported on firewalls running a PAN-OS 11.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.1 Cipher Suites Supported in FIPS-CC Mode.

- IKE Certificate Support
- IKE—Encryption
- IKE—Message Authentication
- IKE—Key Exchange
- PAN-OS Web Certificates

Feature or Function	Ciphers Supported in PAN-OS 11.1 Releases

IKE Certificate Support	• RSA
	  • Keys—512-bit, 1024-bit, 2048-bit, and 3072-bit keys
	  • Digital signature algorithms—SHA-1, SHA-256, SHA-384, or SHA-512

Feature or Function	Ciphers Supported in PAN-OS 11.1 Releases

	• ECDSA
	  • Keys—256-bit and 384-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

IKE—Encryption	• 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC **Starting with PAN-OS 10.0.3:** • AES-128-GCM • AES-256-GCM
IKE—Message Authentication	• HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IKE—Key Exchange	Diffie-Hellman groups • Group 1 (768-bit keys) • Group 2 (1024-bit keys) • Group 5 (1536-bit keys) • Group 14 (2048-bit keys) • Group 15 (3072-bit modular exponential group) • Group 16 (4096-bit modular exponential group) • Group 19 (256-bit elliptic curve group) • Group 20 (384-bit elliptic curve group) • Group 21 (512-bit random elliptic curve group)

PAN-OS Web Certificates	• RSA
	  • Keys—2048-bit, 3072-bit, and 4096-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

Feature or Function	Ciphers Supported in PAN-OS 11.1 Releases

	• ECDSA
	  • Keys—256-bit and 384-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

PAN-OS 11.1 Decryption Cipher Suites

The following table lists cipher suites for decryption that are supported on firewalls running a PAN-OS® 11.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.1 Cipher Suites Supported in FIPS-CC Mode.

- SSH Decryption—Host Key Algorithms
- SSH Decryption (SSHv2 only)—Encryption
- SSH Decryption (SSHv2 only)—Message Authentication
- SSL/TLS Decryption
- SSL/TLS Decryption—NIST-approved Elliptical Curves
- SSL/TLS Decryption—Perfect Forward Secrecy (PFS) Ciphers
- TLS 1.3 Decryption—Signature Algorithms

Feature or Function	Ciphers Supported in PAN-OS 11.1 Releases
SSH Decryption—Host Key Algorithms	• SSH-RSA (2048-bit) • SSH-DSS (2048-bit)
SSH Decryption (SSHv2 only)—Encryption	• AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR • AES-256-CTR
SSH Decryption (SSHv2 only)—Message Authentication	• HMAC-RIPEMD • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-1-96 • HMAC-RIPEMD-160

Feature or Function	Ciphers Supported in PAN-OS 11.1 Releases
	• HMAC-SHA-1
SSL/TLS Decryption	• SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3 cipher suites • RSA 512-bit, 1024-bit, 2048-bit, 3072-bit, 4096-bit, and 8192-bit keys *The firewall can authenticate certificates up to 8192-bit RSA keys from the destination server, however the firewall generated certificate to the client supports only up to 4096-bit RSA keys.* • RSA-RC4-128-MD5 • RSA-RC4-128-SHA-1 • RSA-3DES-EDE-CBC-SHA-1 • RSA-AES-128-CBC-SHA-1 • RSA-AES-256-CBC-SHA-1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • TLS_AES_256_GCM_SHA-384 • TLS_CHACHA20_POLY1305_SHA-256 • TLS_AES_128_GCM_SHA-256
SSL/TLS Decryption—NIST-approved Elliptical Curves	• P-192 (secp192r1) • P-224 (secp224r1) • P-256 (secp256r1) • P-384 (secp384r1) • P-521 (secp521r1) • (TLS 1.3 only) X25519 • (TLS 1.3 only) X448
SSL/TLS Decryption—Perfect Forward Secrecy (PFS) Ciphers	• DHE-RSA-3DES-EDE-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-1 • DHE-RSA-AES-256-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 11.1 Releases
If you use the DHE or ECDHE key exchange algorithms to enable PFS support for SSL decryption, you can use a hardware security module (HSM) to store the private keys used for SSL Inbound Inspection.	• DHE-RSA-AES-256-CBC-SHA-256 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-CBC-SHA-1 • ECDHE-RSA-AES-256-CBC-SHA-1 • ECDHE-RSA-AES-128-CBC-SHA-256 • ECDHE-RSA-AES-256-CBC-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-CBC-SHA-1 • ECDHE-ECDSA-AES-256-CBC-SHA-1 • ECDHE-ECDSA-AES-128-CBC-SHA-256 • ECDHE-ECDSA-AES-256-CBC-SHA-384 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384 • (TLS 1.3 only) TLS_AES_128_GCM_SHA-256 • (TLS 1.3 only) TLS_AES_256_GCM_SHA-384 • (TLS 1.3 only) TLS_CHACHA20_POLY1305_SHA-256
TLS 1.3 Decryption—Signature Algorithms	• ECDSA-SECP256r1-SHA-256 • RSA-PSS-RSAE-SHA-256 • RSA-PKCS1-SHA-256 • ECDSA-SECP384r1-SHA-384 • RSA-PSS-RSAE-SHA-384 • RSA-PKCS1-SHA-386 • RSA-PSS-RSAE-SHA-512 • RSA-PKCS1-SHA-512 • RSA-PKCS1-SHA-1

PAN-OS 11.1 Administrative Session Cipher Suites

The following table lists the cipher suites for administrative sessions that are supported on firewalls running a PAN-OS® 11.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.1 Cipher Suites Supported in FIPS-CC Mode.

- Administrative Sessions to Web Interface

- Administrative Sessions to CLI (SSH)—Encryption
- Administrative Sessions to CLI (SSH)—Message Authentication
- Administrative Sessions to CLI (SSH)—Server Host Key Types
- Administrative Sessions to CLI (SSH)—Key Exchange Algorithms

Feature or Function	Ciphers Supported in PAN-OS 11.1 Releases
Administrative Sessions to Web Interface	TLSv1.1, TLSv1.2, and TLSv1.3 cipher suites  *TLSv1.3 cipher suites begin with "TLS".* • RSA-SEED-SHA1 • RSA-CAMELLIA-128-SHA1 • RSA-CAMELLIA-256-SHA1 • RSA-AES-128-SHA1 • RSA-AES-256-SHA1 • RSA-AES-256-CBC-SHA1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA1 • ECDHE-ECDSA-AES-256-SHA1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384 • TLS-AES-128-CCM-SHA256 • TLS-AES-128-GCM-SHA256 • TLS-AES-256-GCM-SHA384 • TLS-CHACHA20-POLY1305-SHA256
Administrative Sessions to CLI (SSH)—Encryption	• AES-128-CTR • AES-192-CTR • AES-256-CTR • AES-128-GCM

Feature or Function	Ciphers Supported in PAN-OS 11.1 Releases
	• AES-256-GCM • CHACHA20-POLY1305
Administrative Sessions to CLI (SSH)—Message Authentication	• UMAC-64 • UMAC-128 • HMAC-SHA1 • HMAC-SHA2-256 • HMAC-SHA-384 • HMAC-SHA2-512
Administrative Sessions to CLI (SSH)—Server Host Key Types	• RSA keys—2048-bit, 3072-bit, and 4096-bit keys • ECDSA keys—256-bit, 384-bit, and 521-bit keys
Administrative Sessions to CLI (SSH)—Key Exchange Algorithms	• curve25519-sha256 • diffie-hellman-group14-sha1 • diffie-hellman-group14-sha256 • diffie-hellman-group14-sha384 • diffie-hellman-group16-sha512 • diffie-hellman-group-exchange-sha256 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521

PAN-OS 11.1 HA1 SSH Cipher Suites

The following table lists the cipher suites for HA1 control connections using SSH that are supported on firewalls running a PAN-OS® 11.1 release in normal (non-FIPS-CC) or FIPS-CC operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.1 Cipher Suites Supported in FIPS-CC Mode.

Feature or Function	Ciphers Supported in PAN-OS 11.1 Releases
HA1 SSH	• AES 128-bit cipher with Counter Mode • AES 128-bit cipher with GCM (Galois/Counter Mode) • AES 192-bit cipher with Counter Mode • AES 256-bit cipher with Counter Mode

Feature or Function	Ciphers Supported in PAN-OS 11.1 Releases
	• AES 256-bit cipher with GCM • CHACHA20-POLY1305

PAN-OS 11.1 PAN-OS-to-Panorama Connection Cipher Suites

The following table lists the cipher suites for PAN-OS®-to-Panorama™ connections that are supported on firewalls running a PAN-OS 11.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.1 Cipher Suites Supported in FIPS-CC Mode.

Feature or Function	Ciphers Supported in PAN-OS 11.1 Releases
PAN-OS to Panorama Connection	• RSA-RC4-128-SHA-1 • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-1 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1

PAN-OS 11.1 Cipher Suites Supported in FIPS-CC Mode

The following table lists cipher suites that are supported on firewalls running a PAN-OS® 11.1 release in FIPS-CC mode. The Cryptographic Algorithm Validation Program has additional details regarding the algorithm implementation.

If your firewall is running in normal (non-FIPS-CC) operational mode, see Cipher Suites Supported in PAN-OS 11.1

Functions	Standards	Certificates
Asymmetric key generation		

Functions	Standards	Certificates
ECC key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	**Appliances:** #A3453 **VMs:** #A3454
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	**Appliances:** #A3453 **VMs:** #A3454
Cryptographic Key Generation (for IKE Peer Authentication)		
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	**Appliances:** #A3453 **VMs:** #A3454
ECDSA key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	**Appliances:** #A3453 **VMs:** #A3454
Cryptographic Key Establishment		
ECC-based key establishment	SP 800-56A Revision 3	**Appliances:** #A3453 **VMs:** #A3454
FFC-based key establishment	SP 800-56A Revision 3	**Appliances:** #A3453 **VMs:** #A3454
AES Data Encryption/Decryption		
• AES CTR 128/192/256 • AES CBC 128/192/256	• AES as specified in ISO 18033-3	**Appliances:**

Functions	Standards	Certificates
• AES GCM 128/256 • AES CCM 128	• CBC/CTR as specified in ISO 10116 • GCM as specified in ISO 19772 • NIST SP 800-38A/C/D/F • FIPS PUB 197	#A3453 **VMs:** #A3454
Signature Generation and Verification		
RSA (2048 bits or greater)	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSAPKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	**Appliances:** #A3453 **VMs:** #A3454
ECDSA (NIST curves P-256, P-384, and P-521)	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing "NIST curves" P-256, P-384, P-521 ISO/IEC 14888-3, Section 6.4	**Appliances:** #A3453 **VMs:** #A3454
Cryptographic hashing		
SHA-1, SHA-256, SHA-384 and SHA-512 (digest sizes 160, 256, 384 and 512 bits)	ISO/IEC 10118-3:2004 FIPS PUB 180-4	**Appliances:** #A3453 **VMs:** #A3454
Keyed-hash message authentication		
• HMAC-SHA-1 • HMAC-SHA-256	ISO/IEC 9797-2:2011 FIPS PUB 198-1	**Appliances:** #A3453

Functions	Standards	Certificates
• HMAC-SHA-384 • HMAC-SHA-512		**VMs:** #A3454
Random bit generation		
CTR_DRBG (AES-256)	ISO/IEC 18031:2011 NIST SP 800-90A	**Appliances:** #A3453 **VMs:** #A3454

Cipher Suites Supported in PAN-OS 11.0

The following topics list cipher suites that are supported on firewalls running a PAN-OS® 11.0 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode.

The ciphers supported in normal operation mode are grouped according to feature or functionality in the following sections:

- PAN-OS 11.0 GlobalProtect Cipher Suites
- PAN-OS 11.0 IPSec Cipher Suites
- PAN-OS 11.0 IKE and Web Certificate Cipher Suites
- PAN-OS 11.0 Decryption Cipher Suites
- PAN-OS 11.0 HA1 SSH Cipher Suites
- PAN-OS 11.0 Administrative Session Cipher Suites
- PAN-OS 11.0 PAN-OS-to-Panorama Connection Cipher Suites

PAN-OS 11.0 GlobalProtect Cipher Suites

The following table lists cipher suites for GlobalProtect™ supported on firewalls running a PAN-OS® 11.0 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode.

- GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal
- GlobalProtect App/Agent—IPSec mode
- GlobalProtect Portal—Browser Access

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal	• TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
	• RSA-AES-256-GCM-SHA-384 • DHE-RSA-SEED-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA-1 • ECDHE-RSA-AES-128-SHA-1 • ECDHE-RSA-AES-256-SHA-1 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-128-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
GlobalProtect App/Agent—IPSec mode (Keys transported through SSL session with gateway)	• AES-128-CBC-HMAC-SHA-1 • AES-128-GCM-HMAC-SHA-1 • AES-256-GCM-HMAC-SHA-1
GlobalProtect Portal—Browser Access	• SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
	• EDH-RSA-3DES-SHA-1 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384

PAN-OS 11.0 IPSec Cipher Suites

The following table lists the cipher suites for IPSec that are supported on firewalls running a PAN-OS® 11.0 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode.

- IPSec—Encryption
- IPSec—Message Authentication
- IPSec—Key Exchange

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
IPSec—Encryption	• NULL • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CCM • AES-128-GCM • AES-256-GCM
IPSec—Message Authentication	• NONE • HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IPSec—Key Exchange	Diffie-Hellman groups with or without perfect forward secrecy (PFS):

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
	• No PFS—This option specifies that the firewall reuses the same key for IKE phase 1 and phase 2 instead of renewing the key for phase 2. • Group 1 (768-bit keys) with PFS enabled • Group 2 (1024-bit keys) with PFS enabled • Group 5 (1536-bit keys) with PFS enabled • Group 14 (2048-bit keys) with PFS enabled • Group 15 (3072-bit modular exponential group) • Group 16 (4096-bit modular exponential group) • Group 19 (256-bit elliptic curve group) with PFS enabled • Group 20 (384-bit elliptic curve group) with PFS enabled • Group 21 (512-bit random elliptic curve group)

PAN-OS 11.0 IKE and Web Certificate Cipher Suites

The following table lists cipher suites for Internet Key Exchange (IKE) and PAN-OS® web certificates that are supported on firewalls running a PAN-OS 11.0 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode.

- IKE Certificate Support
- IKE—Encryption
- IKE—Message Authentication
- IKE—Key Exchange
- PAN-OS Web Certificates

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases

IKE Certificate Support	• RSA
	  • Keys—512-bit, 1024-bit, 2048-bit, and 3072-bit keys
	  • Digital signature algorithms—SHA-1, SHA-256, SHA-384, or SHA-512
	• ECDSA
	  • Keys—256-bit and 384-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
IKE—Encryption	• 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC **Starting with PAN-OS 10.0.3:** • AES-128-GCM • AES-256-GCM
IKE—Message Authentication	• HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IKE—Key Exchange	Diffie-Hellman groups • Group 1 (768-bit keys) • Group 2 (1024-bit keys) • Group 5 (1536-bit keys) • Group 14 (2048-bit keys) • Group 15 (3072-bit modular exponential group) • Group 16 (4096-bit modular exponential group) • Group 19 (256-bit elliptic curve group) • Group 20 (384-bit elliptic curve group) • Group 21 (512-bit random elliptic curve group)

PAN-OS Web Certificates	• RSA
	  • Keys—2048-bit, 3072-bit, and 4096-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512
	• ECDSA
	  • Keys—256-bit and 384-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

PAN-OS 11.0 Decryption Cipher Suites

The following table lists cipher suites for decryption that are supported on firewalls running a PAN-OS® 11.0 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode.

- SSH Decryption—Host Key Algorithms
- SSH Decryption (SSHv2 only)—Encryption
- SSH Decryption (SSHv2 only)—Message Authentication
- SSL/TLS Decryption
- SSL/TLS Decryption—NIST-approved Elliptical Curves
- SSL/TLS Decryption—Perfect Forward Secrecy (PFS) Ciphers
- TLS 1.3 Decryption—Signature Algorithms

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
SSH Decryption—Host Key Algorithms	• SSH-RSA (2048-bit) • SSH-DSS (2048-bit)
SSH Decryption (SSHv2 only)—Encryption	• AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR • AES-256-CTR
SSH Decryption (SSHv2 only)—Message Authentication	• HMAC-RIPEMD • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-1-96 • HMAC-RIPEMD-160 • HMAC-SHA-1
SSL/TLS Decryption	• SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3 cipher suites

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
	• RSA 512-bit, 1024-bit, 2048-bit, 3072-bit, 4096-bit, and 8192-bit keys *The firewall can authenticate certificates up to 8192-bit RSA keys from the destination server, however the firewall generated certificate to the client supports only up to 4096-bit RSA keys.* • RSA-RC4-128-MD5 • RSA-RC4-128-SHA-1 • RSA-3DES-EDE-CBC-SHA-1 • RSA-AES-128-CBC-SHA-1 • RSA-AES-256-CBC-SHA-1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • TLS_AES_256_GCM_SHA-384 • TLS_CHACHA20_POLY1305_SHA-256 • TLS_AES_128_GCM_SHA-256
SSL/TLS Decryption—NIST-approved Elliptical Curves	• P-192 (secp192r1) • P-224 (secp224r1) • P-256 (secp256r1) • P-384 (secp384r1) • P-521 (secp521r1) • (TLS 1.3 only) X25519 • (TLS 1.3 only) X448
SSL/TLS Decryption—Perfect Forward Secrecy (PFS) Ciphers	• DHE-RSA-3DES-EDE-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-1 • DHE-RSA-AES-256-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
If you use the DHE or ECDHE key exchange algorithms to enable PFS support for SSL decryption, you can use a hardware security module (HSM) to store the private keys used for SSL Inbound Inspection.	• DHE-RSA-AES-256-CBC-SHA-256 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-CBC-SHA-1 • ECDHE-RSA-AES-256-CBC-SHA-1 • ECDHE-RSA-AES-128-CBC-SHA-256 • ECDHE-RSA-AES-256-CBC-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-CBC-SHA-1 • ECDHE-ECDSA-AES-256-CBC-SHA-1 • ECDHE-ECDSA-AES-128-CBC-SHA-256 • ECDHE-ECDSA-AES-256-CBC-SHA-384 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384 • (TLS 1.3 only) TLS_AES_128_GCM_SHA-256 • (TLS 1.3 only) TLS_AES_256_GCM_SHA-384 • (TLS 1.3 only) TLS_CHACHA20_POLY1305_SHA-256
TLS 1.3 Decryption—Signature Algorithms	• ECDSA-SECP256r1-SHA-256 • RSA-PSS-RSAE-SHA-256 • RSA-PKCS1-SHA-256 • ECDSA-SECP384r1-SHA-384 • RSA-PSS-RSAE-SHA-384 • RSA-PKCS1-SHA-386 • RSA-PSS-RSAE-SHA-512 • RSA-PKCS1-SHA-512 • RSA-PKCS1-SHA-1

PAN-OS 11.0 Administrative Session Cipher Suites

The following table lists the cipher suites for administrative sessions that are supported on firewalls running a PAN-OS® 11.0 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode.

- Administrative Sessions to Web Interface

- Administrative Sessions to CLI (SSH)—Encryption
- Administrative Sessions to CLI (SSH)—Message Authentication
- Administrative Sessions to CLI (SSH)—Server Host Key Types
- Administrative Sessions to CLI (SSH)—Key Exchange Algorithms

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
Administrative Sessions to Web Interface	TLSv1.1, TLSv1.2, and TLSv1.3 cipher suites  *TLSv1.3 cipher suites begin with "TLS".* • RSA-SEED-SHA1 • RSA-CAMELLIA-128-SHA1 • RSA-CAMELLIA-256-SHA1 • RSA-AES-128-SHA1 • RSA-AES-256-SHA1 • RSA-AES-256-CBC-SHA1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA1 • ECDHE-ECDSA-AES-256-SHA1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384 • TLS-AES-128-CCM-SHA256 • TLS-AES-128-GCM-SHA256 • TLS-AES-256-GCM-SHA384 • TLS-CHACHA20-POLY1305-SHA256
Administrative Sessions to CLI (SSH)—Encryption	• AES-128-CTR • AES-192-CTR • AES-256-CTR • AES-128-GCM

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
	• AES-256-GCM • CHACHA20-POLY1305
Administrative Sessions to CLI (SSH)—Message Authentication	• UMAC-64 • UMAC-128 • HMAC-SHA1 • HMAC-SHA2-256 • HMAC-SHA-384 • HMAC-SHA2-512
Administrative Sessions to CLI (SSH)—Server Host Key Types	• RSA keys—2048-bit, 3072-bit, and 4096-bit keys • ECDSA keys—256-bit, 384-bit, and 521-bit keys
Administrative Sessions to CLI (SSH)—Key Exchange Algorithms	• curve25519-sha256 • diffie-hellman-group14-sha1 • diffie-hellman-group14-sha256 • diffie-hellman-group14-sha384 • diffie-hellman-group16-sha512 • diffie-hellman-group-exchange-sha256 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521

PAN-OS 11.0 HA1 SSH Cipher Suites

The following table lists the cipher suites for HA1 control connections using SSH that are supported on firewalls running a PAN-OS® 11.0 release in normal (non-FIPS-CC) or FIPS-CC operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode.

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
HA1 SSH	• AES 128-bit cipher with Counter Mode • AES 128-bit cipher with GCM (Galois/Counter Mode) • AES 192-bit cipher with Counter Mode • AES 256-bit cipher with Counter Mode

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
	• AES 256-bit cipher with GCM • CHACHA20-POLY1305

PAN-OS 11.0 PAN-OS-to-Panorama Connection Cipher Suites

The following table lists the cipher suites for PAN-OS®-to-Panorama™ connections that are supported on firewalls running a PAN-OS 11.0 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode.

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
PAN-OS to Panorama Connection	• RSA-RC4-128-SHA-1 • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-1 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1

PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode

The following table lists cipher suites that are supported on firewalls running a PAN-OS® 11.0 release in FIPS-CC mode. The Cryptographic Algorithm Validation Program has additional details regarding the algorithm implementation.

If your firewall is running in normal (non-FIPS-CC) operational mode, see Cipher Suites Supported in PAN-OS 11.0

Functions	Standards	Certificates
Asymmetric key generation		

Functions	Standards	Certificates
ECC key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	**Appliances:** #A3453 **VMs:** #A3454
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	**Appliances:** #A3453 **VMs:** #A3454
Cryptographic Key Generation (for IKE Peer Authentication)		
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	**Appliances:** #A3453 **VMs:** #A3454
ECDSA key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	**Appliances:** #A3453 **VMs:** #A3454
Cryptographic Key Establishment		
ECC-based key establishment	SP 800-56A Revision 3	**Appliances:** #A3453 **VMs:** #A3454
FFC-based key establishment	SP 800-56A Revision 3	**Appliances:** #A3453 **VMs:** #A3454
AES Data Encryption/Decryption		
• AES CTR 128/192/256 • AES CBC 128/192/256	• AES as specified in ISO 18033-3	**Appliances:**

Functions	Standards	Certificates
• AES GCM 128/256 • AES CCM 128	• CBC/CTR as specified in ISO 10116 • GCM as specified in ISO 19772 • NIST SP 800-38A/C/D/F • FIPS PUB 197	#A3453 **VMs:** #A3454
Signature Generation and Verification		
RSA (2048 bits or greater)	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSAPKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	**Appliances:** #A3453 **VMs:** #A3454
ECDSA (NIST curves P-256, P-384, and P-521)	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing "NIST curves" P-256, P-384, P-521 ISO/IEC 14888-3, Section 6.4	**Appliances:** #A3453 **VMs:** #A3454
Cryptographic hashing		
SHA-1, SHA-256, SHA-384 and SHA-512 (digest sizes 160, 256, 384 and 512 bits)	ISO/IEC 10118-3:2004 FIPS PUB 180-4	**Appliances:** #A3453 **VMs:** #A3454
Keyed-hash message authentication		
• HMAC-SHA-1 • HMAC-SHA-256	ISO/IEC 9797-2:2011 FIPS PUB 198-1	**Appliances:** #A3453

Functions	Standards	Certificates
• HMAC-SHA-384 • HMAC-SHA-512		**VMs:** #A3454
Random bit generation		
CTR_DRBG (AES-256)	ISO/IEC 18031:2011 NIST SP 800-90A	**Appliances:** #A3453 **VMs:** #A3454

Cipher Suites Supported in PAN-OS 10.2

The following topics list cipher suites that are supported on firewalls running a PAN-OS® 10.2 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode.

The ciphers supported in normal operation mode are grouped according to feature or functionality in the following sections:

- PAN-OS 10.2 GlobalProtect Cipher Suites
- PAN-OS 10.2 IPSec Cipher Suites
- PAN-OS 10.2 IKE and Web Certificate Cipher Suites
- PAN-OS 10.2 Decryption Cipher Suites
- PAN-OS 10.2 HA1 SSH Cipher Suites
- PAN-OS 10.2 Administrative Session Cipher Suites
- PAN-OS 10.2 PAN-OS-to-Panorama Connection Cipher Suites

PAN-OS 10.2 GlobalProtect Cipher Suites

The following table lists cipher suites for GlobalProtect™ supported on firewalls running a PAN-OS® 10.2 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode.

- GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal
- GlobalProtect App/Agent—IPSec mode
- GlobalProtect Portal—Browser Access

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal	• TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
	• RSA-AES-256-GCM-SHA-384 • DHE-RSA-SEED-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA-1 • ECDHE-RSA-AES-128-SHA-1 • ECDHE-RSA-AES-256-SHA-1 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-128-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
GlobalProtect App/Agent—IPSec mode (Keys transported through SSL session with gateway)	• AES-128-CBC-HMAC-SHA-1 • AES-128-GCM-HMAC-SHA-1 • AES-256-GCM-HMAC-SHA-1
GlobalProtect Portal—Browser Access	• SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
	• EDH-RSA-3DES-SHA-1 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384

PAN-OS 10.2 IPSec Cipher Suites

The following table lists the cipher suites for IPSec that are supported on firewalls running a PAN-OS® 10.2 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode.

- IPSec—Encryption
- IPSec—Message Authentication
- IPSec—Key Exchange

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
IPSec—Encryption	• NULL • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CCM • AES-128-GCM • AES-256-GCM
IPSec—Message Authentication	• NONE • HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IPSec—Key Exchange	Diffie-Hellman groups with or without perfect forward secrecy (PFS):

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
	• No PFS—This option specifies that the firewall reuses the same key for IKE phase 1 and phase 2 instead of renewing the key for phase 2. • Group 1 (768-bit keys) with PFS enabled • Group 2 (1024-bit keys) with PFS enabled • Group 5 (1536-bit keys) with PFS enabled • Group 14 (2048-bit keys) with PFS enabled • Group 15 (3072-bit modular exponential group) • Group 16 (4096-bit modular exponential group) • Group 19 (256-bit elliptic curve group) with PFS enabled • Group 20 (384-bit elliptic curve group) with PFS enabled • Group 21 (512-bit random elliptic curve group)

PAN-OS 10.2 IKE and Web Certificate Cipher Suites

The following table lists cipher suites for Internet Key Exchange (IKE) and PAN-OS® web certificates that are supported on firewalls running a PAN-OS 10.2 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode.

- IKE Certificate Support
- IKE—Encryption
- IKE—Message Authentication
- IKE—Key Exchange
- PAN-OS Web Certificates

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases

IKE Certificate Support	• RSA
	  • Keys—512-bit, 1024-bit, 2048-bit, and 3072-bit keys
	  • Digital signature algorithms—SHA-1, SHA-256, SHA-384, or SHA-512
	• ECDSA
	  • Keys—256-bit and 384-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
IKE—Encryption	• 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC **Starting with PAN-OS 10.0.3:** • AES-128-GCM • AES-256-GCM
IKE—Message Authentication	• HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IKE—Key Exchange	Diffie-Hellman groups • Group 1 (768-bit keys) • Group 2 (1024-bit keys) • Group 5 (1536-bit keys) • Group 14 (2048-bit keys) • Group 15 (3072-bit modular exponential group) • Group 16 (4096-bit modular exponential group) • Group 19 (256-bit elliptic curve group) • Group 20 (384-bit elliptic curve group) • Group 21 (512-bit random elliptic curve group)

PAN-OS Web Certificates	• RSA
	  • Keys—2048-bit, 3072-bit, and 4096-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512
	• ECDSA
	  • Keys—256-bit and 384-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

PAN-OS 10.2 Decryption Cipher Suites

The following table lists cipher suites for decryption that are supported on firewalls running a PAN-OS® 10.2 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode.

- SSH Decryption—Host Key Algorithms
- SSH Decryption (SSHv2 only)—Encryption
- SSH Decryption (SSHv2 only)—Message Authentication
- SSL/TLS Decryption
- SSL/TLS Decryption—NIST-approved Elliptical Curves
- SSL/TLS Decryption—Perfect Forward Secrecy (PFS) Ciphers
- TLS 1.3 Decryption—Signature Algorithms

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
SSH Decryption—Host Key Algorithms	• SSH-RSA (2048-bit) • SSH-DSS (2048-bit)
SSH Decryption (SSHv2 only)—Encryption	• AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR • AES-256-CTR
SSH Decryption (SSHv2 only)—Message Authentication	• HMAC-RIPEMD • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-1-96 • HMAC-RIPEMD-160 • HMAC-SHA-1
SSL/TLS Decryption	• SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3 cipher suites

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
	• RSA 512-bit, 1024-bit, 2048-bit, 3072-bit, 4096-bit, and 8192-bit keys *The firewall can authenticate certificates up to 8192-bit RSA keys from the destination server, however the firewall generated certificate to the client supports only up to 4096-bit RSA keys.* • RSA-RC4-128-MD5 • RSA-RC4-128-SHA-1 • RSA-3DES-EDE-CBC-SHA-1 • RSA-AES-128-CBC-SHA-1 • RSA-AES-256-CBC-SHA-1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • TLS_AES_256_GCM_SHA-384 • TLS_CHACHA20_POLY1305_SHA-256 • TLS_AES_128_GCM_SHA-256
SSL/TLS Decryption—NIST-approved Elliptical Curves	• P-192 (secp192r1) • P-224 (secp224r1) • P-256 (secp256r1) • P-384 (secp384r1) • P-521 (secp521r1) • (TLS 1.3 only) X25519 • (TLS 1.3 only) X448
SSL/TLS Decryption—Perfect Forward Secrecy (PFS) Ciphers	• DHE-RSA-3DES-EDE-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-1 • DHE-RSA-AES-256-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
If you use the DHE or ECDHE key exchange algorithms to enable PFS support for SSL decryption, you can use a hardware security module (HSM) to store the private keys used for SSL Inbound Inspection.	• DHE-RSA-AES-256-CBC-SHA-256 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-CBC-SHA-1 • ECDHE-RSA-AES-256-CBC-SHA-1 • ECDHE-RSA-AES-128-CBC-SHA-256 • ECDHE-RSA-AES-256-CBC-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-CBC-SHA-1 • ECDHE-ECDSA-AES-256-CBC-SHA-1 • ECDHE-ECDSA-AES-128-CBC-SHA-256 • ECDHE-ECDSA-AES-256-CBC-SHA-384 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384 • (TLS 1.3 only) TLS_AES_128_GCM_SHA-256 • (TLS 1.3 only) TLS_AES_256_GCM_SHA-384 • (TLS 1.3 only) TLS_CHACHA20_POLY1305_SHA-256
TLS 1.3 Decryption—Signature Algorithms	• ECDSA-SECP256r1-SHA-256 • RSA-PSS-RSAE-SHA-256 • RSA-PKCS1-SHA-256 • ECDSA-SECP384r1-SHA-384 • RSA-PSS-RSAE-SHA-384 • RSA-PKCS1-SHA-386 • RSA-PSS-RSAE-SHA-512 • RSA-PKCS1-SHA-512 • RSA-PKCS1-SHA-1

PAN-OS 10.2 Administrative Session Cipher Suites

The following table lists the cipher suites for administrative sessions that are supported on firewalls running a PAN-OS® 10.2 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode.

- Administrative Sessions to Web Interface

- Administrative Sessions to CLI (SSH)—Encryption
- Administrative Sessions to CLI (SSH)—Message Authentication
- Administrative Sessions to CLI (SSH)—Server Host Key Types
- Administrative Sessions to CLI (SSH)—Key Exchange Algorithms

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
Administrative Sessions to Web Interface	• TLSv1.1 and TLSv1.2 cipher suites • RSA-SEED-SHA1 • RSA-CAMELLIA-128-SHA1 • RSA-CAMELLIA-256-SHA1 • RSA-AES-128-SHA1 • RSA-AES-256-SHA1 • RSA-AES-256-CBC-SHA1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA1 • ECDHE-ECDSA-AES-256-SHA1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
Administrative Sessions to CLI (SSH)—Encryption	• AES-128-CTR • AES-192-CTR • AES-256-CTR • AES-128-GCM • AES-256-GCM • CHACHA20-POLY1305
Administrative Sessions to CLI (SSH)—Message Authentication	• UMAC-64 • UMAC-128 • HMAC-SHA1 • HMAC-SHA2-256

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
	• HMAC-SHA2-512
Administrative Sessions to CLI (SSH)—Server Host Key Types	• RSA keys—2048-bit, 3072-bit, and 4096-bit keys • ECDSA keys—256-bit, 384-bit, and 521-bit keys
Administrative Sessions to CLI (SSH)—Key Exchange Algorithms	• curve25519-sha256 • diffie-hellman-group14-sha1 • diffie-hellman-group14-sha256 • diffie-hellman-group16-sha512 • diffie-hellman-group-exchange-sha256 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521

PAN-OS 10.2 HA1 SSH Cipher Suites

The following table lists the cipher suites for HA1 control connections using SSH that are supported on firewalls running a PAN-OS® 10.2 release in normal (non-FIPS-CC) or FIPS-CC operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode.

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
HA1 SSH	• AES 128-bit cipher with Counter Mode • AES 128-bit cipher with GCM (Galois/Counter Mode) • AES 192-bit cipher with Counter Mode • AES 256-bit cipher with Counter Mode • AES 256-bit cipher with GCM • CHACHA20-POLY1305

PAN-OS 10.2 PAN-OS-to-Panorama Connection Cipher Suites

The following table lists the cipher suites for PAN-OS®-to-Panorama™ connections that are supported on firewalls running a PAN-OS 10.2 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode.

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
PAN-OS to Panorama Connection	• RSA-RC4-128-SHA-1 • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-1 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1

PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode

The following table lists cipher suites that are supported on firewalls running a PAN-OS® 10.2 release in FIPS-CC mode. The Cryptographic Algorithm Validation Program has additional details regarding the algorithm implementation.

If your firewall is running in normal (non-FIPS-CC) operational mode, see Cipher Suites Supported in PAN-OS 10.2

Functions	Standards	Certificates
Asymmetric key generation		
FFC key pair generation (key size 2048 bits)	FIPS PUB 186-4	**Appliances:** #A2906 **VMs:** #A2907
ECC key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	**Appliances:** #A2906 **VMs:** #A2907
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	**Appliances:** #A2906

Functions	Standards	Certificates
		VMs: #A2907
Cryptographic Key Generation (for IKE Peer Authentication)		
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	**Appliances:** #A2906 **VMs:** #A2907
ECDSA key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	**Appliances:** #A2906 **VMs:** #A2907
Cryptographic Key Establishment		
ECC-based key establishment	SP 800-56A Revision 3	**Appliances:** #A2906 **VMs:** #A2907
FFC-based key establishment	SP 800-56A Revision 3	**Appliances:** #A2906 **VMs:** #A2907
AES Data Encryption/Decryption		
• AES CTR 128/192/256 • AES CBC 128/192/256 • AES GCM 128/256 • AES CCM 128	• AES as specified in ISO 18033-3 • CBC/CTR as specified in ISO 10116 • GCM as specified in ISO 19772 • NIST SP 800-38A/C/D/F • FIPS PUB 197	**Appliances:** #A2906 **VMs:** #A2907

Functions	Standards	Certificates
Signature Generation and Verification		
RSA (2048 bits or greater)	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSAPKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	**Appliances:** #A2906 **VMs:** #A2907
ECDSA (NIST curves P-256, P-384, and P-521)	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing "NIST curves" P-256, P-384, P-521 ISO/IEC 14888-3, Section 6.4	**Appliances:** #A2906 **VMs:** #A2907
Cryptographic hashing		
SHA-1, SHA-256, SHA-384 and SHA-512 (digest sizes 160, 256, 384 and 512 bits)	ISO/IEC 10118-3:2004 FIPS PUB 180-4	**Appliances:** #A2906 **VMs:** #A2907
Keyed-hash message authentication		
• HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512	ISO/IEC 9797-2:2011 FIPS PUB 198-1	**Appliances:** #A2906 **VMs:** #A2907
Random bit generation		
CTR_DRBG (AES-256)	ISO/IEC 18031:2011 NIST SP 800-90A	**Appliances:** #A2906

Functions	Standards	Certificates
		VMs: #A2907

Cipher Suites Supported in PAN-OS 10.1

The following topics list cipher suites that are supported on firewalls running a PAN-OS® 10.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode.

The ciphers supported in normal operation mode are grouped according to feature or functionality in the following sections:

- PAN-OS 10.1 GlobalProtect Cipher Suites
- PAN-OS 10.1 IPSec Cipher Suites
- PAN-OS 10.1 IKE and Web Certificate Cipher Suites
- PAN-OS 10.1 Decryption Cipher Suites
- PAN-OS 10.1 HA1 SSH Cipher Suites
- PAN-OS 10.1 Administrative Session Cipher Suites
- PAN-OS 10.1 PAN-OS-to-Panorama Connection Cipher Suites

PAN-OS 10.1 GlobalProtect Cipher Suites

The following table lists cipher suites for GlobalProtect™ supported on firewalls running a PAN-OS® 10.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode.

- GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal
- GlobalProtect App/Agent—IPSec mode
- GlobalProtect Portal—Browser Access

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal	• TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
	• RSA-AES-256-GCM-SHA-384 • DHE-RSA-SEED-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA-1 • ECDHE-RSA-AES-128-SHA-1 • ECDHE-RSA-AES-256-SHA-1 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-128-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
GlobalProtect App/Agent—IPSec mode (Keys transported through SSL session with gateway)	• AES-128-CBC-HMAC-SHA-1 • AES-128-GCM-HMAC-SHA-1 • AES-256-GCM-HMAC-SHA-1
GlobalProtect Portal—Browser Access	• SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
	• EDH-RSA-3DES-SHA-1 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384

PAN-OS 10.1 IPSec Cipher Suites

The following table lists the cipher suites for IPSec that are supported on firewalls running a PAN-OS® 10.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode.

- IPSec—Encryption
- IPSec—Message Authentication
- IPSec—Key Exchange

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
IPSec—Encryption	• NULL • DES • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CCM • AES-128-GCM • AES-256-GCM
IPSec—Message Authentication	• NONE • HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IPSec—Key Exchange	Diffie-Hellman groups with or without perfect forward secrecy (PFS):

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
	• No PFS—This option specifies that the firewall reuses the same key for IKE phase 1 and phase 2 instead of renewing the key for phase 2. • Group 1 (768-bit keys) with PFS enabled • Group 2 (1024-bit keys) with PFS enabled • Group 5 (1536-bit keys) with PFS enabled • Group 14 (2048-bit keys) with PFS enabled • Group 19 (256-bit elliptic curve group) with PFS enabled • Group 20 (384-bit elliptic curve group) with PFS enabled

PAN-OS 10.1 IKE and Web Certificate Cipher Suites

The following table lists cipher suites for Internet Key Exchange (IKE) and PAN-OS® web certificates that are supported on firewalls running a PAN-OS 10.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode.

- IKE Certificate Support
- IKE—Encryption
- IKE—Message Authentication
- IKE—Key Exchange
- PAN-OS Web Certificates

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases

IKE Certificate Support	• RSA
	  • Keys—512-bit, 1024-bit, 2048-bit, and 3072-bit keys
	  • Digital signature algorithms—SHA-1, SHA-256, SHA-384, or SHA-512
	• ECDSA
	  • Keys—256-bit and 384-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

IKE—Encryption	• DES • 3DES • AES-128-CBC

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
	• AES-192-CBC • AES-256-CBC **Starting with PAN-OS 10.0.3:** • AES-128-GCM • AES-256-GCM
IKE—Message Authentication	• HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IKE—Key Exchange	Diffie-Hellman groups • Group 1 (768-bit keys) • Group 2 (1024-bit keys) • Group 5 (1536-bit keys) • Group 14 (2048-bit keys) • Group 19 (256-bit elliptic curve group) • Group 20 (384-bit elliptic curve group)

PAN-OS Web Certificates	• RSA
	  • Keys—512-bit, 1024-bit, 2048-bit, 3072-bit, and 4096-bit keys
	  • Digital signature algorithms—SHA-1, SHA-256, SHA-384, or SHA-512
	• ECDSA
	  • Keys—256-bit and 384-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

PAN-OS 10.1 Decryption Cipher Suites

The following table lists cipher suites for decryption that are supported on firewalls running a PAN-OS® 10.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode.

- SSH Decryption—Host Key Algorithms

- SSH Decryption (SSHv2 only)—Encryption
- SSH Decryption (SSHv2 only)—Message Authentication
- SSL/TLS Decryption
- SSL/TLS Decryption—NIST-approved Elliptical Curves
- SSL/TLS Decryption—Perfect Forward Secrecy (PFS) Ciphers
- TLS 1.3 Decryption—Signature Algorithms

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
SSH Decryption—Host Key Algorithms	• SSH-RSA (2048-bit) • SSH-DSS (2048-bit)
SSH Decryption (SSHv2 only)—Encryption	• AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR • AES-256-CTR
SSH Decryption (SSHv2 only)—Message Authentication	• HMAC-RIPEMD • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-1-96 • HMAC-RIPEMD-160 • HMAC-SHA-1
SSL/TLS Decryption	• SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3 cipher suites • RSA 512-bit, 1024-bit, 2048-bit, 3072-bit, 4096-bit, and 8192-bit keys *The firewall can authenticate certificates up to 8192-bit RSA keys from the destination server, however the firewall generated certificate to the client supports only up to 4096-bit RSA keys.* • RSA-RC4-128-MD5 • RSA-RC4-128-SHA-1 • RSA-3DES-EDE-CBC-SHA-1 • RSA-AES-128-CBC-SHA-1 • RSA-AES-256-CBC-SHA-1 • RSA-AES-128-CBC-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
	• RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • TLS_AES_256_GCM_SHA-384 • TLS_CHACHA20_POLY1305_SHA-256 • TLS_AES_128_GCM_SHA-256
SSL/TLS Decryption—NIST-approved Elliptical Curves	• P-192 (secp192r1) • P-224 (secp224r1) • P-256 (secp256r1) • P-384 (secp384r1) • P-521 (secp521r1) • (TLS 1.3 only) X25519 • (TLS 1.3 only) X448
SSL/TLS Decryption—Perfect Forward Secrecy (PFS) Ciphers  *If you use the DHE or ECDHE key exchange algorithms to enable PFS support for SSL decryption, you can use a hardware security module (HSM) to store the private keys used for SSL Inbound Inspection.*	• DHE-RSA-3DES-EDE-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-1 • DHE-RSA-AES-256-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-256 • DHE-RSA-AES-256-CBC-SHA-256 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-CBC-SHA-1 • ECDHE-RSA-AES-256-CBC-SHA-1 • ECDHE-RSA-AES-128-CBC-SHA-256 • ECDHE-RSA-AES-256-CBC-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-CBC-SHA-1 • ECDHE-ECDSA-AES-256-CBC-SHA-1 • ECDHE-ECDSA-AES-128-CBC-SHA-256 • ECDHE-ECDSA-AES-256-CBC-SHA-384 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384 • (TLS 1.3 only) TLS_AES_128_GCM_SHA-256 • (TLS 1.3 only) TLS_AES_256_GCM_SHA-384

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
	• (TLS 1.3 only) TLS_CHACHA20_POLY1305_SHA-256
TLS 1.3 Decryption—Signature Algorithms	• ECDSA-SECP256r1-SHA-256 • RSA-PSS-RSAE-SHA-256 • RSA-PKCS1-SHA-256 • ECDSA-SECP384r1-SHA-384 • RSA-PSS-RSAE-SHA-384 • RSA-PKCS1-SHA-386 • RSA-PSS-RSAE-SHA-512 • RSA-PKCS1-SHA-512 • RSA-PKCS1-SHA-1

PAN-OS 10.1 Administrative Session Cipher Suites

The following table lists the cipher suites for administrative sessions that are supported on firewalls running a PAN-OS® 10.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode.

- Administrative Sessions to Web Interface
- Administrative Sessions to CLI (SSH)—Encryption
- Administrative Sessions to CLI (SSH)—Message Authentication
- Administrative Sessions to CLI (SSH)—Server Host Key Types
- Administrative Sessions to CLI (SSH)—Key Exchange Algorithms

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
Administrative Sessions to Web Interface	• TLSv1.1 and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-256-CBC-SHA-1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
	• RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-3DES-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
Administrative Sessions to CLI (SSH)—Encryption	• AES-128-CTR • AES-192-CTR • AES-256-CTR • AES-128-GCM • AES-256-GCM • CHACHA20-POLY1305
Administrative Sessions to CLI (SSH)—Message Authentication	• UMAC-64 • UMAC-128 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-512
Administrative Sessions to CLI (SSH)—Server Host Key Types	• RSA keys—2048-bit, 3072-bit, and 4096-bit keys • ECDSA keys—256-bit, 384-bit, and 521-bit keys
Administrative Sessions to CLI (SSH)—Key Exchange Algorithms	• curve25519-SHA-256 • diffie-hellman-group14-SHA-1 • diffie-hellman-group14-SHA-256 • diffie-hellman-group16-SHA-512 • diffie-hellman-group-exchange-SHA-256 • ecdh-SHA-2-nistp256 • ecdh-SHA-2-nistp384 • ecdh-SHA-2-nistp521

PAN-OS 10.1 HA1 SSH Cipher Suites

The following table lists the cipher suites for HA1 control connections using SSH that are supported on firewalls running a PAN-OS® 10.1 release in normal (non-FIPS-CC) or FIPS-CC operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode.

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
HA1 SSH	• AES 128-bit cipher with Counter Mode • AES 128-bit cipher with GCM (Galois/Counter Mode) • AES 192-bit cipher with Counter Mode • AES 256-bit cipher with Counter Mode • AES 256-bit cipher with GCM • CHACHA20-POLY1305

PAN-OS 10.1 PAN-OS-to-Panorama Connection Cipher Suites

The following table lists the cipher suites for PAN-OS®-to-Panorama™ connections that are supported on firewalls running a PAN-OS 10.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode.

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
PAN-OS to Panorama Connection	• RSA-RC4-128-SHA-1 • RSA-3DES-SHA-1 • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-1 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1

PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode

The following table lists cipher suites that are supported on firewalls running a PAN-OS® 10.1 release in FIPS-CC mode. The Cryptographic Algorithm Validation Program has additional details regarding the algorithm implementation.

If your firewall is running in normal (non-FIPS-CC) operational mode, see Cipher Suites Supported in PAN-OS 10.1

Functions	Standards	Certificates
Asymmetric key generation		
FFC key pair generation (key size 2048 bits)	FIPS PUB 186-4	**Appliances:** #A2137 **VMs:** #A2244
ECC key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	**Appliances:** #A2137 **VMs:** #A2244
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	**Appliances:** #A2137 **VMs:** #A2244
Cryptographic Key Generation (for IKE Peer Authentication)		
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	**Appliances:** #A2137 **VMs:** #A2244
ECDSA key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	**Appliances:** #A2137 **VMs:** #A2244
Cryptographic Key Establishment		

Functions	Standards	Certificates
ECDSA-based key establishment	NIST SP 800-56A Revision 3	**Appliances:** #A2137 **VMs:** #A2244
FFC-based key establishment	NIST SP 800-56A Revision 3	**Appliances:** #A2137 **VMs:** #A2244
AES Data Encryption/Decryption		
• AES CTR 128/192/256 • AES CBC 128/192/256 • AES GCM 128/256 • AES CCM 128	• AES as specified in ISO 18033-3 • CBC/CTR as specified in ISO 10116 • GCM as specified in ISO 19772 • NIST SP 800-38A/C/D/F • FIPS PUB 197	**Appliances:** #A2137 **VMs:** #A2244
Signature Generation and Verification		
RSA Digital Signature Algorithm (rDSA) (2048 bits or greater)	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSAPKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	**Appliances:** #A2137 **VMs:** #A2244
ECDSA (NIST curves P-256, P-384, and P-521)	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing "NIST	**Appliances:** #A2137 **VMs:**

Functions	Standards	Certificates
	curves" P-256, P-384, P-521 ISO/IEC 14888-3, Section 6.4	#A2244
Cryptographic hashing		
SHA-1, SHA-256, SHA-384 and SHA-512 (digest sizes 160, 256, 384 and 512 bits)	ISO/IEC 10118-3:2004 FIPS PUB 180-4	**Appliances:** #A2137 **VMs:** #A2244
Keyed-hash message authentication		
• HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512	ISO/IEC 9797-2:2011 FIPS PUB 198-1	**Appliances:** #A2137 **VMs:** #A2244
Random bit generation		
CTR_DRBG (AES-256)	ISO/IEC 18031:2011 NIST SP 800-90A	**Appliances:** #A2137 **VMs:** #A2244

Cipher Suites Supported in PAN-OS 9.1

The following topics list cipher suites that are supported on firewalls running a PAN-OS® 9.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode.

The ciphers supported in normal operation mode are grouped according to feature or functionality in the following sections:

- PAN-OS 9.1 GlobalProtect Cipher Suites
- PAN-OS 9.1 IPSec Cipher Suites
- PAN-OS 9.1 IKE and Web Certificate Cipher Suites
- PAN-OS 9.1 Decryption Cipher Suites
- PAN-OS 9.1 HA1 SSH Cipher Suites
- PAN-OS 9.1 Administrative Session Cipher Suites
- PAN-OS 9.1 PAN-OS-to-Panorama Connection Cipher Suites

PAN-OS 9.1 GlobalProtect Cipher Suites

The following table lists cipher suites for GlobalProtect™ supported on firewalls running a PAN-OS® 9.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode.

- GlobalProtect App/Agent—SSL
- GlobalProtect App/Agent—IPSec mode
- GlobalProtect Portal—Browser Access

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal	• TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
	• RSA-AES-256-GCM-SHA-384 • DHE-RSA-SEED-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA-1 • ECDHE-RSA-AES-128-SHA-1 • ECDHE-RSA-AES-256-SHA-1 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-128-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
GlobalProtect App/Agent—IPSec mode (Keys transported through SSL session with gateway)	• AES-128-CBC-HMAC-SHA-1 • AES-128-GCM-HMAC-SHA-1 • AES-256-GCM-HMAC-SHA-1
GlobalProtect Portal—Browser Access	• SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
	• EDH-RSA-3DES-SHA-1 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384

PAN-OS 9.1 IPSec Cipher Suites

The following table lists the cipher suites for IPSec that are supported on firewalls running a PAN-OS® 9.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode.

- IPSec—Encryption
- IPSec—Message Authentication
- IPSec—Key Exchange

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
IPSec—Encryption	• NULL • DES • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CCM • AES-128-GCM • AES-256-GCM
IPSec—Message Authentication	• NONE • HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IPSec—Key Exchange	Diffie-Hellman groups with or without perfect forward secrecy (PFS):

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
	• No PFS—This option specifies that the firewall reuses the same key for IKE phase 1 and phase 2 instead of renewing the key for phase 2. • Group 1 (768-bit keys) with PFS enabled • Group 2 (1024-bit keys) with PFS enabled • Group 5 (1536-bit keys) with PFS enabled • Group 14 (2048-bit keys) with PFS enabled • Group 19 (256-bit elliptic curve group) with PFS enabled • Group 20 (384-bit elliptic curve group) with PFS enabled

PAN-OS 9.1 IKE and Web Certificate Cipher Suites

The following table lists cipher suites for Internet Key Exchange (IKE) and PAN-OS® web certificates that are supported on firewalls running a PAN-OS 9.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode.

- IKE Certificate Support
- IKE—Encryption
- IKE—Message Authentication
- IKE—Key Exchange
- PAN-OS Web Certificates

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases

IKE Certificate Support	• RSA
	  • Keys—512-bit, 1024-bit, 2048-bit, and 3072-bit keys
	  • Digital signature algorithms—SHA-1, SHA-256, SHA-384, or SHA-512
	• ECDSA
	  • Keys—256-bit and 384-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

IKE—Encryption	• DES • 3DES • AES-128-CBC

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
	• AES-192-CBC • AES-256-CBC
IKE—Message Authentication	• HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IKE—Key Exchange	Diffie-Hellman groups • Group 1 (768-bit keys) • Group 2 (1024-bit keys) • Group 5 (1536-bit keys) • Group 14 (2048-bit keys) • Group 19 (256-bit elliptic curve group) • Group 20 (384-bit elliptic curve group)

PAN-OS Web Certificates	• RSA
	  • Keys—512-bit, 1024-bit, 2048-bit, 3072-bit, and 4096-bit keys
	  • Digital signature algorithms—SHA-1, SHA-256, SHA-384, or SHA-512
	• ECDSA
	  • Keys—256-bit and 384-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

PAN-OS 9.1 Decryption Cipher Suites

The following table lists cipher suites for decryption that are supported on firewalls running a PAN-OS® 9.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode.

- SSH Decryption—Host Key Algorithms
- SSH Decryption (SSHv2 only)—Encryption
- SSH Decryption (SSHv2 only)—Message Authentication
- SSL/TLS Decryption

- SSL/TLS Decryption—NIST-approved Elliptical Curves
- SSL/TLS Decryption—Perfect Forward Secrecy (PFS) Ciphers

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
SSH Decryption—Host Key Algorithms	• SSH-RSA (2048-bit) • SSH-DSS (2048-bit)
SSH Decryption (SSHv2 only)—Encryption	• AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR • AES-256-CTR
SSH Decryption (SSHv2 only)—Message Authentication	• HMAC-RIPEMD • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-1-96 • HMAC-RIPEMD-160 • HMAC-SHA-1
SSL/TLS Decryption	• SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA 512-bit, 1024-bit, 2048-bit, 3072-bit, 4096-bit, and 8192-bit keys *The firewall can authenticate certificates up to 8192-bit RSA keys from the destination server, however the firewall generated certificate to the client supports only up to 4096-bit RSA keys.* • RSA-RC4-128-MD5 • RSA-RC4-128-SHA-1 • RSA-3DES-EDE-CBC-SHA-1 • RSA-AES-128-CBC-SHA-1 • RSA-AES-256-CBC-SHA-1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
SSL/TLS Decryption—NIST-approved Elliptical Curves	• P-192 (secp192r1) • P-224 (secp224r1) • P-256 (secp256r1) • P-384 (secp384r1) • P-521 (secp521r1)
SSL/TLS Decryption—Perfect Forward Secrecy (PFS) Ciphers *If you use the DHE or ECDHE key exchange algorithms to enable PFS support for SSL decryption, you can use a hardware security module (HSM) to store the private keys used for SSL Inbound Inspection.*	• DHE-RSA-3DES-EDE-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-1 • DHE-RSA-AES-256-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-256 • DHE-RSA-AES-256-CBC-SHA-256 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-CBC-SHA-1 • ECDHE-RSA-AES-256-CBC-SHA-1 • ECDHE-RSA-AES-128-CBC-SHA-256 • ECDHE-RSA-AES-256-CBC-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-CBC-SHA-1 • ECDHE-ECDSA-AES-256-CBC-SHA-1 • ECDHE-ECDSA-AES-128-CBC-SHA-256 • ECDHE-ECDSA-AES-256-CBC-SHA-384 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384

PAN-OS 9.1 Administrative Session Cipher Suites

The following table lists the cipher suites for administrative sessions that are supported on firewalls running a PAN-OS® 9.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode.

- Administrative Sessions to Web Interface
- Administrative Sessions to CLI (SSH)—Encryption
- Administrative Sessions to CLI (SSH)—Message Authentication

- Administrative Sessions to CLI (SSH)—Server Host Key Types
- Administrative Sessions to CLI (SSH)—Key Exchange Algorithms

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
Administrative Sessions to Web Interface	• TLSv1.1 and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-256-CBC-SHA-1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-3DES-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
Administrative Sessions to CLI (SSH)—Encryption	• 3DES-CBC • ARCFOUR128 • ARCFOUR256 • BLOWFISH-CBC • CAST128-CBC • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
	• AES-256-CTR • AES-128-GCM • AES-256-GCM
Administrative Sessions to CLI (SSH)—Message Authentication	• UMAC-64 • UMAC-128 • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-1-96 • HMAC-RIPEMD-160 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-512
Administrative Sessions to CLI (SSH)—Server Host Key Types	• RSA keys—2048-bit, 3072-bit, and 4096-bit keys • ECDSA keys—256-bit, 384-bit, and 521-bit keys
Administrative Sessions to CLI (SSH)—Key Exchange Algorithms	• diffie-hellman-group1-SHA-1 • diffie-hellman-group14-SHA-1 • diffie-hellman-group-exchange-SHA-1 • diffie-hellman-group-exchange-SHA-256 • ecdh-SHA-2-nistp256 • ecdh-SHA-2-nistp384 • ecdh-SHA-2-nistp521

PAN-OS 9.1 HA1 SSH Cipher Suites

The following table lists the cipher suites for HA1 control connections using SSH that are supported on firewalls running a PAN-OS® 9.1 release in normal (non-FIPS-CC) or FIPS-CC operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode.

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
HA1 SSH	• AES 128-bit cipher with Cipher Block Chaining • AES 128-bit cipher with Counter Mode

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
	• AES 128-bit cipher with GCM (Galois/Counter Mode) • AES 192-bit cipher with Cipher Block Chaining • AES 192-bit cipher with Counter Mode • AES 256-bit cipher with Cipher Block Chaining • AES 256-bit cipher with Counter Mode • AES 256-bit cipher with GCM

PAN-OS 9.1 PAN-OS-to-Panorama Connection Cipher Suites

The following table lists the cipher suites for PAN-OS®-to-Panorama™ connections that are supported on firewalls running a PAN-OS 9.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode.

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
PAN-OS to Panorama Connection	• RSA-RC4-128-SHA-1 • RSA-3DES-SHA-1 • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-1 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1

PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode

The following table lists cipher suites that are supported on firewalls running a PAN-OS® 9.1 release in FIPS-CC mode. The Cryptographic Algorithm Validation Program has additional details regarding the algorithm implementation. Also, there were no changes made to the Palo Alto Networks crypto module between PAN-OS 9.0 and PAN-OS 9.1 so all FIPS certificates still apply for this PAN-OS 9.1 release.

If your firewall is running in normal (non-FIPS-CC) operational mode, see Cipher Suites Supported in PAN-OS 9.1

Functions	Standards
Asymmetric key generation	
FFC key pair generation (key size 2048 bits)	FIPS PUB 186-4
ECC key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4
RSA key generation (2048 bits or greater)	FIPS PUB 186-4
Cryptographic Key Generation (for IKE Peer Authentication)	
RSA key generation (2048 bits or greater)	FIPS PUB 186-4
ECDSA key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4
Cryptographic Key Establishment	
ECDSA-based key establishment	NIST SP 800-56A Revision 2
FFC-based key establishment	NIST SP 800-56A Revision 2
AES Data Encryption/Decryption	
• AES CTR 128/192/256 • AES CBC 128/192/256 • AES GCM 128/256 • AES CCM 128	• AES as specified in ISO 18033-3 • CBC/CTR as specified in ISO 10116 • GCM as specified in ISO 19772 • NIST SP 800-38A/C/D/F • FIPS PUB 197
Signature Generation and Verification	
RSA Digital Signature Algorithm (rDSA) (2048 bits or greater)	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSAPKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3

Functions	Standards
ECDSA (NIST curves P-256, P-384, and P-521)	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing "NIST curves" P-256, P-384, ISO/IEC 14888-3, Section 6.4
Cryptographic hashing	
SHA-1, SHA-256, SHA-384, and SHA-512 (digest sizes 160, 256, 384, and 512 bits)	ISO/IEC 10118-3:2004 FIPS PUB 180-4
Keyed-hash message authentication	
• HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512	ISO/IEC 9797-2:2011 FIPS PUB 198-1
Random bit generation	
CTR_DRBG (AES-256)	ISO/IEC 18031:2011 NIST SP 800-90A

GlobalProtect

The following topics provide support information for the GlobalProtect™ app (originally referred to as the GlobalProtect agent on Windows and Mac).

Where Can I Install the GlobalProtect App?

The following sections show operating systems on which you can install each release of the GlobalProtect™ app.

The compatibility lists that follow show compatibility with major versions for each platform only and does specifically call out minor versions. However, support the stated support for the major versions implicitly includes support for all minor versions for the listed major versions.

- Apple macOS
- Microsoft Windows
- Linux
- Apple iOS and iPadOS
- Google Android
- Google Chrome
- Internet of Things (IoT)
- Hypervisors

Use the OS compatibility information to determine what version of the GlobalProtect app you want your users to run on their endpoints.

Because the version that an end user must download and install to enable successful connectivity to your network depends on your environment, there is no direct download link for the GlobalProtect app on the Palo Alto Networks site. In addition, the way you deploy the GlobalProtect app to your users depends on the OS of the endpoint.

All GlobalProtect 5.x releases are end-of-life (EoL). GlobalProtect 5.1.x reached end-of-life (EoL) status on December 31, 2024 and GlobalProtect 5.2.x on February 28, 2024.

See the Palo Alto Networks End-of-Life Summary for more information about the GlobalProtect EoL schedule.

Apple macOS

The following table shows which macOS versions support which versions of the GlobalProtect app. For instructions on installing the GlobalProtect app on a macOS endpoint, see the installation instructions for 6.0, 6.1, 6.2, and 6.3.

OS	GP App 6.0 FIPS-CC	GP App 6.1	GP App 6.2	GP App 6.3
macOS 10.15 (Catalina)	√ *	√	√ *	—

OS	GP App 6.0 FIPS-CC	GP App 6.1	GP App 6.2	GP App 6.3
macOS 11 (Big Sur)	√ *	√	√ *	—
macOS 12 (Monterey)	√ *	√	√ *	√
macOS 13 (Ventura)	√ * 6.0.3 or later (x86 & ARM-Based MacBooks)	√	√ *	√
macOS 14 (Sonoma)	√ * 6.0.7 or later	√ 6.1.2 or later	√ * 6.2.1 or later	√
macOS 15 (Sequoia)	6.0.11 and later 6.0.x releases	—	√ 6.2.6 and later 6.2.x releases	√ 6.3.2 and later 6.3.x releases

** Embedded browser framework for SAML authentication upgraded to WebKit in the following releases:*

- *GlobalProtect 6.2.3 and later*
- *GlobalProtect 6.0.9 and later*

Microsoft Windows

The following table shows which Microsoft Windows versions support which versions of the GlobalProtect app. For instructions on installing the GlobalProtect app on a Windows endpoint, see the installation instructions for 6.0, 6.1, 6.2, and 6.3.

OS	GP App 6.0 FIPS-CC	GP App 6.1	GP App 6.2	GP App 6.3
Windows 10	√ * 64-bit (x64), 32-bit (x86), and ARM64 devices	√ 64-bit (x64), 32-bit (x86), and ARM64 devices	√ * 64-bit (x64), 32-bit (x86), and ARM64 devices	√
Windows 10 UWP	√	√	√	—

OS	GP App 6.0 FIPS-CC	GP App 6.1	GP App 6.2	GP App 6.3
Windows 11	√ * 64-bit (x64) and ARM64 devices	√ 64-bit (x64) and ARM64 devices	√ * 64-bit (x64) and ARM64 devices	√
Windows 365 Cloud PC	—	—	√ 6.2.6-c857 and later 6.2.x releases	√ 6.3.2 and later 6.3.x releases

** Embedded browser framework for SAML authentication upgraded to WebView2 in the following releases:*

- *GlobalProtect 6.2.3 and later*
- *GlobalProtect 6.0.9 and later*

Linux

The following table shows compatibility between Linux versions and GlobalProtect app versions. For instructions on installing the GlobalProtect app on a Linux endpoint, see the installation instructions for 6.0,6.1, and 6.2.

GlobalProtect Linux supports 64-bit x86 endpoints. Starting with GlobalProtect version 6.2.6, the CLI-only agent also supports ARM64 endpoints. The GlobalProtect for Linux UI agent is supported on GNOME with X11 on compatible Linux platforms.

OS	GP App 6.0 FIPS-CC	GP App 6.1	GP App 6.2
Red Hat Enterprise Linux (RHEL) 8.10			√ Supported on 6.2.0 and later
Red Hat Enterprise Linux (RHEL) 9.4	—	—	√ Supported on 6.2.1 and later
Ubuntu 20.04	√ CLI only	√ CLI-based and GUI-based GlobalProtect app	√ (Supported on 6.2.1 and later)

OS	GP App 6.0 FIPS-CC	GP App 6.1	GP App 6.2
Ubuntu 22.04 LTS	—	√ CLI-based and GUI-based GlobalProtect app	√ Supported on 6.2.1 and later
Ubuntu 24.04 LTS			√ Supported on 6.2.1 and later
Fedora Linux 41	—	—	√ Supported on 6.2.1 and later
Fedora Linux 42	—	—	√ Supported on 6.2.6 and later
Rocky Linux 9.5	—	—	√ Supported on 6.2.6 and later

Apple iOS and iPadOS

The following table shows compatibility between iOS versions and GlobalProtect app versions. For instructions on installing the GlobalProtect app on a Apple iOS and iPadOS endpoint, see the installation instructions for 6.0.

OS	GP App 6.0 FIPS-CC	GP App 6.1	GP App 6.2
iOS 10	√ (64-bit devices only)	√ (GlobalProtect app 6.1.0 or later)	N/A
iOS 11	√ (64-bit devices only)	√ (GlobalProtect app 6.1.0 or later)	N/A
iOS 12	√	√	N/A

OS	GP App 6.0 FIPS-CC	GP App 6.1	GP App 6.2
	(64-bit devices only)	(GlobalProtect app 6.1.0 or later)	
iOS 13	√ (64-bit devices only)	√ (GlobalProtect app 6.1.0 or later)	N/A
iOS 14	√ (64-bit devices only)	√ (GlobalProtect app 6.1.0 or later)	N/A
iOS 15	√ (64-bit devices only)	√ (GlobalProtect app 6.1.0 or later)	N/A
iOS 16	√ (64-bit devices only running GlobalProtect app 6.0.4 or later)	√ (GlobalProtect app 6.1.0 or later)	N/A
iOS 17	–	√ (GlobalProtect app 6.1.0 or later)	N/A
iOS 18	–	√ (GlobalProtect app 6.1.6 or later)	N/A

Google Android

The following table shows compatibility between Google Android versions and GlobalProtect app versions. For instructions on installing the GlobalProtect app on a Google Android endpoint, see the installation instructions for 6.0.

OS	GP App 6.0 FIPS-CC	GP App 6.1	GP App 6.2
Google Android 6.x	√ (Not supported on GlobalProtect app	N/A	N/A

OS	GP App 6.0 FIPS-CC	GP App 6.1	GP App 6.2
	version 6.0.7 and later)		
Google Android 7.x	√ (Not supported on GlobalProtect app version 6.0.7 and later)	N/A	N/A
Google Android 8.x	√	√ (GlobalProtect app version 6.1.0 or later)	N/A
Google Android 9.x	√	√ (GlobalProtect app version 6.1.0 or later)	N/A
Google Android 10.x	√	√ (GlobalProtect app version 6.1.0 or later)	N/A
Google Android 11.x	√	√ (GlobalProtect app version 6.1.0 or later)	N/A
Google Android 12.x	√	√ (GlobalProtect app version 6.1.0 or later)	N/A
Google Android 13.x	√ 6.0.3 or later	√ (GlobalProtect app version 6.1.0 or later)	N/A
Google Android 14.x	—	√ (GlobalProtect app version 6.1.0 or later)	N/A
Google Android 15.x	—	√ (GlobalProtect app version 6.1.6 or later)	N/A

OS	GP App 6.0 FIPS-CC	GP App 6.1	GP App 6.2
Chrome OS Systems Supporting Android Apps	√	√ (GlobalProtect app version 6.1.0 or later)	N/A

Google Chrome

The following table shows compatibility between Google Chrome OS systems supporting Android apps and GlobalProtect app versions. For instructions on installing the GlobalProtect app on a Google Chrome endpoint, see the installation instructions for 6.0.

OS	GP App 6.0	GP App 6.1	GP App 6.2
Chrome OS Systems Supporting Android Apps	√	N/A	N/A

Internet of Things (IoT)

The following table shows compatibility between IoT platforms and GlobalProtect app versions. For instructions on installing the GlobalProtect app on a IoT endpoint, see the installation instructions for 6.0, and 6.1. See the supported features list to see which GlobalProtect app features are supported on IoT devices.

OS	GP App 6.0	GP App 6.1	GP App 6.2
Android	√	N/A	N/A
Raspbian	√	√	N/A
Ubuntu	√	√	N/A
Windows IoT Enterprise	√	√	N/A

Hypervisors

The following table shows hypervisor support on each GlobalProtect app version.

OS	GP App 6.0	GP App 6.1	GP App 6.2
Citrix Xen Desktop	√	√	√

OS	GP App 6.0	GP App 6.1	GP App 6.2
	6.0.3 and later		
VMWare Horizon and Vcenter	√	√	√

Third-Party VPN Client Support

The following topics provide support information for third-party clients:

- What Third-Party VPN Clients are Supported?
- What GlobalProtect Features Do Third-Party Clients Support?
- How Many Third-Party Clients Does Each Firewall Model Support?

What Third-Party VPN Clients are Supported?

The following table lists third-party VPN client support for PAN-OS® software.

For stronger security, higher tunnel capacities, and a greater breadth of features, we recommend that you use the GlobalProtect™ app instead of a third-party VPN client.

Third-Party IPSec Client	Minimum PAN-OS Version
iOS built-in IPSec client	9.1
Android built-in IPSec client	9.1
VPNC on Ubuntu Linux 10.04 and later versions and CentOS 6 and later versions	9.1
strongSwan on Ubuntu Linux and CentOS*	9.1
* To set up authentication for strongSwan Ubuntu and CentOS clients for PAN-OS 9.1 and later releases, refer to the GlobalProtect Administrator's Guide for your release.	

Clients emulating GlobalProtect are not supported.

What GlobalProtect Features Do Third-Party Clients Support?

Third-party clients support the following GlobalProtect™ features:

GlobalProtect Feature	iOS Built-In IPSec Client	Android Built-In IPSec Client	VPNC on Ubuntu Linux 10.04 and later versions and CentOS 6 and later versions	strongSwan on Ubuntu Linux and CentOS
Mixed Authentication Method Support for	√	√	√	√

GlobalProtect Feature	iOS Built-In IPSec Client	Android Built-In IPSec Client	VPNC on Ubuntu Linux 10.04 and later versions and CentOS 6 and later versions	strongSwan on Ubuntu Linux and CentOS
Certificates or User Credentials				
IPSec VPN Connections	√	√	√	√
IPv4 Addressing	√	√	√	√
Gateway-Level IP Pools	√	√	√	√
Primary Username Visiblity on GlobalProtect Gateways	√	√	√	√

How Many Third-Party Clients Does Each Firewall Model Support?

The following table lists the maximum number of third-party X-Auth IPSec clients supported by each firewall model.

Palo Alto Networks Firewall Model	Maximum Third-Party X-Auth IPSec Clients
Hardware Firewalls	
PA-7080	2,000
PA-7050	2,000
PA-5450	4,000
PA-5440	4,000
PA-5430	4,000
PA-5420	4,000
PA-5410	4,000
PA-5280	2,500
PA-5260	2,500

Palo Alto Networks Firewall Model	Maximum Third-Party X-Auth IPSec Clients
PA-5250	2,000
PA-5220	1,500
PA-3440	2,000
PA-3430	2,000
PA-3420	1,500
PA-3410	1,500
PA-3260	1,500
PA-3250	1,500
PA-3220	1,000
PA-1420	1,400
PA-1410	1,400
PA-850	500
PA-820	500
PA-460	1,400
PA-450	1,400
PA-445	1,400
PA-440	1,400
PA-415	500
PA-410	500
PA-220R	500
PA-220**	500
VM-Series Firewalls	
VM-700	1,000

Palo Alto Networks Firewall Model	Maximum Third-Party X-Auth IPSec Clients
VM-500	500
VM-300	500
VM-200	500
VM-100	500
VM-50	125

* PA-220 firewalls are supported only on PAN-OS 10.2 and earlier supported PAN-OS versions. Refer to hardware end-of-life (EoL) dates for more information about end-of-life products.

What Features Does GlobalProtect Support?

The following table lists the features supported on GlobalProtect™ by operating system (OS). An entry in the table indicates the first supported release of the feature on the OS (however, you should review the End-of-Life Summary to ensure you are using a supported release). A dash ("—") indicates that the feature is not supported. For recommended minimum GlobalProtect app versions, see Where Can I Install the GlobalProtect App?.

For Chromebook and other Chrome OS devices, use Android App 5.0 or a later version to get GlobalProtect app features introduced in GlobalProtect app 5.0 and later releases. (Refer also to the end-of-life (EoL) information for the GlobalProtect app.)

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	Windows 365 Cloud PC	macOS	Linux
Authentication								
Embedded Browser with Captive Portal	—	—	—	6.3.3	—	—	—	—
Cloud Identity Engine Authentication	—	—	—	6.0.0	—	—	6.0.0	—
Multi-Factor Authentication Policy	—	—	—	4.0.0	—	—	4.0.0	—
SAML Authentication	4.0.0	4.0.0 (**On-Demand** connect method only)	4.1.0	4.0.0	—	6.2.5	4.0.0	5.1 (GUI-based GlobalProtect app)
SAML Authentication with Cloud Authentication Service	6.0.0	6.0.0 (**On Demand** connect method only)	6.0.0	6.0.0	—	6.2.5	6.0.0	6.0.0

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	Windows 365 Cloud PC	macOS	Linux
Note: Requires use of Default System Browser								
Default System Browser for SAML Authentication	5.2.0	5.2.0	5.2.0	5.2.0	—	6.2.5	5.2.0	5.2.0
SAML Authentication Via Trusted IP Addresses	—	—	6.3.3	—	—	—	—	—
Expired Active Directory Password Change for Remote Users	4.1.0	4.1.0 (notifications only) 5.0.0 (full support)	4.1.0	4.1.0	4.1.0	—	4.1.0	—
Active Directory Password Change Using the GlobalProtect Credential Provider	—	—	—	4.1.0	—	—	—	—
Mixed Authentication Method Support or Certificates or User Credentials	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	—	4.1.0	4.1.0

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	Windows 365 Cloud PC	macOS	Linux
Pre-Logon Followed by Two-Factor Authentication	—	—	—	4.1.0	—	• 6.2.6-c857 and later 6.2.x releases • 6.3.2 and later 6.3.x releases	4.1.0	—
Pre-Logon Followed by SAML Authentication	—	—	—	4.1.0	—	• 6.2.6-c857 and later 6.2.x releases • 6.3.2 and later 6.3.x releases	4.1.0	—
Single Sign-On (SSO)								
SSO (Credential Provider)	—	—	—	1.2.0	—	—	—	—
Kerberos SSO	—	—	—	3.0.0	—	—	4.1.0	—
SAML SSO	5.1.0	5.2.0	5.1.0	5.2.0	—	6.2.5	5.2.0	5.2.0
SSO (Smart Card Authentication)	—	—	—	6.0.0 Windows 10 or later	—	—	—	—
VPN Connections								

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	Windows 365 Cloud PC	macOS	Linux
IPSec	1.3.0	1.3.0	3.1.1	1.0.0	—	6.2.5	1.0.0	4.1.0
SSL	1.3.0	1.3.0	3.1.1	1.0.0	3.1.3	6.2.5	1.0.0	4.1.0
SSL Tunnel Enforcement	5.1.0	5.1.0	—	5.1.0	—	6.2.5	5.1.0	5.0.6 (CLI) 5.1.0 (web interface)
Clientless VPN	— (no client required)	— (no client required)	— (no client required)	— (no client required)	— (no client required)	—	— (no client required)	— (no client required)
Connect Methods								
User-logon (always on)	1.3.0	1.3.0	5.0.0 (through extended support for the GlobalProtect app for Android)	1.0.0	3.1.3 (Always On configured from third-party MDM)	6.2.5	1.0.0	4.1.0
Pre-logon (always-on)	—	—	—	1.1.0	—	—	1.1.0	—
Pre-logon (then on-demand)	—	—	—	3.1.0	—	—	3.1.0	—
On-demand	1.3.0	1.3.0	3.1.1	1.0.0	3.1.3	6.2.5	1.0.0	4.1.0
Connect Before Logon	—	—	—	5.2.0	—	—	—	—
Conditional Connect Method	—	—	—	6.2.0	6.2.0	—	6.2.0	—

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	Windows 365 Cloud PC	macOS	Linux
Connection Priority								
External Gateway Priority by Source Region	4.0.0	4.0.0	4.0.0	4.0.0	4.0.0	—	4.0.0	4.1.0
Internal Gateway Selection by Source IP Address	4.0.0 (Except DHCP options)	4.0.0 (Except DHCP options)	—	4.0.0	—	—	4.0.0	4.1.0
Modes								
Internal mode	1.3.0	1.3.0	—	1.0.0	—	—	1.0.0	4.1
External mode	1.3.0	1.3.0	3.1.1	1.0.0	3.1.3	—	1.0.0	4.1
Prisma Access Explicit Proxy Connectivity in GlobalProtect	—	—	—	6.2.0	6.2.0	—	6.2.0	—
Networking								
Intelligent Internal Host Detection	—	—	6.3.1	6.3.1	6.3.1	—	6.3.1	6.3.1
Traffic Enforcement	—	—	6.3.1	6.3.1	6.3.1	—	6.3.1	6.3.1
IPv4 Addressing	1.3.0	1.3.0	3.1.1	1.0.0	3.1.3	6.2.5	1.0.0	4.1

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	Windows 365 Cloud PC	macOS	Linux
IPv6 Addressing	4.0.0	4.0.0	4.0.0	4.0.0	4.0.0	6.2.5	4.0.0	4.1
Split Tunnel to Exclude by Access Route	—	4.0.0	4.0.0	4.0.0	4.0.0	6.2.5	4.0.0	4.1
Optimized Split Tunneling for GlobalProtect	—	—	—	4.1.0	—	—	4.1.0	6.1.0 Domain-based split tunneling only; application-based split tunneling not supported
Enhanced Split Tunneling	—	—	—	6.2.0	6.2.0	6.2.5	6.2.0	—
Wildcard Support for Split Tunnel Settings Based on the Application	—	—	—	6.3.1	—	6.3.1	6.3.1	—
Split DNS for iOS	—	6.1.6	—	—	—	—	—	—
Split DNS	—	—	—	5.2.0	—	6.2.5	5.2.0	6.1.0
Per-App VPN	4.0.0	4.0.0				—		
No Direct Access	—	—	—	4.0.0	—	—	4.0.0	6.0.0

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	Windows 365 Cloud PC	macOS	Linux
to Local Network								
Endpoint Traffic Policy Enforcement	—	—	—	6.0.0 Windows 10 or later	—	6.2.6-c857 and later 6.2.x releases or 6.3.2 and later 6.3.x releases	6.0.0 macOS 11 and later	—
Customization								
Reveal Password on Windows Logon Screen	—	—	—	6.3.3	—	—	—	—
Autonomous DEM Integration for User Experience Management	—	—	—	5.2.6	—	—	5.2.6	—
GlobalProtect App Log Collection for Troubleshooting	5.2.5	5.2.5	5.2.5	5.2.5	—	—	5.2.5	5.2.5
Configurable Maximum Transmission Unit for GlobalProtect Connections	5.2.4	5.2.4	5.2.4	5.2.4	5.2.4	—	5.2.4	5.2.4
Connect Before Logon	—	—	—	5.2.0	—	—	—	—

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	Windows 365 Cloud PC	macOS	Linux
User-Initiated Pre-Logon Connection	-	-	-	5.0.3	-	—	-	-
Support for Preferred Gateways	5.0.3	5.0.7	-	5.0.3	-	—	5.0.3	-
GlobalProtect Gateway Location Configuration	5.0.0	5.0.0	-	5.0.0	-	—	5.0.0	-
Automatic Launching of Web Browser in Captive Portal Environment	-	-	-	4.1.0	-	—	4.1.0	-
GlobalProtect Tunnel Preservation On User Logout	-	-	-	4.1.0	-	—	-	-
Endpoint Tunnel Configurations Based on Source Region or IP Address	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	—	4.1.0	4.1.0
Portal Configuration Assignment and HIP-Based Access Control Using	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	—	4.1.0	4.1.0

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	Windows 365 Cloud PC	macOS	Linux
New Endpoint Attributes								
HIP Report Redistribution	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	—	4.1.0	4.1.0
DNS Configuration Assignment Based on Users or User Groups	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	—	4.1.0	4.1.0
Tunnel Restoration and Authentication Cookie Usage Restrictions	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	—	4.1.0	4.1.0
Concurrent Support for IPv4 and IPv6 DNS Servers	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	—	4.1.0	4.1.0
Support for IPv6-Only GlobalProtect Deployment	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	—	4.1.0	4.1.0
FIPS-CC	—	—	—	FIPS Validated on 5.1.4 CC Certified on 5.1.5 x86 platforms	—	—	FIPS Validated on 5.1.4 CC Certified on 5.1.5	6.0.7

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	Windows 365 Cloud PC	macOS	Linux
				FIPS-CC available on 6.0.7			x86 platforms FIPS-CC available on 6.0.7	
MDM Integration for HIP-Based Policy Enforcement	5.0.0	5.0.0	—	—	—	—	—	—
Captive Portal Notification Delay	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	—	4.1.0	4.1.0
Tunnel Connections Over Proxies	—	—	—	4.1.7	—	—	4.1.7	—
PAC deployment via GlobalProtect app	—	—	—	6.1.0	—	—	6.1.0	6.1.0
End-user Notification about GlobalProtect Session Logout	—	—	—	6.1.0	—	—	6.1.0	6.1.0
GlobalProtect Credentials Provier Pre-Logon Connection Status	—	—	—	4.1.0	—	—	—	—

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	Windows 365 Cloud PC	macOS	Linux
Static IP Address Assignment	—	—	—	4.1.0	—	—	—	—
Multiple Portal Support	—	—	—	4.1.0	—	—	4.1.0	—
Customizable Username and Password Labels	4.1.0	4.1.0	—	4.1.0	4.1.0	—	4.1.0	4.1.0
Gateway-Level IP Pools	4.0.0	4.0.0	4.0.0	4.0.0	4.0.0	—	4.0.0	4.1.0
Resilient VPN	4.0.3	4.0.3	—	4.0.3	—	—	4.0.3	—
Pre-logon tunnel rename timeout	—	—	—	4.0.2	—	—	—	—
Restrict Transparent Agent Upgrades to Internal Network Connections	—	—	—	4.0.0	—	—	4.0.0	—
Enforce GlobalProtect for Network Access	—	—	—	3.1.0	3.1.3 (VPN Lockdown configured from third-party MDM)	6.2.5	3.1.0	—

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	Windows 365 Cloud PC	macOS	Linux
Enforce GlobalProtect Exclusions	—	—	—	5.1.0	—	6.2.5	5.1.0	—
Enforce GlobalProtect Connections with FQDN Exclusions	—	—	—	5.2.0	—	6.2.5	5.2.0	—
Certificate selection by OID	—	—	—	3.0.0	—	—	3.0.0	—
Deployment of SSL Forward Proxy CA certificates in the trust store	—	—	—	3.0.0	—	6.2.5	3.0.0	—
HIP reports	1.3.0	1.3.0	3.0.0	1.0.0	3.1.3 (Host information only; Notifications not supported)	6.2.5	1.0.0	4.1.0 (Host information only)
Run scripts before and after sessions	—	—	—	2.3.0	—	—	2.3.0	—
Allow users to disable GlobalProtect	6.0	—	—	2.2.0	—	—	2.2.0	4.1.0

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	Windows 365 Cloud PC	macOS	Linux
Welcome and help pages	1.3.0	1.3.0	3.0.0	1.0.0	—	—	1.0.0	—
HIP Exceptions for Patch Management	—	—	—	6.2.0	6.2.0	—	6.2.0	—
HIP Process Remediation	—	—	—	6.2.0	6.2.0	—	6.2.0	—
Extend User Session for GlobalProtect Users	—	—	—	6.2.0	6.2.0	—	6.2.0	—
Other								
Support for 100 Manual Gateways	5.0.3	5.0.7	-	5.0.3	-	—	5.0.3	5.0.3
GlobalProtect Portal and Gateway Support for TLSv1.3	6.0.8, 6.1.3,6.2.1 or later versions	6.0.8, 6.1.3,6.2.1 or later versions	6.0.8, 6.1.3,6.2.1 or later versions	6.0.8, 6.1.3,6.2.1, or later versions (Minimum version of Windows 11 required)	6.0.8, 6.1.3,6.2.1, or later versions	—	6.0.8, 6.1.3,6.2.1, or later versions	6.0.8, 6.1.3,6.2.1, or later versions (Ubuntu 20)
User Location Visibility on GlobalProtect Gateways	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	—	4.1.0	4.1.0

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	Windows 365 Cloud PC	macOS	Linux
and Portals								
Gateway and Portal Location Visibility for End Users	5.0.0	5.0.0	—	5.0.0	—	—	5.0.0	—
Primary Username Visiblity on GlobalProtect Gateways	4.0.0	4.0.0	4.0.0	4.0.0	4.0.0	—	4.0.0	4.1.0
Automatic VPN Reconnect for Chromebooks	—	—	4.1.0	—	—	—	—	—
Support for Native Certificate Store for Prisma Access and GloabProtect App on Linux Endpoints	—	—	—	—	—	—	—	6.2.0 or later versions
Enhanced HIP Remediation Process	—	—	—	6.3.0 or later versions	—	—	6.3.0 or later versions	—
Enhancements for Authentication Using	—	—	—	6.3.0 or later versions	—	—	6.3.1 or later versions	—

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	Windows 365 Cloud PC	macOS	Linux
Smart Cards								
Enhancements for Authentication Using Smart Cards-Removal of Multiple PIN Prompts	—	—	—	6.3.0 or later versions	—	—	6.3.0 or later versions	—
Intelligent Portal				6.3 (**Pre-logon (Always On)** connect method only)		—	6.3	
Best Gateway Selection Criteria	—	—	—	6.3.1	—	—	6.3.1	—
CLI Support for SAML Authentication with Default Browser for GlobalProtect App on Linux Endpoints	—	—	—	—	—	—	—	6.2.1 or later versions
Identification and Quarantine of	5.1.0	5.1.0	5.1.0	5.1.0	5.1.0	—	5.1.0	5.1.0

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	Windows 365 Cloud PC	macOS	Linux
Compromised Devices (Deprecates Device Block List)								

What Features Does GlobalProtect Support for IoT?

The following table describes the features supported for GlobalProtect™ IoT by OS:

Feature	Android	Raspbian	Ubuntu	Windows IoT Enterprise
IPSec VPN	√	√	√	√
SSL VPN	√	√	√	√
Pre-Logon Connect Mode	—	—	—	√
User-Logon Connect Mode	√ Certificate or username and password	√ Certificate or username and password	√ Certificate or username and password	√ Certificate or username and password
On-Demand Connect Mode	—	—	—	√
External Gateway Priority by Source Region	√	√	√	√
Internal Gateway Selection by Source IP Address	√	√	√	✓
Internal Mode	√	√	√	√
External Mode	√	√	√	√
IPv4 Addressing	√	√	√	√
IPv6 Addressing	√	√	√	√
Split Tunnel Based on Access Route	√	√	√	√
Split Tunnel Based on Destination	—	—	—	√

Feature	Android	Raspbian	Ubuntu	Windows IoT Enterprise
Domain, Client Process, and Video Streaming Application				
Multiple Portal Support	—	—	—	√
Resilient VPN	√	√	√	√
Pre-Logon Tunnel Rename Timeout	—	—	—	√
Restrict Transparent App Upgrades to Internal Network Connections	√	—	—	√
Enforce GlobalProtect for Network Access	√	—	—	√
Deployment of SSL Forward Proxy CA Certificates in the Trust Store	√	√	√	√
HIP Reports	√	√	√	√
Run Scripts Before and After Sessions	—	√	√	√
Certificate Selection by OID	—	—		√
Allow Users to Disable GlobalProtect	—	—	—	√

Feature	Android	Raspbian	Ubuntu	Windows IoT Enterprise
Multi-Factor Authentication (MFA)	—	—	—	√
SAML Authentication	—	—	—	√
Expired Active Directory (AD) Password Change for Remote Users	—	—	—	√
Active Directory (AD) Password Change Using the GlobalProtect Credential Provider	—	—	—	√
SSO (Credential Provider)	—	—	—	√
Kerberos SSO	—	—	—	√
Welcome and Help Pages	—	—	—	√
Headless-Mode Without Icon, Pop-Up, Dialogs, and UI	√	√	√	√

What GlobalProtect Features Do Third-Party Mobile Device Management Systems Support?

The following table lists the GlobalProtect™ features supported on third-party mobile device management (MDM) systems. A dash ("—") indicates that the feature is not supported.

Feature	Workspace ONE	Microsoft Intune	MobileIron	Google Admin Console	Jamf Pro
GlobalProtect App Deployment	√	√	√	√	√ (macOS only; requires GlobalProtect app 6.1 or later)
Always on VPN Configuration	√ (iOS and Android only)	√ (Android, iOS, and Windows 10 UWP only)	√ (iOS and Android only)	√ (Android only)	—
Remote Access VPN Configuration	√ (iOS and Android only)	√ (Android and iOS only)	√ (iOS only)	√	—
Per-App VPN Configuration	√	√ (Android, iOS, and Windows 10 UWP only)	√ (iOS only)	—	—
MDM Integration with HIP	√	—	—	—	—
VPN Lockdown	√	—	—	—	—

Prisma Access

The following topics provide support information for Prisma® Access:

What Features Does Prisma Access Support?

Prisma Access helps you to deliver consistent security to your remote networks and mobile users. There are two ways that you can deploy and manage Prisma Access:

- **Prisma Access (Managed by Strata Cloud Manager)**—If you're not using Panorama™ software to manage your next-generation firewalls, the Prisma Access app on the hub gives you a simplified way to onboard and manage Prisma Access.
- **Prisma Access (Managed by Panorama)**—If you're already using Panorama software to manage your next-generation firewalls, you can use Panorama to deploy Prisma Access and leverage your existing configurations. However, you'll need the Cloud Services plugin to use Prisma Access (Managed by Panorama).

The features and IPSec parameters supported for Prisma Access vary depending on the management interface you're using—Panorama or the Prisma Access app. You cannot switch between the management interfaces after you activate your Prisma Access license. This means you must decide how you want to manage Prisma Access before you begin setting up the product. Review the Prisma Access Feature Support information to help you select your management interface.

For a description of the features supported in GlobalProtect™, see the features that GlobalProtect supports.

- Prisma Access Feature Support
- Integration with Other Palo Alto Networks Products
- Panorama Managed Multitenant Unsupported Features and Functionality

Prisma Access Feature Support

The following sections provide you with the supported features and network settings for Prisma Access (both Prisma Access (Managed by Strata Cloud Manager) and Prisma Access (Managed by Panorama)).

Management

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
Best Practice Checks	√ Learn more	—
Default Configurations Default settings enable you to get started quickly and securely	√ Examples include: • Default DNS settings • Default GlobalProtect settings, including for the Prisma Access portal • Default Prisma Access infrastructure settings	—
Built-in Best Practice Rules To ensure that your network is as secure as possible, enable your users and applications based on best practice templates. With best practices as your basis, you can then refine policy based on your enterprise needs.	√ Features with best practice rules include: • Security rules • Security profiles • Decryption • M365	—
Onboarding Walkthroughs for First-Time Setup	√ Learn more Guided walkthroughs include: • Onboard Remote Networks • Onboard Mobile Users (GlobalProtect) • Onboard Your HQ or Data Centers • Turn on Decryption	—
Centralized Management Dashboards These can include best practice scores and usage information	√ Dashboards are available for features including: • Security Policy • Security Profiles • Decryption	—

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
	• Authentication • Certificates • SaaS Application Management	
Hit Counts	√ Hit counts for Security profiles include counts that measure the profile's effectiveness, and these can depend on the profile (for example, unblocked critical and high severity vulnerabilities, or WildFire submission types).	√ Learn more
Policy Rule Usage	√	
Policy Optimizer	√	√
Profile Groups	√ Learn more	√
Configuration Table Export	—	√

Remote Networks

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
IPSec Tunnels See the list of Supported IKE Cipher Suites. We do not support FQDNs for peer IPSec addresses; use an IP address for the peer address instead.	√	√
Secure Inbound Access	√ Learn more	√ Learn more
Tunnel Monitoring		
Dead Peer Detection (DPD)	√	√
ICMP	√	√
Bidirectional Forwarding Detection (BFD)	—	—
SNMP Use Tunnel Monitoring instead of SNMP to monitor the tunnels in Prisma Access.	—	—

Service Connections

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
IPSec Tunnels See the list of Supported IKE Cipher Suites.	√	√ We do not support FQDNs for peer IPSec addresses; use an IP address for the peer address instead.
Tunnel Monitoring		
Dead Peer Detection (DPD)	√	√
ICMP	√	√
Bidirectional Forwarding Detection (BFD)	—	—
SNMP Use Tunnel Monitoring instead of SNMP to monitor the tunnels in Prisma Access.	—	—
Traffic Steering (using policy-based forwarding rules to forward internet-bound traffic to service connections)	√ Learn more	√ Learn more Introduced in 1.7.

Mobile Users—GlobalProtect

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
Using On-Premises Gateways (Hybrid Deployments)		
On-premises gateway integration with Prisma Access	√	√ We support using on-premises gateways with Prisma Access gateways.
Priorities for Prisma Access and On-Premises Gateways	√	√ Supported for deployments that have on-premises GlobalProtect gateways. You can set a priority separately for on-premises gateways and collectively for all gateways in Prisma Access. You can also specify source regions for on-premises gateways.
Manual Gateway Selection Users can manually select a cloud gateway from their client machines using the GlobalProtect app.	√ Learn more	√ Learn more
GlobalProtect Gateway Modes		
External Mode	√	√
Internal Mode	√ Introduced in 5.1 Preferred and Innovation. If you are running a version below 5.1 Innovation, you can add one or more on-premise gateways and configure them as internal gateways.	√ Introduced in 5.1 Preferred and Innovation. If you are running a version below 5.1 Innovation, you can add one or more on-premise gateways and configure them as internal gateways.

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
GlobalProtect App Connect Methods		
User-Logon (always on)	√	√
Pre-Logon (always on)	√	√
Pre-Logon (then on-demand)	√	√
On-Demand	√	√
Clientless VPN		
Clientless VPN	√ Learn more	√ Learn more
Mobile User—GlobalProtect Features		
Support for Mutliple Username Formats	√	√
Mobile Device Management (MDM)	—	√ Learn more
MDM Integration with HIP Prisma Access does not support AirWatch MDM HIP service integration; however, you can use the GlobalProtect App for iOS and Android MDM Integration for HIP-Based Policy Enforcement	√	√
Optimized Split Tunneling for GlobalProtect	√	√
Administratively Log Out Mobile Users	√	√ Learn more Introduced in 1.4.
DHCP Prisma Access uses the IP address pools you specify during mobile user setup to assign IP addresses to	—	—

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
mobile users and does not use DHCP.		
GlobalProtect App Version Controls	√ One-click configuration for GlobalProtect agent log collection	√ Learn more

Mobile Users—Explicit Proxy

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
Explicit Proxy Support	√ Learn more	√ Learn more Introduced in 2.0 Innovation.
Explicit Proxy Connectivity in GlobalProtect for Always-On Internet Security	√ Learn more Introduced in 4.0 Preferred with GlobalProtect app version 6.2	√ Learn more Introduced in 4.0 Preferred with GlobalProtect app version 6.2

Security Services

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
Security Policy	√	√
DoS Protection The Prisma Access infrastructure manages DoS protection.	√	√
SaaS Application Management	√ Learn more Supported for: • Microsoft 365 apps *Includes a guided walkthrough to safely enable M365* • Google apps • Dropbox • YouTube	–
IoT Security	√	√
Security Profiles		
Supported Profile Types	√ • Antispyware • DNS Security • Vulnerability Protection • WildFire and Antivirus • URL Filtering Domain Credential Filter detection is not supported with URL filtering. • File Blocking • Data Loss Prevention (DLP)	√ • Antispyware • DNS Security (enabled via an Antispyware profile) • Vulnerability Protection • Antivirus • WildFire • URL Filtering Domain Credential Filter detection is not supported with URL filtering. • File Blocking

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
	• HTTP Header Insertion	• Data Loss Prevention (DLP)
Dashboards for Security Profiles	√ Learn more Dashboards are tailored to each profile, and give you: • centralized management for security service features • visibility into profile usage and effectiveness • access to cloud databases (search for threat coverage, for example)	–
Best Practice Scores for Security Profiles	√ Learn more	–
Response pages	√	√ We support HTTP response pages for mobile users and users at remote networks. To use HTTPS response pages, open a CLI session in the Panorama that manages Prisma Access, enter the **`set template Mobile_User_Template config deviceconfig settingssl-decrypt url-proxyyes`** command in configuration mode, and commit your changes.
HTTP Header Insertion		
HTTP Header Insertion Profiles	√	√
Decryption		
Decryption Policies	√	√
Decryption Profiles	√	√

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
Automatic SAN Support for SSL Decryption	√	√
SSL Forward Proxy	√	√
SSL Inbound Inspection	—	√
SSH Proxy	—	√
Guided Walkthrough: Turn on Decryption	√	—

Network Services

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
Network Services		
Quality of Service (QoS) Prisma Access uses the same QoS policy rules and QoS profiles and supports the same DSCP markings as Palo Alto Networks Next-Generation Firewalls.	√	√ We introduced QoS for Remote network deployments that allocate bandwidth by compute location in 3.0 Preferred.
Application Override	√	√
IPv4 Addressing	√	√
IPv6 Addressing IPv6 addressing for private apps introduced in 2.2 Preferred; IPv6 addressing for public (internet) and private apps introduced in 5.2.1.	√	√
Split Tunnel Based on Access Route	√	√
Split Tunnel Based on Destination Domain, Client Process, and Video Streaming Application	√	√
NetFlow	—	—
NAT Prisma Access automatically manages outbound NAT; you cannot configure the settings.	√	√
SSL VPN Connections	√	√
Routing Features		

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
Static Routing	√	√
Dynamic Routing (BGP)	√	√
Dynamic Routing (OSPF)	—	—
High Availability		
High availability	*Palo Alto Networks maintains Availability.*	√
SMTP	√ Prisma Access sometimes blocks SMTP port 25 for security reasons and to mitigate the risk from known vulnerabilities that exploit nonsecure SMTP. Palo Alto Networks recommends using ports 465, 587, or an alternate port 2525 for SMTP.	√ Prisma Access sometimes blocks SMTP port 25 for security reasons and to mitigate the risk from known vulnerabilities that exploit nonsecure SMTP. Palo Alto Networks recommends using ports 465, 587, or an alternate port 2525 for SMTP.

Identity Services

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
Authentication Types		
SAML	√	√
Cloud Identity Engine	√	√
TACACS+	√	√
RADIUS	√	√
LDAP	√	√ On-Premises LDAP Authentication
Kerberos	√ We support Kerberos only on Windows clients.	√ Kerberos SSO
MFA	√	√ Multi-Factor Authentication (MFA)
Local Database Authentication	√	√
Authentication Features		
Authentication Rules	√	√
Authentication Portal	√	√
Certificate-Based Authentication	√ Supported for both IPSec and mobile users with GlobalProtect.	√ Supported for both IPSec and mobile users with GlobalProtect.
RADIUS Vendor-Specific Attributes (VSAs)	—	—

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
Framed IP-Address retrieval from a RADIUS server	—	—
Extensible Authentication Protocol (EAP) Support for RADIUS	√	√
Single Sign-On (SSO)	√	√
Terminal Server (TS) Agent	√ Supported for the following platforms: • Citrix XenApp 7.*x* • Windows Server 2019 • Windows 10 Enterprise Multi-session We support a maximum of 400 TS agents.	√ Supported for the following platforms: • Citrix XenApp 7.*x* • Windows Server 2019 • Windows 10 Enterprise Multi-session We support a maximum of 400 TS agents.
Cloud Identity Engine (Directory Sync Component)		
Directory Sync for User and Group-Based Policy	√ Supports on-premises Active Directory and Azure Active Directory. • Learn more	√ You can retrieve user and group information using the Directory Sync component of the Cloud Identity Engine. Prisma Access supports on-premises Active Directory, Azure Active Directory, and Google IdP. Introduced in 1.6. Support for Azure Active Directory introduced in 2.0 Preferred. Support for Google IdP introduced in 3.0 Preferred and Innovation.
Identity Redistribution • IP address-to-username mappings	√	√

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
• HIP • Device Quarantine • IP-Tag • User-Tag		
Ingestion of IP address-to-username mappings from a third-party integration (NAC)	—	√
Include username in HTTP header insertion entries	√	√ Introduced in 1.7. Requires Panorama running a minimum PAN-OS 9.1.1 version.

Policy Objects

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
Addresses	√	√
Address Groups	√	√
Dynamic Address Groups (DAGs) and Auto-Tags	—	—
XML API - Based Dynamic Address Group Updates	—	√
Regions	√	√
Dynamic User Groups (DUGs)	√	√
App-ID (Applications)	√	√
Simplified Application Dependency Workflow (App Dependency tab for commits)	√	— We do not support commit warnings for Prisma Access.
Service-Based Session Timeouts	√	√ Learn more
Application Groups	√	√
Application Filters	√	√
Services	√	√
Service Groups	√	√
Tags	√	√
Streamlined Application-Based Policy (Tag-based application filters)	√	√ Introduced in 1.7. Requires Panorama running a minimum PAN-OS 9.1.1 version.
Auto-Tag Actions	√	√

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
HIP Objects		
HIP	√	√
HIP Match Log	√	√
HIP-Based Security Policy	√	√
HIP Notifications	√	√
HIP Report Submission	√	√
HIP Checks	√	√
HIP Report Viewing	—	√ Introduced in 1.5.
HIP Redistribution	√	√ Introduced in 1.5.
HIP Objects and Profiles	√	√
External Dynamic Lists	√	√
Certificate Management		
Custom Certificates	√	√
Palo Alto Networks Issued Certificates	√	√
Certificate Profiles	√	√
Custom Certificates	√	√
SSL/TLS Service Profiles	√	√
SSL We support SSL only for mobile users, not for site-to-site VPNs.	√	√
SCEPs	√	√

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
OCSP Responders	√	√
Default Trusted Certificate Authorities	√	√

Logs

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
Enhanced Application Logging	√	√
Strata™ Logging Service (formerly Cortex® Data Lake) Log Storage	√	√
Forward logs stored in Strata Logging Service to syslog and email destinations	√	√
Log Forwarding Profiles	√ Default Log Forwarding profile	√ We do not support HTTP, SNMP, auto-tagging in Built-in Actions.
Enhanced Mobile Users Visibility for Administrators (GlobalProtect logs)	√	√ Introduced in 1.7. Requires Panorama running a minimum PAN-OS 9.1.1 version.

Reports

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
Reports	√ Learn More You can also use Dashboards for a comprehensive view of the applications, ION devices, threats, users, and security subscriptions at work in your network.	√ Learn more Introduced in Prisma Access 1.8.
App Report	√ Learn more	√ Learn more This feature has the following Strata Logging Service-based limitation: **SaaS Application Usage** report (**Monitor** > **PDF Reports** > **SaaS Application Usage**)—You cannot filter the logs for user groups (we do not support the **Include user group information in the report** option).
Usage Report	√ Learn more	√ Learn more
User Activity Report	√ Learn more	√ Learn more
Best Practices Report	√ Learn more	√
WildFire Reports	√ Learn More	√ Support introduced in 2.0 Innovation.

Integration with Other Palo Alto Networks Products

Feature	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)
Cortex XSOAR integration	–	√ We support source IP-based allow lists and malicious user activity detection.
Enterprise Data Loss Prevention (DLP) integration	√	√
Cortex XDR integration	√ Prisma Access is compatible with the Cortex XDR version of Strata Logging Service. Cortex XDR receives Prisma Access log information from Strata Logging Service (formerly Cortex Data Lake).	√ Prisma Access is compatible with the Cortex XDR version of Strata Logging Service. Cortex XDR receives Prisma Access log information from Strata Logging Service (formerly Cortex Data Lake).
Prisma SaaS integration	√ We support SaaS visibility with Strata Logging Service.	√ We support SaaS visibility with Strata Logging Service.

Panorama Managed Multitenant Unsupported Features and Functionality

We do not support the following features in a Prisma Access (Managed by Panorama) multitenant deployment:

- Dynamic DNS Registration Support for Mobile Users—GlobalProtect
- IoT Security
- ZTNA Connector

In addition, a Panorama managed multitenant deployment has changes to the following functionality:

- You cannot view your Panorama managed tenants under Common Services: Tenant Management.
- For Prisma Access (Managed by Panorama), continue to use Panorama for managing Prisma Access and the admin access that Panorama controls locally. You cannot manage users, roles, and services accounts using Common Services: Identity and Access for Prisma Access (Managed by Panorama). However, you can use Common Services: Identity and Access for managing other apps such as ADEM and Insights.
- You cannot use the Prisma Access APIs in pan-dev.

The following Prisma Access components and add-ons have the following caveats when used in a multitenant deployment:

- For Prisma Access—Explicit Proxy deployments, if you have an existing Prisma Access non-multitenant deployment and convert it to a multitenant deployment, only the first tenant (the tenant you migrated) supports Explicit Proxy. Any subsequent tenants you create for the multitenant deployment after the first one do not support Explicit Proxy.
- SaaS Security and Enterprise Data Loss Prevention (Enterprise DLP) support multitenancy with the following restrictions:
  - Only a superuser on Panorama can create DLP profiles and patterns and can associate DLP profiles to Security policy rules for tenants.
  - A superuser must commit all changes to Panorama whenever they make changes in DLP profiles and patterns.
  - All tenants share a single copy of profiles and pattern configurations and, therefore, changes occur on all tenants.
  - Since Security policy rules can be different across tenants, each tenant can have different data filtering profiles associated with Security policy rules.
- If you enable high availability (HA) with active and passive Panorama appliances in a multitenant deployment, you cannot change the HA pair association after you enable multitenancy.

- You can use these features with a Prisma Access (Managed by Panorama) multitenant deployment; however you can only use them in one tenant per multitenant deployment:
  - Prisma SD-WAN, including CloudBlade and Easy Onboarding (non-CloudBlade) deployments
  - Configuring multiple portals in Prisma Access

Prisma Access and Panorama Version Compatibility

This section provides you with the minimum and maximum versions of Panorama™ to use with Prisma® Access.

- Supported IKE Cipher Suites
- Minimum Required Panorama Software Versions

Supported IKE Cipher Suites

The following table documents the IKE cryptographic settings that we support with Prisma Access.

Component	Phase 1 Supported Crypto Parameters	Phase 2 Supported Crypto Parameters
Encryption	3des aes-128-cbc aes-192-cbc aes-256-cbc aes-128-gcm aes-256-gcm	null (not recommended) 3des aes-128-cbc aes-192-cbc aes-256-cbc aes-128-gcm aes-256-gcm
Authentication	non-auth *If you select an AES with Galois/Counter Mode (AES-GCM) algorithm for encryption, you must select the Authentication setting **non-auth** or the commit will fail. The hash is automatically selected based on the DH Group selected. DH Group 19 and below uses **sha256**; DH Group 20 uses **sha384**.* md5 sha1 sha256	md5 none *If you select an AES-GCM algorithm for encryption, you must select **none** for Phase 2 authentication or the commit will fail. The hash is automatically selected based on the DH Group selected. DH Group 19 and below uses **sha256**; DH Group 20 uses **sha384**.* sha1 sha256 sha384

Component	Phase 1 Supported Crypto Parameters	Phase 2 Supported Crypto Parameters
	sha384 sha512	sha512
DH Group	Group 1 Group 2 Group 5 Group 14 Group 19 Group 20	No PFS *(not recommended)* Group 1 Group 2 Group 5 Group 14 Group 19 Group 20
Security Association (SA) Lifetime	Configurable	Configurable
SA Lifebytes	N/A	Configurable

Minimum Required Panorama Software Versions

The Cloud Services plugins require the following minimum Panorama™ software versions.

For more information about the versions used with Prisma Access, including the recommended Panorama and GlobalProtect versions, see the Prisma Access Release Notes for your Release:

- Prisma Access 6.0
- Prisma Access 5.2
- Prisma Access 5.1
- Prisma Access 5.0, 5.0.1, 4.0, 4.1, and 4.2

Cloud Services Plugin Version	Minimum Required Panorama Version
6.0 Preferred and Innovation	• PAN-OS 11.2.6 (Prisma Access 6.0 runs the 11.2.6 dataplane) • PAN-OS 11.1.0 • PAN-OS 11.0.1 • PAN-OS 10.2.10
5.2 and 5.2.1 Preferred and Innovation	• PAN-OS 11.2.4 (the minimum version required for 5.2.1 Innovation) • PAN-OS 11.2.3 (the minimum version required for 5.2 Innovation) • PAN-OS 11.1.0 • PAN-OS 11.0.1 • PAN-OS 10.2.10 (the minimum version required for 5.2 and 5.2.1 Preferred)
5.1 and 5.1.1 Preferred and Innovation	• PAN-OS 11.2 (the minimum version required for 5.1 and 5.1.1 Innovation) • PAN-OS 11.1.0 • PAN-OS 11.0.1 • PAN-OS 10.2.4 (the minimum version required for 5.1 and 5.1.1 Preferred)
4.0, 4.1, and 4.2 Preferred 5.0 and 5.0.1 Preferred and Innovation	• PAN-OS 11.1.0 • PAN-OS 11.0.0 Running Panorama with PAN-OS 11.0 or PAN-OS 11.1 does not give you access to PAN-OS 11.0 features in Prisma Access. • PAN-OS 10.2.3

Cloud Services Plugin Version	Minimum Required Panorama Version
	• PAN-OS 10.1.7 You must have a Panorama appliance running PAN-OS 10.2 to take advantage of the PAN-OS 10.2 features in Prisma Access. *For Panorama versions supported and required for FedRAMP deployments, see* Prisma Access FedRAMP Requirements.

Prisma SD-WAN

These tables provide version and compatibility details for Prisma SD-WAN ION Devices and Releases.

- ION Release versions on the Prisma SD-WAN Hardware and Virtual ION Devices
- Virtual ION Form Factors on the Cloud Platforms
- Prisma Access, Cloud Services Plugin, and PAN OS versions for Prisma Access for Networks CloudBlades
- Prisma Access and Panorama Integration Plugin Versions for Prisma SASE Easy Onboarding

Table 1: ION Release Versions on the Prisma SD-WAN Hardware and Virtual ION Devices

Palo Alto Networks Prisma SD-WAN ION Device Models	ION Release 5.6.1 or Higher	ION Release 6.1.1 or Higher	ION Release 6.1.3 or Higher	ION Release 6.2.1 or Higher	ION Release 6.3.1 or Higher	ION Release 6.4.2 or Higher	ION Release 6.5.1 or Higher
ION 1000	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ION 2000	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ION 3000	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ION 7000*	Yes	Yes	Yes	Yes	Yes	No	No
ION 9000	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ION 1200	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ION 1200-C-NA	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ION 1200-C-ROW	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ION 1200-C5G-EXP	—	—	Yes	Yes	Yes	Yes	Yes
ION 1200-S	—	Yes	Yes	Yes	Yes	Yes	Yes
ION 1200-S-C-NA	—	Yes	Yes	Yes	Yes	Yes	Yes
ION 1200-S-C-ROW	—	Yes	Yes	Yes	Yes	Yes	Yes

Palo Alto Networks Prisma SD-WAN ION Device Models	ION Release 5.6.1 or Higher	ION Release 6.1.1 or Higher	ION Release 6.1.3 or Higher	ION Release 6.2.1 or Higher	ION Release 6.3.1 or Higher	ION Release 6.4.2 or Higher	ION Release 6.5.1 or Higher
ION 1200-S-C5G-WW	—	Yes	Yes	Yes	Yes	Yes	Yes
ION 3200	—	Yes	Yes	Yes	Yes	Yes	Yes
ION 3200H	—	—	—	—	—	Yes	Yes
ION 3200H-C5G-WW	—	—	—	—	—	Yes	Yes
ION 5200	—	Yes	Yes	Yes	Yes	Yes	Yes
ION 9200	—	Yes	Yes	Yes	Yes	Yes	Yes
ION 3102V	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ION 3104V	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ION 3108V	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ION 7108V	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ION 7116V	No	No	No	No	No	No	Yes

*Note: Last Supported release for ION 7000 is 5.6.x. For customers with ION 7000 devices already running software versions 6.1.x, 6.2.x or 6.3.x, it is recommended to maintain the sustained CPU load at or below 50% for branch deployments for stable operations.

Table 2: Virtual ION Form Factors on the Cloud Platforms

vION Model	OpenStack	ESXi	AWS	Azure	GCP
ION 3102V	Yes	Yes	Yes	Yes	Yes
ION 3104V	Yes	Yes	Yes	Yes	Yes
ION 3108V	Yes	Yes	Yes	Yes	Yes
ION 7108V	Yes	Yes	Yes	Yes	Yes
ION 7116V	Yes	Yes	Yes	Yes	Yes

Table 3: Prisma Access, Cloud Services Plugin, and PAN OS Versions for Prisma Access for Networks CloudBlades

Prisma SD-WAN CloudBlade	Prisma Access	Recommended Minimum Version of Cloud Services Plugin	Supported PAN OS Versions
Prisma Access for Networks (Panorama Managed) 4.0.0	6.0	>=6.0.0-h3	PAN-OS 9.1.4 or a later PAN-OS 9.1 PAN-OS 10.0.3 or a later PAN-OS 10.0 PAN-OS 10.1.7 and 10.1.8 PAN-OS 10.2.3-H2 PAN-OS 11.1.3, 11.1.5 and 11.1.6 PAN-OS 11.2
	5.2	>=5.2.0-h24	
	5.1	>=5.1.0-h26	
	5.0	>=5.0.0-h48	
	4.1	>=4.1.0-h72	
	4.0	>=4.0.0-h72	
	3.2	>=3.2.1-h83	
Prisma Access for Networks (Panorama Managed) 3.1.6	5.2	any latest on 5.2.0	
	5.1	>=5.1.0-h26	
	5	>=5.0.0-h48	
	4.1	>=4.1.0-h72	
	4.0	>=4.0.0-h72	
	3.2	3.2.0-h42 and 3.2.1-h70	
	3.1	>=3.1.0-h52	
	3	>=3.0.0-h29	
	2.2	>=2.2.0-h48 Preferred	
Prisma Access for Networks (Cloud Managed) 3.1.6	2.1.2 or later with Aggregate Bandwidth	—	—

Table 4: Prisma Access and Panorama Integration Plugin Versions for Prisma SASE Easy Onboarding

Prisma Access Version	Panorama Integration Plugin
10.2.4	cloud_services-5.2.0-h24

Strata Cloud Manager and Panorama Feature Parity

Strata Cloud Manager and Panorama both enable you to centrally manage large-scale firewall deployments. These are the features each supports.

- Software
- Management
- Optimization
- Reporting
- Hardware
- Cloud-Delivered Security Services
- Cloud

Software

Feature	Strata Cloud Manager	Panorama
PAN-OS 11.0 support	Yes	Yes
PAN-OS 10.2 support	Yes (PAN-OS 10.2.3 minimum)	Yes
PAN-OS 10.1 support	No	Yes
PAN-OS 9.1 support	No	Yes
VM-Series support	Yes (VM Flex support)	Yes
CN-Series support	No	Yes
Cloud NGFW support	Yes	Yes
Prisma Access	Yes	Yes

Management

Feature	Strata Cloud Manager	Panorama
Proxied Management Connection	Yes (requires internet connectivity)	Yes
Dynamic Address Groups	Yes	Yes

Dynamic User Groups	Yes	Yes
Reusable Configuration Snippets	Yes	No
Templates	No	Yes
REST API	Yes	Yes
Log Collectors	Strata Logging Service is supported by default	Yes
Application Command Center	Equivalent functionality through Activity Insights	Yes
Context Switching	No	Yes
Local Config Management	No	No
Multi-VSYS	No	Yes
PAN-OS SD-WAN	Yes	Yes
Automated VPN creation	Yes (no extra licensing required)	Requires SD-WAN license

Optimization

Feature	Strata Cloud Manager	Panorama
Policy Optimizer	Yes	No
Rule Hit Counts	Captures the number of days that the policy rule is not triggered	Yes
Unused Rules	Yes	No
Unused Objects	Yes	No

Reporting

Feature	Strata Cloud Manager	Panorama
Report Scheduler	Yes	Yes
Custom Reports	No	Yes

Custom Dashboards	Yes	No

Hardware

Feature	Strata Cloud Manager	Panorama
Gen 4 Hardware Support	Yes	Yes
Gen 3 Hardware Support	Yes (requires manual Device Certificate retrieval)	Yes
Gen 2 Hardware Support	No	Yes

Cloud-Delivered Security Services

Feature	Strata Cloud Manager	Panorama
Device Security	Yes	Yes
Enterprise DLP	Yes	Yes
SaaS Inline	Yes	Yes
DNS Security	Yes	Yes
Advanced Threat Prevention	Yes	Yes
Advanced URL Filtering	Yes	Yes
Advanced WildFire	Yes	Yes
AIOps for NGFW	Yes	Yes
Strata Logging Service	Yes	Yes
SaaS Application Endpoints	Yes	No
Bootstrap Onboarding	Yes (yet to be released)	Yes

Cloud

Feature	Strata Cloud Manager	Panorama
Cloud Provider Tag Harvesting	Yes	Yes

Identity

Feature	Strata Cloud Manager	Panorama
Cloud Identity Engine	Yes	Yes

User-ID Agent

You install the User-ID™ agent on a domain server that is running a supported operating system (OS) and then connect the User-ID agent to exchange or directory servers.

Where Can I Install the User-ID Agent?

The following table shows the operating systems on which you can install each release of the Windows-based User-ID™ agent. The system must also meet the minimum requirements (see the User-ID agent release notes).

Operating System	Release 9.1	Release 10.1	Release 10.2	Release 11.0
Windows Server 2022	√ 9.1.4 & later	√	√	√
Windows Server 2019	√	√	√	√
Windows Server 2016	√	√	√	√
Windows Server 2012 and 2012 R2	√	√	√	√

Which Servers Can the User-ID Agent Monitor?

The following are the exchange and directory servers you can monitor with the PAN-OS® integrated and Windows-based User-ID™ agents:

You can install only specific releases of the Windows-based User-ID agent on supported Microsoft Windows servers.

Server	Versions Supported

Microsoft Exchange Server	• 2019—Only with Windows User-ID agent 9.0.2 and later releases or with PAN-OS integrated User-ID agents running the following PAN-OS releases:
	  • PAN-OS 11.0 (all releases)
	  • PAN-OS 10.2 (all releases)
	  • PAN-OS 10.1 (all releases)
	  • PAN-OS 9.1 (all releases)
	• 2016—Only with Windows User-ID agent or with PAN-OS integrated User-ID agents running the following PAN-OS releases:
	  • PAN-OS 11.0 (all releases)
	  • PAN-OS 10.2 (all releases)
	  • PAN-OS 10.1 (all releases)
	  • PAN-OS 9.1 (all releases)
	• 2013

Microsoft Windows Server	• 2022—Only with Windows User-ID agent or with PAN-OS integrated User-ID agents running the following PAN-OS releases:
	  • PAN-OS 11.0 (all releases)
	  • PAN-OS 10.2.1 and later PAN-OS 10.2 releases
	  • PAN-OS 10.1.1 and later PAN-OS 10.1 releases
	  • PAN-OS 9.1.4 and later PAN-OS 9.1 releases
	• 2019—Only with Windows User-ID agent 9.1 and later versions or with PAN-OS integrated User-ID agents running the following PAN-OS releases:
	  • PAN-OS 11.0 (all releases)
	  • PAN-OS 10.2 (all releases)
	  • PAN-OS 10.1 (all releases)
	  • PAN-OS 9.1 (all releases)

Server	Versions Supported

	• 2016—Only with Windows User-ID agent or with PAN-OS integrated User-ID agents running the following PAN-OS releases:
	  • PAN-OS 11.0 (all releases)
	  • PAN-OS 10.2 (all releases)
	  • PAN-OS 10.1 (all releases)
	  • PAN-OS 9.1 (all releases)
	• 2012 and 2012 R2

Novell eDirectory Server	8.8

Where Can I Install the User-ID Credential Service?

The following table shows the Read-Only Domain Controller (RODC) on which you can install each release of the Windows User-ID™ agent with the User-ID credential service to detect credential submissions. The credential service is an add-on for the Windows User-ID agent; you must install the add-on separately.

Server	PAN-OS Version Supported	Windows User-ID Agent Version Supported
Windows Server 2022	• 11.0	• 11.0
Windows Server 2019	• 11.0 • 10.2.3 • 10.1.11 • 10.0.11-h1* • 10.1.7 • 9.1.15	• 11.0 • 10.2.1 • 10.1.2 • 10.1.1 • 9.1.4

Terminal Server (TS) Agent

You install the Terminal Server (TS) agent on a domain server that is running a supported operating system (OS) and then report username-to-port mapping information to PAN-OS® firewalls.

Where Can I Install the Terminal Server (TS) Agent?

The following table shows the operating systems on which you can install each release of the Terminal Server (TS) agent.

For optimal configuration, install the TS agent version that matches the PAN-OS version running on your firewall. If there is not a TS agent version that matches your PAN-OS version, install the latest version that is closest to the PAN-OS version.

Operating System	TS Agent 9.1	TS Agent 10.1	TS Agent 10.2	TS Agent 11.0
Windows Server 2022	√ 9.1.4 & later	√	√	√
Windows Server 2019	√	√	√	√
Windows Server 2016	√	√	√	√
Windows Server 2012 R2	√	√	√	√
Windows 11 Enterprise Multi-session	√ 9.1.4 & later	√	√	√
Windows 10 Enterprise Multi-session	√ 9.1.1 & later	√	√	√
Citrix Metaframe Presentation Server 4.x	√	√	√	√
Citrix XenApp 5.x	√	√	√	√
Citrix XenApp 6.x	√	√	√	√
Citrix XenApp 7.x	√	√	√	√

How Many TS Agents Does My Firewall Support?

The following table shows how many Terminal Server (TS) agents each hardware-based and VM-Series firewall supports. To confirm which PAN-OS® releases are supported on your firewall, review the Supported PAN-OS releases for each model.

For optimal configuration, install the TS agent version that matches the PAN-OS version running on the firewall. If there is not a TS agent version that matches the PAN-OS version, install the latest version that is closest to the PAN-OS version.

Firewall or VM Model	PAN-OS 9.1	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
Hardware Firewalls				
PA-7000 Series	2,000	2,000	2,000	2,000
PA-7000 Series with SMC-B	2,500	2,500	2,500	2,500
PA-5450	—	2,500	2,500	2,500
PA-5440	—	—	—	2,500
PA-5410, PA-5420, and PA-5430	—	—	2,500	2,500
PA-5200 Series	2,500	2,500	2,500	2,500
PA-3430 and PA-3440	—	—	2,000	2,000
PA-3410 and PA-3420	—	—	400	400
PA-3200 Series	2,000	2,000	2,000	2,000
PA-1400 Series	—	—	—	400
PA-800 Series	1,000	1,000	1,000	1,000
PA-460	—	1,000	1,000	1,000
PA-450	—	400	400	400
PA-445	—	—	—	800
PA-440	—	800	800	800
PA-415	—	—	—	400

Firewall or VM Model	PAN-OS 9.1	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
PA-410	—	400 10.1.2 & later	400	400
PA-220R	400	400	400	400
PA-220	400	400	400	—
VM-Series Firewalls				
VM-700	2,500	2,500	2,500	2,500
VM-500	2,000	2,000	2,000	2,000
VM-300	400	400	400	400
VM-100	400	400	400	400
VM-50 Lite	400	400	400	400

Strata Logging Service Software Compatibility

To forward firewall log data to Strata Logging Service (formerly Cortex® Data Lake), you must ensure that your firewalls are running a supported PAN-OS® version. The PAN-OS version you need depends on whether you use Panorama™ to onboard several firewalls simultaneously or you onboard firewalls individually.

To onboard firewalls to Strata Logging Service using Panorama, you must also install a supported version of the Cloud Services plugin. If you use the Cloud Services plugin to enable Prisma® Access, ensure that your Panorama is running supported versions of PAN-OS and the Cloud Services plugin.

Version Requirements for Panorama Managed Firewalls

Software versions required to integrate a Panorama-managed deployment with Strata Logging Service.

Software	Version	Description
PAN-OS*	Minimum: 9.1	To forward logs from Panorama-managed firewalls to Strata Logging Service, both Panorama and the firewalls must run PAN-OS 9.1 or a later supported PAN-OS version. For enhanced application logging and more reliable service, upgrade to PAN-OS 9.1 or a later supported PAN-OS version.
Cloud Services plugin	Minimum: 1.5.0-h6 Recommended: the latest version	The Cloud Services plugin enables you to send log data from Panorama-managed firewalls. To download the plugin, see the step describing how to install the plugin when you configure Panorama for Strata Logging Service. *Ensure that your Panorama is running a PAN-OS version that supports your Cloud Services plugin version. Failure to do so can result in a loss of data.*

Version Requirements for Individually Managed Firewalls

Software	Version	Description
PAN-OS	Minimum: PAN-OS 9.1	Individually managed firewalls must run PAN-OS 9.1 or a later supported PAN-OS version to authenticate to Strata Logging Service.
Content Version	Minimum: 8274	Install the latest content updates to ensure your firewall can authenticate to Strata Logging Service.

Cortex XDR

Compatibility information for Cortex XDR® has a new home. Going forward, when you click the links below, you will be redirected to the Palo Alto Networks docs-cortex website.

- Where Can I Install the Cortex XDR Agent?
- Cortex XDR Supported Kernel Module Versions by Distribution
- Cortex XDR and Traps Compatibility with Third-Party Security Products

Endpoint Security Manager (ESM)

You can install the Traps™ agent, now known as the Cortex XDR® agent, and the Endpoint Security Manager (ESM) Components (comprised of the ESM Console, one or more ESM Servers, and the database) only on servers and endpoints that are running a supported operating system (OS).

Where Can I Install the Endpoint Security Manager (ESM)?

The Endpoint Security Manager (ESM) comprises the ESM Console, one or more ESM Servers, and a database and is now documented with the Cortex® XDR agent.

Compatibility information for Cortex XDR (and Traps) has a new home. Going forward, you can determine Endpoint Operating Systems Supported with Cortex XDR and Traps *by going to the* Palo Alto Networks docs-cortex website*.*

Where Can I Install the Cortex XDR Agent?

The Traps™ agent is now the Cortex XDR® agent in Cortex XDR agent release 7.0 and later releases.

Compatibility information for Cortex XDR (and Traps) has a new home. Going forward, you can determine where you can install the Cortex XDR agent *by going to the* Palo Alto Networks docs-cortex website.

IPv6 Support by Feature

Use the following table to review PAN-OS® features (listed by category) that support IPv6 traffic.

- Security
- Management & Panorama
- SD-WAN
- Networking
- VPN
- Host Dynamic Address Configuration
- Device
- User-ID™

PAN-OS Feature	PAN-OS 9.1	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
Security						
WildFire® Appliance	—	√	√	√	√	√
App-ID™ and Firewalling in Layer 2 and Layer 3	√	√	√	√	√	√
User-ID™	√	√	√	√	√	√
Content-ID™	√	√	√	√	√	√
Block IPv6 in IPv4 Tunneling (via App-ID)	√	√	√	√	√	√
Zone Protection	√	√	√	√	√	√
Packet-Based Attack Protection	√	√	√	√	√	√
Reconnaissance Protection	√	√	√	√	√	√
URL Filtering	√	√	√	√	√	√
SSL Decryption	√	√	√	√	√	√
SSH Decryption	√	√	√	√	√	√

PAN-OS Feature	PAN-OS 9.1	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
DoS Rulebase	√	√	√	√	√	√
IPv6 Access to PAN-DB	√	√	√	√	√	√
DNS Sinkhole	√	√	√	√	√	√
External Dynamic List (EDL)	√	√	√	√	√	√
Management & Panorama™						
SSH Management (dedicated MGMT port)	√	√	√	√	√	√
Web Interface Management (dedicated MGMT port)	√	√	√	√	√	√
Interface Management (ping, telnet, ssh, http, https - all ports)	√	√	√	√	√	√
Device to Panorama SSL TCP Connection	√	√	√	√	√	√
Panorama HA Connection Between Peers	√	√	√	√	√	√
DNS	√	√	√	√	√	√
Dynamic DNS Support for Firewall Interfaces (DHCP-based interfaces)	√	√	√	√	√	√
RADIUS	√	√	√	√	√	√
LDAP	√	√	√	√	√	√
SYSLOG	√	√	√	√	√	√
SNMP	√	√	√	√	√	√
NTP	√	√	√	√	√	√
Device DNS (device only)	√	√	√	√	√	√
DNS Proxy	√	√	√	√	√	√

PAN-OS Feature	PAN-OS 9.1	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
Reporting and Visibility in to IPv6	√	√	√	√	√	√
IPv6 Address Objects	√	√	√	√	√	√
IPv6 FQDN Address Objects	√	√	√	√	√	√
SD-WAN						
SD-WAN IPv6 Basic Connectivity	—	—	—	√ (11.0.2 & later)	√	√
SD-WAN for NGFW IPv6 support	—	—	—	—	√	√
Networking						
IPv6 Static Routes	√	√	√	√	√	√
PBF	√	√	√	√	√	√
PBF Next-Hop Monitor (v6 endpoint)	√	√	√	√	√	√
OSPFv3	√	√	√	√	√	√
MP-BGP	√	√	√	√	√	√
GRE Tunneling Support	√	√	√	√	√	√
ECMP	√	√	√	√	√	√
Dual Stack Support for L3 Interfaces	√	√	√	√	√	√
QoS Policy	√	√	√	√	√	√
QoS Marking	√	√	√	√	√	√
DSCP (session based)	√	√	√	√	√	√
Neighbor Discovery and Duplicate Address Detection	√	√	√	√	√	√

PAN-OS Feature	PAN-OS 9.1	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
Tunnel Content Inspection	√	√	√	√	√	√
Virtual Wires	√	√	√	√	√	√
NPTv6 (stateless prefix translation)	√	√	√	√	√	√
NAT64 (IP-IPv6 protocol translation)	√	√	√	√	√	√
LLDP (Link Layer Discovery Protocol)	√	√	√	√	√	√
Bidirectional Forwarding Detection (BFD)	√	√	√	√	√	√
IPv6 PPPoE Client	—	—	—	—	√	√
Dynamic IPv6 Addressing on the Management Interface	—	—	—	—	√	√
VPN						
GlobalProtect™	√	√	√	√	√	√
IKE/IPSec	√	√	√	√	√	√
IKEv2	√	√	√	√	√	√
IPv6 over IPv4 IPSec Tunnel	√	√	√	√	√	√
Large Scale VPN (LSVPN)	√	√	√	√	√	√
Host Dynamic Address Configuration						
DHCPv6 Relay	√	√	√	√	√	√
DHCPv6 Client with Prefix Delegation (Dataplane Interface only)	—	—	—	√	√	√
SLAAC (Router Advertisements)	√	√	√	√	√	√
SLAAC (Router Preference)	√	√	√	√	√	√

PAN-OS Feature	PAN-OS 9.1	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0	PAN-OS 11.1	PAN-OS 11.2
SLAAC (RDNSS)	√	√	√	√	√	√
Device						
High Availability (HA)—Active/Active	√	√	√	√	√	√
HA—Active/Passive	√	√	√	√	√	√
HA—IPv6 transport for HA1 & HA2	√	√	√	√	√	√
HA Path Monitoring (IPv6 Endpoint)	√	√	√	√	√	√
HA Clustering	—	√	√	√	√	√
User-ID						
Map IPv6 Address to Users	√	√	√	√	√	√
Captive Portal for IPv6	√	√	√	√	√	√
Connection to User-ID Agents over IPv6	√	√	√	√	√	√
User-ID XML API for IPv6	√	√	√	√	√	√
Terminal Server Agent IPv6	√	√	√	√	√	√

Mobile Network Infrastructure Feature Support

Review the lists of Specific Palo Alto Networks firewall models and PAN-OS® software versions that support GTP, SCTP, 5G, PFCP, and RADIUS Security, as well as 3GPP Technical Standards:

- PAN-OS Releases by Model that Support GTP, SCTP, and 5G Security
- PAN-OS Releases by Model that Support Intelligent Security Correlation (PFCP, RADIUS, and GTP)
- 3GPP TS References for GTP Security
- 3GPP TS References for 5G Security
- 3GPP TS References for 5G Multi-Edge Security
- 3GPP TS References for UE-to-IP Address Correlation with PFCP in 4G

PAN-OS Releases by Model that Support GTP, SCTP, and 5G Security

The following table lists which firewall models and PAN-OS software versions support the following security methods:

- General Packet Radio Service (GPRS) Tunnelling Protocol (GTP) security
- Stream Control Transmission Protocol (SCTP) security
- 5G security

Firewall Model	PAN-OS 9.1 (GTP and SCTP)	PAN-OS 10.1 (GTP, SCTP, and 5G)	PAN-OS 10.2 (GTP, SCTP, and 5G)	PAN-OS 11.0 (GTP, SCTP, and 5G)	PAN-OS 11.1 (GTP, SCTP, and 5G)	PAN-OS 11.2 (GTP, SCTP, and 5G)
VM-Series Firewalls	√	√	√	√	√	√
CN-Series Firewalls*	—	√	√	√	√	√
PA-7500 Firewalls (Standalone only)	—	—	—	—	√	√
PA-7000 Series Firewalls that use three of the following cards**: • PA-7000-100G-NPC card; • PA-7000-LFC-A card; and • PA-7050-SMC-B card OR PA-7080-SMC-B card	√	√	√	√	√	√
PA-5410, PA-5420, and PA-5430 Firewalls	—	—	√	√	√	√
PA-5440 Firewalls	—	—	—	√	√	√
PA-5445 Firewalls	—	—	—	—	√	√

Firewall Model	PAN-OS 9.1 (GTP and SCTP)	PAN-OS 10.1 (GTP, SCTP, and 5G)	PAN-OS 10.2 (GTP, SCTP, and 5G)	PAN-OS 11.0 (GTP, SCTP, and 5G)	PAN-OS 11.1 (GTP, SCTP, and 5G)	PAN-OS 11.2 (GTP, SCTP, and 5G)
PA-5450 Firewalls	—	√	√	√	√	√
PA-5200 Series Firewalls	√	√	√	√	√	√
PA-3430 and PA-3440 Firewalls	—	—	√	√	√	√

* CN-Series Daemonset mode supports GTP, SCTP, and 5G security in PAN-OS 10.1 and later PAN-OS versions. Additionally, CN-Series firewalls running PAN-OS 10.2 and later PAN-OS versions support GTP, SCTP, and 5G security in both K8s cloud-native network (CNF) mode and Daemonset mode.

*** To verify that your PA-7000 Series firewall is installed with the cards that support GTP and SCTP, use the **`show chassis inventory`** CLI command. However, it is possible that cards are installed but are not functional if your firewall does not account for all dependencies. Refer to the PA-7000 Series Firewall Hardware Reference for installation instructions and to review the dependencies for each card.*

PAN-OS Releases by Model that Support Intelligent Security Correlation (PFCP, RADIUS, and GTP)

The following table lists which firewall models and PAN-OS software versions support Intelligent Security Correlation:

- Packet Forwarding Control Protocol (PFCP)
- Remote Authentication Dial-In User Service (RADIUS)
- General Packet Radio Service (GPRS) Tunnelling Protocol (GTP)

Firewall Model	PAN-OS 11.0 (PFCP* and RADIUS**)	PAN-OS 11.1 (PFCP and RADIUS	PAN-OS 11.2 (PFCP, RADIUS, and GTP)
VM-Series Firewalls	√	√	√
CN-Series Firewalls	√	√	√
PA-7500 Series Firewalls	—	√ *HA cluster with PAN-OS 11.1.5 for RADIUS only	—
PA-7000 Series Firewalls that use three of the following cards***: • PA-7000-100G-NPC card; • PA-7000-LFC-A card; and • PA-7050-SMC-B card OR PA-7080-SMC-B card	√	√	√
PA-5410, PA-5420, PA-5430, PA-5440, and PA-5450 Firewalls	√	√	√
PA-5445 Firewalls	—	√	√
PA-5200 Series Firewalls	—	√	√
PA-3430 and PA-3440 Firewalls	√	√	√

* In PAN-OS 11.0, we support only 4G CUPS architecture for Intelligent Security with PFCP.

** We support Intelligent Security with RADIUS in PAN-OS 11.0.2 and all later PAN-OS versions.

*** To verify that your PA-7000 Series firewall is installed with the cards that support PFCP, RADIUS, and GTP, use the **`show chassis inventory`** CLI command. However, it is possible that cards are installed but are not functional if your firewall does not account for all dependencies. Refer to the PA-7000 Series Firewall Hardware Reference for installation instructions and to review the dependencies for each card.*

3GPP TS References for GTP Security

3GPP TS references for GTP security on firewalls that support GTP security.

	Protocol	3GPP TS	3GPP TS Release
PAN-OS 10.2 **PAN-OS 10.1**	GTPv2-C	29.274	Up to 15.2
	GTPv1-C	29.060	Up to 15.5.0
	GTP-U	29.281	Up to 15.0.0
	—	43.129	15.0.0
	—	23.401	15.12.0
PAN-OS 9.1	GTPv2-C	29.274	Up to 15.2
	GTPv1-C	29.060	Up to 15.1
	GTP-U	29.281	Up to 15.0.0
PAN-OS 8.1 (only where supported)	GTPv2-C	29.274	Up to 13.4
	GTPv1-C	29.060	Up to 13.4
	GTP-U	29.281	Up to 13.0

3GPP TS References for 5G Security

3GPP Technical Standards references for 5G network slice, 5G subscriber ID, and 5G equipment ID security on firewalls that support GTP security.

- Procedures for the 5G System (5GS)
- 5GS Session Management Services

	3GPP TS	3GPP TS Release
PAN-OS 10.2	23.502	Up to 15.5.0
PAN-OS 10.1	29.502	Up to 15.4.0

3GPP TS References for 5G Multi-Edge Security

5G Multi-Edge Security supports Packet Forwarding Control Protocol (PFCP) messages over N4 interfaces for the following technical specifications in the 3GPP TS release:

- Interface between the Control Plane and the User Plane nodes

3GPP Technical Standards reference for 5G Multi-Edge Security on firewalls that support 5G MEC Security:

	3GPP TS	3GPP TS Release
PAN-OS 10.2 **PAN-OS 10.1**	29.244	Up to 16.5.0

3GPP TS References for UE-to-IP Address Correlation with PFCP in 4G

The below table provides the 3GPP Technical Standards reference for firewalls that leverage User Equipment (UE)-to-IP Address Correlation using the Packet Forwarding Control Protocol (PFCP) for 4G network traffic.

	3GPP TS	3GPP TS Release
PAN-OS 11.0	23.214	Up to 16.2.0
	29.244	Up to 16.9.1

