Palo Alto Networks® Compatibility Matrix

techDOCS paloalto NETWORKS

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 www.paloaltonetworks.com/documentation.
- To search for a specific topic, go to our search page www.paloaltonetworks.com/documentation/document-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

March 3, 2020

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-Gen Firewalls
- Palo Alto Networks Appliances
- HA Port and Processor Support

Palo Alto Networks Next-Gen Firewalls

The following table shows the PAN-OS® releases supported for each firewall model.

Palo Alto Networks Firewall Model	PAN-OS 7.1	PAN-OS 8.1	PAN-OS 9.0	PAN-OS 9.1
Hardware Firewalls				
PA-200 Firewall (EoS*)	✓	✓	–	–
PA-220 Firewall	–	✓	✓	✓
PA-220R Firewall	–	✓	✓	✓
PA-500 Firewall (EoS*)	✓	✓	–	–
PA-800 Series Firewalls	–	✓	✓	✓
PA-2000 Series Firewalls (EoS*)	✓	–	–	–
PA-3000 Series Firewalls (EoS*)	✓	✓	✓	✓
PA-3200 Series Firewalls	–	✓	✓	✓
PA-4000 Series Firewalls (EoS*)	✓	–	–	–
PA-5000 Series Firewalls (EoS*)	✓	✓	–	–
PA-5200 Series Firewalls	–	✓	✓	✓
PA-7000 Series Firewalls	✓	✓	✓	✓
VM-Series Firewalls				
VM-50 Firewall	–	✓	✓	✓
VM-100 Firewall	✓	✓	✓	✓
VM-200 Firewall	✓	✓	✓	✓
VM-300 Firewall	✓	✓	✓	✓
VM-500 Firewall	–	✓	✓	✓
VM-700 Firewall	–	✓	✓	✓

Palo Alto Networks Firewall Model	PAN-OS 7.1	PAN-OS 8.1	PAN-OS 9.0	PAN-OS 9.1
VM-1000-HV Firewall	✓	✓	✓	✓

* For more specific information about firewalls and appliances that have reached end-of-sale (EoS) status, refer to Hardware End-of-Life Dates.

Palo Alto Networks Appliances

The following table shows OS release support for each Palo Alto Networks appliance.

Palo Alto Networks Appliance	Release 6.2	Release 7.1	Release 8.1	Release 9.0	Release 9.1
GP-100 Appliance (EoS*)	✓	–	–	–	–
Panorama Virtual Appliance	–	✓	✓	✓	✓
M-100 Appliance (EoS*)	–	✓	✓	✓ **	✓ **
M-200 Appliance	–	–	✓	✓	✓
M-500 Appliance	–	✓	✓	✓	✓
M-600 Appliance	–	–	✓	✓	✓
WF-500 Appliance	–	✓	✓	✓	✓

* For more specific information about firewalls and appliances that have reached end-of-sale (EoS) status, refer to Hardware End-of-Life Dates.

** PAN-OS 9.0 and PAN-OS 9.1 releases support M-100 appliances only after you upgrade the M-100 appliance to 32GB of memory (from the default of 16GB).

HA Port and Processor Support

The following table identifies which Palo Alto Networks® next-gen firewalls can support the HA ports and processor functionality you require in your network.

Palo Alto Networks Firewall Model	Separate Mgmt Plane Processor	Network Processor	Signature Match	First Packet Processor	HA1 Port	HA2 Port	HSCI Port
PA-200 (EoS*)	–	–	–	–	–	–	–
PA-220	–	–	–	–	–	–	–
PA-220R	–	–	–	–	–	–	–
PA-500 (EoS*)	✓	–	–	–	–	–	–
PA-820	–	–	–	–	✓	✓	–
PA-850	–	–	–	–	✓	✓	–
PA-3020	✓	–	✓	–	✓	✓	–
PA-3050	✓	✓	✓	–	✓	✓	–
PA-3060	✓	✓	✓	–	✓	✓	–
PA-3220	✓	✓	–	–	✓ (x2)	–	✓
PA-3250	✓	✓	✓	–	✓ (x2)	–	✓
PA-3260	✓	✓	✓	–	✓ (x2)	–	✓
PA-5020 (EoS*)	✓	✓	✓	–	✓	✓	–
PA-5050 (EoS*)	✓	✓	✓	–	✓	✓	–
PA-5060 (EoS*)	✓	✓	✓	–	✓	✓	–
PA-5220	✓	✓	✓	✓	✓ (x2)	–	✓
PA-5250	✓	✓	✓	✓	✓ (x2)	–	✓
PA-5260	✓	✓	✓	✓	✓ (x2)	–	✓

Palo Alto Networks Firewall Model	Separate Mgmt Plane Processor	Network Processor	Signature Match	First Packet Processor	HA1 Port	HA2 Port	HSCI Port
PA-5280	✓	✓	✓	✓	✓ (x2)	–	✓
PA-7050	✓	✓	✓	✓	✓ (x2)	–	✓ (x2)
PA-7080	✓	✓	✓	✓	✓ (x2)	–	✓ (x2)

* For more specific information about firewalls and appliances that have reached end-of-sale (EoS) status, refer to Hardware End-of-Life Dates.

VM-Series Firewalls

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

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

VM-Series Firewall Hypervisor Support

The following table shows hypervisor version support on the VM-Series firewall.

*The PAN-OS Version Support column displays the range of versions and the minimum version in parentheses. For example, the PAN-OS Version column could say **PAN-OS 8.1.x (8.1.3)**; this means the integration supports PAN-OS 8.1, beginning with PAN-OS 8.1.3.*

Deployment	PAN-OS Version Support (Minimum)	Hypervisor Version Support (Minimum)	I/O Enhancement Support	Base Image Required from the Palo Alto Networks Support Portal
Private Cloud Deployments				
VM-Series for VMware vSphere Hypervisor (ESXi) (without VMware NSX)	PAN-OS 7.1.x (7.1.0) PAN-OS 8.1.x (8.1.0) PAN-OS 9.0.x (9.0.0)	5.1 (not supported on PAN-OS 9.0), 5.5 and 6.0	—	**PA-VM-ESX-7.1.0.ova** **PA-VM-ESX-8.1.0.ova** **PA-VM-ESX-9.0.0.ova**
	PAN-OS 7.1.x (7.1.0) PAN-OS 8.1.x (8.1.0) PAN-OS 9.0.x (9.0.0)	6.5	PAN-OS 8.0 and later: • SR-IOV • DPDK	**PA-VM-ESX-7.1.0-u1.ova** **PA-VM-ESX-8.1.0.ova** **PA-VM-ESX-9.0.0.ova**
	PAN-OS 8.1.x (8.1.0) PAN-OS 9.0.x (9.0.0) PAN-OS 9.1.x (9.1.0)	6.7	• SR-IOV • DPDK	**PA-VM-ESX-8.1.0.ova** **PA-VM-ESX-9.0.0.ova** **PA-VM-ESX-9.1.0.ova**
VM-Series for VMware NSX-V vSphere with VMware NSX and Panorama The combinations listed in this document have been approved by Palo Alto Networks. For versions of PAN-	PAN-OS 7.1.x (7.1.0)	vSphere: 5.5 NSX Manager: 6.0, 6.1, and 6.2	—	**PA-VM-NSX-7.1.0.zip**
		vSphere: 6.0 and 6.5a NSX Manager: 6.1, 6.2, 6.3, and 6.4	—	

Deployment	PAN-OS Version Support (Minimum)	Hypervisor Version Support (Minimum)	I/O Enhancement Support	Base Image Required from the Palo Alto Networks Support Portal
OS certified by VMware, see the VMware Compatibility Guide. Panorama 8.0 and higher requires the VMware NSX plugin. For more information, see VMware NSX. Available on all VM-Series models except the VM-50 and the VM-700.	PAN-OS 8.1.x (8.1.0) with NSX Plugin 2.0.2 or later	vSphere: 6.0 and 6.5 NSX Manager: 6.3.x and 6.4.0	LRO	**PA-VM-NSX-8.1.0.zip** with **vmware_nsx-2.0.2**
		vSphere: 6.0, 6.5, and 6.7 NSX Manager: 6.4.1 and later		
	PAN-OS 9.0.x (9.0.0)with NSX Plugin 2.0.3 or later	vSphere: 6.0 and 6.5 NSX Manager: 6.3.x and 6.4.0		**PA-VM-NSX-9.0.0.zip** with **vmware_nsx-2.0.3**
		vSphere: 6.0, 6.5, and 6.7 NSX Manager: 6.4.1 and later		
VM-Series for VMware NSX-T	PAN-OS 9.0.x (9.0.4)	NSX-T Manager: 2.4.0 and later	—	**PA-VM-NST-9.0.4.zip** with **vmware_nsx-3.0.0**
	PAN-OS 9.1.x (9.1.0)	NSX-T Manager: 2.5.0 and later	—	**PA-VM-NST-9.1.0.zip** with **vmware_nsx-3.1.0**
VM-Series for Citrix SDX	PAN-OS 7.1.x (7.1.0)	SDX 10.1+ XenServer 6.0.2 and later	—	**PAN-OS for VM-Series SDX Base Images** For example, the download-able image name is: **PA-VM-SDX-7.1.2.zip** **PA-VM-SDX-8.0.0.zip**
VM-Series for KVM	PAN-OS 7.1.x (7.1.0)	• Ubuntu: 12.04 LTS, 14.04 LTS, and 16.04 LTS	SR-IOV	**PA-VM-KVM-7.1.0.qcow2**

Deployment	PAN-OS Version Support (Minimum)	Hypervisor Version Support (Minimum)	I/O Enhancement Support	Base Image Required from the Palo Alto Networks Support Portal
		• CentOS/Red Hat Enterprise Linux: 6.5, 7.0, 7.1, and 7.2		

	PAN-OS 8.1.x (8.1.0)
	VM-Series on KVM - Requirements and Prerequisites
		• Ubuntu:
		  • 14.04 LTS (QEMU-KVM 2.0.0 and libvirt 1.2.2)
		  • 16.04 LTS (QEMU-KVM 2.5.0 and libvirt 1.3.1)
		• CentOS/Red Hat Enterprise Linux 7.2 (QEMU-KVM 1.5.3 and libvirt 2.0.0)
			• DPDK
			• SR-IOV
				PA-VM-KVM-8.1.0.qcow2

	PAN-OS 8.1.x (8.1.3) PAN-OS 9.0.x (9.0.0) PAN-OS 9.1.x (9.1.0) VM-Series on KVM - Requirements and Prerequisites	CentOS 7.5 (QEMU-KVM 1.5.3 and libvirt 3.9.0)	Packet MMAP mode support only; so you must disable DPDK with op-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)	**PA-VM-KVM-8.1.3.qcow2** **PA-VM-KVM-9.0.0.qcow2** **PA-VM-KVM-9.1.0.qcow2**
	PAN-OS 9.0.x.xfr (9.0.3.xfr)	CentOS 7.6 (QEMU-KVM 2.12.0 and libvirt 4.5.0)	DPDK	**PA-VM-KVM-9.0.3.xfr.qcow2**
	PAN-OS 8.1.x (8.1.3) PAN-OS 9.0.x (9.0.1) PAN-OS 9.0.x.xfr (9.0.3.xfr)	RHEL 7.6 (QEMU-KVM 2.12.0 and libvirt 4.5.0)	• 8.1.3 - Packet MMAP/SR-IOV only • 8.1.10 - SR-IOV-DPDK only	**PA-VM-KVM-8.1.3.qcow2** **PA-VM-KVM-8.1.10.qcow2** **PA-VM-KVM-9.0.1.qcow2**

Deployment	PAN-OS Version Support (Minimum)	Hypervisor Version Support (Minimum)	I/O Enhancement Support	Base Image Required from the Palo Alto Networks Support Portal
	PAN-OS 9.1.x (9.1.0)		• 9.0.1 - Packet MMAP and SR-IOV only • 9.0.4 - SR-IOV-DPDK only • 9.0.3.xfr - Virtio/SR-IOVwith DPDK	**PA-VM-KVM-9.0.3.xfr.qcow2** **PA-VM-KVM-9.0.4.qcow2** **PA-VM-KVM-9.1.0.qcow2**

	PAN-OS 8.1.x (8.1.3)
	PAN-OS 9.0.x (9.0.1)
	PAN-OS 9.1.x (9.1.0)
		• CentOS 7.7 (QEMU-KVM 1.5.3 and libvirt 4.5.0)
		• CentOS 8.0 (QEMU-KVM 2.12.0 and libvirt 4.5.0)
			• DPDK with Virtio: 9.1 and later
			• DPDK with SR-IOV:
			  • 8.1.11 and later
			  • 9.0.6 and later
			  • 9.1 and later
				PA-VM-KVM-8.1.11.qcow2
				PA-VM-KVM-9.0.6.qcow2
				PA-VM-KVM-9.1.0.qcow2

VM-Series for Nutanix	PAN-OS 8.1.x (8.1.0) Layer 2, Layer 3, and virtual wire deployments	AHV Nutanix AOS Version 5.1.5 Nutanix AHV Release 20160925.121	—	**PA-VM-8.1.0.qcow2**
	PAN-OS 8.1.x (8.1.2) Layer 3 deployments only	AHV Nutanix AOS Version 5.5.4 and later Nutanix AHV Release 20170830.156S	Packet MMAP support for Layer 3 deployment. You must disable DPDK with **`op-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`**.	**PA-VM-8.1.0.qcow2** and upgrade to PAN-OS 8.1.2.

Deployment	PAN-OS Version Support (Minimum)	Hypervisor Version Support (Minimum)	I/O Enhancement Support	Base Image Required from the Palo Alto Networks Support Portal
	PAN-OS 8.1.x (8.1.3) Layer 3 deployments, and Virtual wire deployments with Service Chaining.	AHV • Nutanix AOS Version 5.9 Nutanix AHV Release 20170830.171 • Nutanix AOS Version 5.10 Nutanix AHV Release 20170830.185	Packet MMAP support only. You must disable DPDK with **`op-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`**.	**PA-VM-8.1.3.qcow2**
	PAN-OS 9.0.x (9.0.0) PAN-OS 9.1.x (9.1.0) Layer 3 deployments, and virtual wire deployments with Service Chaining.	AHV Nutanix AOS Version 5.10 Nutanix AHV Release 20170830.185	Packet MMAP support only. You must disable DPDK with **`op-cmd-dpdk-pkt-io=off`** in the init-cfg.txt file used for bootstrapping or use the **`set system setting dpdk-pkt-io off`** CLI command.	**PA-VM-9.0.0.qcow2** **PA-VM-9.1.0.qcow2**
VM-Series for Hyper-V	PAN-OS 7.1.x (7.1.0) PAN-OS 8.1.x (8.1.0) PAN-OS 9.0.x (9.0.0)	• Windows Server 2012 R2 with Hyper-V role or Hyper-V 2012 R2 • Windows Server 2016 with Hyper-V role or Hyper-V 2016	—	**PAN-OS for VM-Series Hyper-V Base Images** For example, the download-able image name is: **PA-VM-HPV-7.1.0.vhdx** **PA-VM-HPV-8.1.0.vhdx** **PA-VM-HPV-9.0.0.vhdx**
VM-Series for OpenStack	PAN-OS 7.1.x (7.1.12)	KVM: Ubuntu 14.04	—	**PAN-OS for VM-Series KVM Base Images**

Deployment	PAN-OS Version Support (Minimum)	Hypervisor Version Support (Minimum)	I/O Enhancement Support	Base Image Required from the Palo Alto Networks Support Portal
	PAN-OS 8.1.x (8.1.0)	OpenStack: Mirantis 8.0 with Contrail 3.2		PA-VM-KVM-7.1.12.qcow2 PA-VM-KVM-8.1.0.qcow2
	PAN-OS 8.1.x (8.1.0) PAN-OS 9.0.x (9.0.0)	Redhat OpenStack Newton 10	Virtio only	**PAN-OS for VM-Series KVM Base Images** PA-VM-KVM-8.1.0.qcow2 PA-VM-KVM-9.0.0.qcow2
	PAN-OS 9.0.x (9.0.3) PAN-OS 9.0.x.xfr (9.0.3.xfr)	Redhat OpenStack Queens 13	• 9.0.3 - Packet MMAP and SR-IOV only • 9.0.3.xfr - Virtio/SR-IOV with DPDK	**PAN-OS for VM-Series KVM Base Images** PA-VM-KVM-9.0.3.qcow2 PA-VM-KVM-9.0.3.xfr.qcow2
Hardware and VM-Series Firewalls in Cisco ACI	Managed Mode only: PAN-OS 7.1.x (7.1.0)	ACI: 2.3 and 3.0	N/A	Device Package 1.3
	Unmanaged Mode only: PAN-OS 8.1.x (8.1.0) PAN-OS 9.0.x (9.0.0)	ACI: 2.3(1e), 3.1, and 3.2	N/A	**Panorama Plugin for Cisco ACI** cisco-1.0.0
	Unmanaged Mode only: PAN-OS 8.1.x (8.1.0) PAN-OS 9.0.x (9.0.0)	ACI: 2.3(1e), 3.1, 3.2, and 4.0 and later	N/A	**Panorama Plugin for Cisco ACI** cisco-1.0.1
Public Cloud Deployments				
VM-Series on AWS	PAN-OS 7.1.x (7.1.0)	N/A	PAN-OS 8.0 and later: DPDK	N/A

Deployment	PAN-OS Version Support (Minimum)	Hypervisor Version Support (Minimum)	I/O Enhancement Support	Base Image Required from the Palo Alto Networks Support Portal
List of supported AWS and AWS Gov Cloud Regions.	PAN-OS 8.1.x (8.1.0) PAN-OS 9.0.x (9.0.0) PAN-OS 9.1.x (9.1.0)		is supported in addition to SR-IOV, but is disabled by default. PAN -OS 9.0.x where x is less than or equal to 3, DPDK is supported on all except C5 and M5 instances; only SR-IOV is supported. PAN -OS 9.0.3.xfr supports both DPDK and SR-IOV for all instance types, but DPDK is disabled by default.	
VM-Series on vCloud Air	PAN-OS 7.1.x (7.1.0) PAN-OS 8.1.x (8.1.0)	N/A	—	**PAN-OS for VM-Series Base Images** For example, the download-able image name is: PA-VM-ESX-7.1.0.ova PA-VM-ESX-8.0.0.ova PA-VM-ESX-8.1.0.ova
VM-Series on Azure List of supported Azure Regions.	PAN-OS 7.1.x (7.1.0) PAN-OS 8.1.x (8.1.0) PAN-OS 9.0.x (9.0.0) PAN-OS 9.1.x (9.1.0)	N/A	DPDK is not supported	N/A

Deployment	PAN-OS Version Support (Minimum)	Hypervisor Version Support (Minimum)	I/O Enhancement Support	Base Image Required from the Palo Alto Networks Support Portal
VM-Series on Google Cloud	PAN-OS 8.1.x (8.1.0) PAN-OS 9.0.x (9.0.0) PAN-OS 9.1.x (9.1.0)	N/A	DPDK is supported and enabled by default	N/A
VM-Series on Oracle Cloud Infrastructure	PAN-OS 8.1.x (8.1.0) PAN-OS 9.0.x (9.0.0) PAN-OS 9.1.x (9.1.0)	N/A	Packet MMAP support only. DPDK is enabled by default and must be disabled.	**PAN-OS for VM-Series KVM Base Images** PA-VM-KVM-8.1.0.qcow2 PA-VM-KVM-9.0.0.qcow2 PA-VM-KVM-9.1.0.qcow2
VM-Series on Alibaba Cloud	PAN-OS 8.1.x (8.1.0) PAN-OS 9.0.x (9.0.0) PAN-OS 9.1.x (9.1.0)	N/A	DPDK and Packet MMAP are supported. DPDK is enabled by default.	**PAN-OS for VM-Series KVM Base Images** PA-VM-KVM-8.1.3.qcow2 PA-VM-KVM-9.0.0.qcow2 PA-VM-KVM-9.1.0.qcow2

Partner Interoperability for VM-Series Firewalls

The following section shows the partner products with which the VM-Series firewall interoperates. Refer to the following tables for details about hardware platforms and software versions on which you can deploy the VM-Series firewall.

*The Partner Software Version and PAN-OS Version columns display the range of versions and the minimum version in parentheses. For example, the PAN-OS Version column could say **PAN-OS 8.1.x (8.1.3)**; this means the integration supports PAN-OS 8.1, beginning with PAN-OS 8.1.3.*

Ciena

The following table shows the Ciena products with which the VM-Series firewall interoperates.

Hardware	Hyperv	SAOS Supported Software Version (Minimum)	SAOS Tested Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documer
3906mvi and 3926mvi	KVM	18.x.x (18.06.00)	18.06.x (18.06.00)	8.1.x (8.1.3) 9.0.x (9.0.0) 9.0.x.xfr (9.0.3.xfr) 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 the VM-Series firewall interoperates.

Hardware	Hyperv	CSP Supported Software Version (Minimum)	CSP Tested Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documer
CSP5400 Series and CSP2100 Series	KVM	2.x.x (2.4.0)	2.4.x (2.4.0)	8.1.x (8.1.3) 9.0.x (9.0.1)	Layer 2, Layer3, Virtual wire deployments on all VM-Series models except VM-50 VM-Series Firewalls in an HA configuration SR-IOV, and Packet MMAP mode 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`**	VM-Series on Cisco CSP
				9.0.x.xfr (9.0.3.xfr) 9.1.x (9.1.0)	Layer 2, Layer3, Virtual wire deployments on all VM-Series models except VM-50 VM-Series Firewalls in an HA configuration SR-IOV, and Packet MMAP mode	

Cisco Enterprise Computer System (ENCS)

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

Hardware	Hyperv	NFVIS Supported Software Version (Minimum)	Tested NFVIS Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documer
Cisco 5400 Series	KVM	3.x.x (3.8)	3.8.x (3.8.1)	8.1.x (8.1.3)	• Layer 2, Layer3, Virtual wire deployments • Firewalls in an HA configuration for NFVIS 3.10.x and 3.12.x with PAN-OS 9.0.x • 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`**	VM-Series on Cisco ENCS
			3.10.x (3.10.1)	8.1.x (8.1.3) 9.0.x (9.0.2)		
			3.12.x (3.12.1)	8.1.x (8.1.11) 9.0.x (9.0.5)		
			3.10.x (3.10.1) 3.12.x (3.12.1)	9.0.x.xfr (9.0.3.xfr) 9.1.x (9.1.0)	• Layer 2, Layer3, Virtual wire deployments • Firewalls in HA • Virtio with DPDK mode enabled by default	VM-Series on Cisco ENCS

Citrix SD-WAN

The following table shows the Citrix SD-WAN products with which the VM-Series firewall interoperates.

Hardware	Hypervis	Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Document
Citrix SD-WAN 1100 Appliance	KVM	11.0.x (11.0.1)	8.1.x (8.1.3) 9.0.x (9.0.1) 9.1.x (9.1.0)	Virtual wire deployments VirtIO with packet MMAP mode support only; so you must disable	• Citrix SD-WAN

Hardware	Hypervis	Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documenta
				DPDK with **`op-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`**	Deployment Guide • Citrix SD-WAN Solution Brief
			9.0.x.xfr (9.0.3.xfr) 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 the VM-Series firewall interoperates.

Hardware	Hypervis	Junos Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documenta
NFX 250	KVM	15.1X53-D470.x (15.1X53-D470.5)	8.0.x (8.0.5) 8.1.x (8.1.0)	Layer 2, Layer3, Virtual wire deployments VirtIO only	Juniper NFX documentation
			9.0.x.xfr (9.0.3.xfr) 9.1.x (9.1.0)	Layer 2, Layer 3, Virtual Wire DPDK mode	

NSX SD-WAN by VeloCloud

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

Hardware	Hyperv	VCE Supported Software Version (Minimum)	Tested VCE Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Docume
Edge 520v Edge 840	KVM	3.x.x (3.2.0)	3.2.x (3.2.0)	8.0.x (8.0.5)	Virtual wire deployments VirtIO only	NSX SD-WAN by VeloCloud documentation
			3.3.x (3.3.1)	8.1.x (8.1.0) 9.0.x (9.0.0)	Virtual wire deployments	

Hardware	Hyperv	VCE Supported Software Version (Minimum)	Tested VCE Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documer
					VirtIO with packet MMAP mode only	
				9.0.x.xfr (9.0.3.xfr) 9.1.x (9.1.0)	Virtual wire deployments DPDK	

Nuage Networks

The following table shows the Nuage Networks products with which the VM-Series firewall interoperates.

Hardware	Hypervis	VSP Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Document
Nuage NSG-X series	—	5.3.x (5.3.3U3)	8.1.x (8.1.3) 9.0.x (9.0.0)	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

Nutanix

The following table shows the Nutanix products with which the VM-Series firewall interoperates.

Partner Hardware	Hypervis	Nutanix Software Version	PAN-OS Version	Deployment Modes Supported	Document
—	AHV	• VM-Series on Nutanix • Nutanix Documentation			

Versa Networks

The following table shows the Versa Networks products with which the VM-Series firewall interoperates.

Hardware	Hypervis	Versa FlexVNF Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Document
Versa VF 100 Series (Versa-120)	KVM	20.1.x (20.1.1)	8.1.x (8.1.3)	Virtual wire deployments with DPDK	Versa Networks documentation

Vyatta

The following table shows the Vyatta products with which the VM-Series firewall interoperates.

Platform	Hypervis	Vyatta Software Version	PAN-OS Version (Minimum)	Deployment Modes Supported	Document
AT&T vRouter 5600	KVM	19.x (1903f)	9.0.x.xfr (9.0.3.xfr) 9.1.x (9.1.0)	Virtual wire, L2, L3 deployments with DPDK VM-50, VM-100, and VM-300	—

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 from Panorama.

To manage the VM-Series plugin configuration of 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 shows the features introduced in each version of the VM-Series Plugin. For additional information about each version, refer to the release notes.

VM-Series Plugin Version	Minimum PAN-OS Version	New Features or Changes
1.0.0 or later	9.0.0	First VM-Series plugin. The VM-Series plugin enables publishing metrics for supported public clouds: AWS, Azure, and Google Cloud Platform
1.0.2 1.0.3 1.0.4	9.0.1	Supported on all VM-Series models.  *If you want to enable management interface swap on GCP or AWS platforms and are running PAN-OS 9.0.2, you must install VM-Series plugin 1.0.3.*
1.0.5	9.0.3.xfr 9.0.4	Supported on all VM-Series models. The PAN-OS accelerated feature releases (images with .xfr in the filename) are for VM-Series firewalls only, and are delivered to enable support for new features and bug fixes for VM-Series firewalls. PAN-OS 9.0.3.xfr and PAN-OS 9.0.4 require plugin 1.0.5 or later.
1.0.6	9.0.4	Required for the VM-Series firewall on NSX-T (North-South).
1.0.7	9.0.4	Includes bug fixes along with support for high availability (HA) on Azure Government for the VM-Series on Azure. Supported on all VM-Series models; Required if you want to enable (HA) on Azure Government for the VM-Series on Azure.
1.0.8	9.1.0	Minimum version required for the VM-Series firewalls on 9.1.0.
1.0.9	9.0.4	Introduces support for marketplace deployment and high availability for the VM-Series firewall

VM-Series Plugin Version	Minimum PAN-OS Version	New Features or Changes
		on Oracle Cloud Infrastructure; PAN-OS 9.1.1 is required to use these OCI features.

AWS and AWS Gov Cloud Regions

The AWS regions 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) PAN-OS 9.0.1 and later	ap-east-1
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Osaka-Local) Starting with PAN-OS 9.0.3.xfr 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 (Beijing) PAN-OS 9.0.1 and later	cn-north-1
Asia Pacific (Ningxia) PAN-OS 9.0.1 and later	cn-northwest-1
Canada Central	ca-canada-1
EU (Frankfurt)	eu-central-1
EU (Ireland)	eu-west-1
EU (London)	eu-west-2

AWS Regions	Region ID
EU (Paris) PAN-OS 9.0.0 and later	eu-west-3
EU (Stockholm) PAN-OS 9.0.0 and later	eu-north-1
South America (Sao Paulo)	sa-east-1
Middle East (Bahrain) PAN-OS 9.0.1 and later	me-south-1
AWS Gov Cloud (US)  *PAN-OS 9.0.1 and later for us-gov-east*	us-gov-west us-gov-east

Azure Regions

The Azure locations in which you can deploy the VM-Series firewall from the Azure public and the Azure Government Marketplace.

Azure Public Cloud Locations (For PAN-OS 7.1, 8.1, 9.0, and 9.1)		
Americas	Asia Pacific	Europe
• East US	• Australia East	• West Europe
• East US 2	• Australia Southeast	• North Europe
• West US	• East Asia	• UK West
• West US 2	• Japan East	• UK South
• Central US	• Japan West	
• West Central US	• Korea Central	
• North Central US	• Korea South	
• South Central US	• Southeast Asia	
• Canada Central	• China North	
• Canada East	• China East	
• Brazil South		
Azure Government (US) Locations (For PAN-OS 7.1.1, 8.1, 9.0, and 9.1)		
• Iowa		
• Virginia		
• Texas (PAN-OS 8.1)		
Azure DoD Locations (For PAN-OS 8.1, 9.0, and 9.1)		
• US DoD East • US DoD Central		
Azure Germany (For PAN-OS 8.1, 9.0, and 9.1)		
Germany Northeast		
Germany Central		

Google Cloud Regions

You can deploy a VM-Series firewall with PAN-OS 8.1, PAN-OS 9.0, or PAN-OS 9.1 in all Google Cloud Platform regions.

Alibaba Cloud Regions

You can deploy the VM-Series firewall with a PAN-OS 8.1.3 or later PAN-OS 8.1 release or a PAN-OS 9.0 or later release in all Alibaba Cloud regions.

VM-Series Firewall Amazon Machine Images (AMI) List

For your convenience, the AMI IDs for the PAN-OS versions and licensing options, in the supported regions, are collated for use with Palo Alto Networks CFTs to auto scale the VM-Series firewall on AWS. See Use the AWS CLI to get the AMI IDs to find the AMI IDs for automating the deployment of the VM-Series firewall for other use cases.

The two most recent versions—2.0 and 2.1—of the CFT for auto scaling the VM-Series firewall on AWS are supported. VM-Series Auto Scaling Template for AWS v2.0 requires the AMI for PAN-OS 8.0.6 or later, and VM-Series Auto Scaling Template for AWS v2.1 requires PAN-OS 8.1 or later.

Images for PAN-OS 9.0

List of PAN-OS 9.0 AMI IDs for the different licensing options: BYOL, and PAYG bundle 1 and 2, for use with the VM-Series Auto Scaling template v2.1 and v2.0. See Use the AWS CLI to get the AMI IDs to find the AMI IDs for automating the deployment of the VM-Series firewall for other use cases.

AMI IDs for PAN-OS 9.0.1

Use the following AMIs with the VM-Series Auto Scaling template v2.1 and v2.0.

AWS Regions		PAN-OS 9.0.0 AMI IDs that correspond to the licensing options		
		BYOL	PAYG Bundle 2	PAYG Bundle 1
us-east-1	US East (N. Virginia)	ami-0012adac0a4148630	ami-050725600cf371a1c	ami-0725ec6c13a8d9bd1
us-east-2	US East (Ohio)	ami-04cb91d704368a8b9	ami-0340ae9cf0a892bab	ami-0ab88c7bfee0fd533
us-west-1	US West (N. California)	ami-0ca25d8ac63d17ad6	ami-02aa6330cd84b4020	ami-0dd6697dad89db412
us-west2	US West (Oregon)	ami-094f3a5479b5096b8	ami-019b369b2201d17e1	ami-03e60b21ae6660711
sa-east-1	South America (SaoPaulo)	ami-0f4804ea341d4a897	ami-05a40658314a5dc06	ami-020546007f963c752
eu-west-1	EU (Ireland)	ami-05a20ed554111d2f6	ami-08e82ba0784b4e5ad	ami-08d3fcfe3bd131583
eu-west-2	EU (London)	ami-04e0b601413d8a139	ami-0cea9a41443754f56	ami-0d570b21bbe1dd096

AWS Regions		PAN-OS 9.0.0 AMI IDs that correspond to the licensing options		
eu-central-1	EU (Frankfurt)	ami-00f2ea8ebc2983ai	ami-087597cf0637e3ba9	ami-0852f5e901fab29fa
ca-central-1	Canada (Central)	ami-0c3940cfe30fd7853	ami-0d179c6cdc2589b25	ami-0ca7f26ddbf814033
ap-northeast-1	Asia Pacific (Tokyo)	ami-0a1fa1c292897d88e	ami-0ca2e94970201db8d	ami-0dfd9708425ae9fae
ap-northeast-2	Asia Pacific (Seoul)	ami-0e8e239b8b61bdc29	ami-0a72f886dd8026ca5	ami-0b7322f0dbbf53ab7
ap-southeast-1	Asia Pacific (Singapore)	ami-0b6d59afd928a6807	ami-050d7488f46b8e776	ami-06b34656abc31ce12
ap-southeast-2	Asia Pacific (Sydney)	ami-0a31b0cc246e903e2	ami-0c3ced1b6948e91ad	ami-05e41c650f585f3d3
ap-south-1	Asia Pacific (Mumbai)	ami-09b1600161c83f304	ami-01923acdc459e45f8	ami-0565f10a22e9f15c1

Images for PAN-OS 8.1

List of PAN-OS 8.1 AMI IDs for the different licensing options: BYOL, and PAYG bundle 1 and 2, for use with the VM-Series Auto Scaling template. See Use the AWS CLI to get the AMI IDs to find the AMI IDs for automating the deployment of the VM-Series firewall for other use cases.

- AMI IDs for PAN-OS 8.1.0

AMI IDs for PAN-OS 8.1.0

Use the following AMIs with the VM-Series Auto Scaling template v2.1 and v2.0 .

AWS Regions		PAN-OS 8.1.0 AMI IDs that correspond to the licensing options		
		BYOL	PAYG Bundle 2	PAYG Bundle 1
us-east-1	US East (N. Virginia)	ami-a2fa3bdf	ami-bffd3cc2	ami-ce01c0b3
us-east-2	US East (Ohio)	ami-11e1d774	ami-9ef3c5fb	ami-10f3c575
us-west-1	US West (N. California)	ami-a95b4fc9	ami-854551e5	ami-235b4f43
us-west2	US West (Oregon)	ami-d424b5ac	ami-9a29b8e2	ami-8a22b3f2
sa-east-1	South America (SaoPaulo)	ami-9c0154f0	ami-d80653b4	ami-9e0154f2
eu-west-1	EU (Ireland)	ami-62b5fb1b	ami-1fb1ff66	ami-edb0fe94

AWS Regions		PAN-OS 8.1.0 AMI IDs that correspond to the licensing options		
eu-west-2	EU (London)	ami-876a8de0	ami-c4688fa3	ami-f46a8d93
eu-central-1	EU (Frankfurt)	ami-55bfd73a	ami-1ebdd571	ami-1bbdd574
ca-central-1	Canada (Central)	ami-64038400	ami-57048333	ami-dd0582b9
ap-northeast-1	Asia Pacific (Tokyo)	ami-57662d31	ami-75652e13	ami-39662d5f
ap-northeast-2	Asia Pacific (Seoul)	ami-49bd1127	ami-a8bf13c6	ami-4eb81420
ap-southeast-1	Asia Pacific (Singapore)	ami-27baeb5b	ami-36bdec4a	ami-55bced29
ap-southeast-2	Asia Pacific (Sydney)	ami-00d61562	ami-add013cf	ami-aed112cc
ap-south-1	Asia Pacific (Mumbai)	ami-e780d988	ami-ee80d981	ami-d385dcbc

Images for PAN-OS 8.0

List of AMI IDs for the different licensing options: bring your own license (BYOL) and pay-as-you-go (PAYG) bundles 1 and 2, for use with the VM-Series Auto Scaling template. See Use the AWS CLI to get the AMI IDs to find the AMI IDs for automating the deployment of the VM-Series firewall for other use cases.

- AMI IDs for PAN-OS 8.0.6
- AMI IDs for PAN-OS 8.0.8
- AMI IDs for PAN-OS 8.0.9
- PAN-OS Images for AWS GovCloud

AMI IDs for PAN-OS 8.0.6

Use the following AMIs with the VM-Series Auto Scaling template v2.0 .

AWS Regions		PAN-OS 8.0.6 AMI IDs that correspond to the licensing options		
		BYOL	PAYG Bundle 2	PAYG Bundle 1
us-east-1	US East (N. Virginia)	ami-493c7233	ami-69a2f513	ami-b6a4f3cc
us-east-2	US East (Ohio)	ami-924269f7	ami-66183303	ami-10193275
us-west-1	US West (N. California)	ami-5d59583d	ami-a29a9bc2	ami-5a9a9b3a

AWS Regions		PAN-OS 8.0.6 AMI IDs that correspond to the licensing options		
us-west2	US West (Oregon)	ami-7c812804	ami-725ef50a	ami-d258f3aa
sa-east-1	South America (SaoPaulo)	ami-cdd595a1	ami-fb86c597	ami-0787c46b
eu-west-1	EU (Ireland)	ami-d6c44faf	ami-fc4fdb85	ami-844bdffd
eu-west-2	EU (London)	ami-166c7472	ami-e9dcc48d	ami-45d8c021
eu-central-1	EU (Frankfurt)	ami-5b2cba34	ami-a1ad3dce	ami-9151c1fe
ca-central-1	Canada (Central)	ami-3913a95d	ami-50cb4e34	ami-d9cc49bd
ap-northeast-1	Asia Pacific (Tokyo)	ami-4a6eff2c	ami-b5af32d3	ami-11a43977
ap-northeast-2	Asia Pacific (Seoul)	ami-9b2889f5	ami-32f3535c	ami-4bf35325
ap-southeast-1	Asia Pacific (Singapore)	ami-e2cba19e	ami-5ef78022	ami-aff582d3
ap-southeast-2	Asia Pacific (Sydney)	ami-1af80b78	ami-059f6d67	ami-0d9f6d6f
ap-south-1	Asia Pacific (Mumbai)	ami-dd4316b2	ami-f9005496	ami-e106528e

AMI IDs for PAN-OS 8.0.8

Use the following AMIs with the VM-Series Auto Scaling template v2.0 .

AWS Regions		PAN-OS 8.0.8 AMI IDs that correspond to the licensing options		
		BYOL	PAYG Bundle 2	PAYG Bundle 1
us-east-1	US East (N. Virginia)	ami-66c63b1b	ami-ce3cc1b3	ami-b038c5cd
us-east-2	US East (Ohio)	ami-cb8eb9ae	ami-bb8bbcde	ami-0480b761
us-west-1	US West (N. California)	ami-d4f3f9b4	ami-78f1fb18	ami-e0f1fb80
us-west2	US West (Oregon)	ami-4f118437	ami-b21287ca	ami-6d1e8b15
sa-east-1	South America (SaoPaulo)	ami-1ff1ba73	ami-9df0bbf1	ami-1ff7bc73

AWS Regions		PAN-OS 8.0.8 AMI IDs that correspond to the licensing options		
eu-west-1	EU (Ireland)	ami-a0b5f5d9	ami-cdbfffb4	ami-cbc080b2
eu-west-2	EU (London)	ami-3d93745a	ami-6891760f	ami-3a94735d
eu-central-1	EU (Frankfurt)	ami-aff19ec0	ami-45c8a72a	ami-96caa5f9
ca-central-1	Canada (Central)	ami-d4be39b0	ami-56bd3a32	ami-0abb3c6e
ap-northeast-1	Asia Pacific (Tokyo)	ami-aa662bcc	ami-7a7c311c	ami-e77f3281
ap-northeast-2	Asia Pacific (Seoul)	ami-8109a4ef	ami-8a0fa2e4	ami-610ea30f
ap-southeast-1	Asia Pacific (Singapore)	ami-f61a4e8a	ami-d50054a9	ami-15075369
ap-southeast-2	Asia Pacific (Sydney)	ami-9131f0f3	ami-ae2eefcc	ami-3230f150
ap-south-1	Asia Pacific (Mumbai)	ami-2a471945	ami-8c421ce3	ami-14401e7b

AMI IDs for PAN-OS 8.0.9

Use the following AMIs with the VM-Series Auto Scaling template v2.0 .

AWS Regions		PAN-OS 8.0.9 AMI IDs that correspond to the licensing options		
		BYOL	PAYG Bundle 2	PAYG Bundle 1
us-east-1	US East (N. Virginia)	ami-49900636	ami-b69305c9	ami-ea950395
us-east-2	US East (Ohio)	ami-8e98a5eb	ami-8998a5ec	ami-3f9aa75a
us-west-1	US West (N. California)	ami-04273e64	ami-26243d46	ami-cb253cab
us-west2	US West (Oregon)	ami-659eec1d	ami-089be970	ami-3398ea4b
sa-east-1	South America (SaoPaulo)	ami-1eb2ee72	ami-70bfe31c	ami-49b4e825
eu-west-1	EU (Ireland)	ami-ef80b096	ami-c69dadbf	ami-e19bab98
eu-west-2	EU (London)	ami-3bcc215c	ami-becf22d9	ami-39cd205e

AWS Regions		PAN-OS 8.0.9 AMI IDs that correspond to the licensing options		
eu-central-1	EU (Frankfurt)	ami-f3c2ed18	ami-f0c2ed1b	ami-80c3ec6b
ca-central-1	Canada (Central)	ami-9751d1f3	ami-3f51d15b	ami-bd4eced9
ap-northeast-1	Asia Pacific (Tokyo)	ami-621bec1d	ami-691ceb16	ami-491ceb36
ap-northeast-2	Asia Pacific (Seoul)	ami-38b61e56	ami-e7b41c89	ami-3fb61e51
ap-southeast-1	Asia Pacific (Singapore)	ami-39586945	ami-c05968bc	ami-f85a6b84
ap-southeast-2	Asia Pacific (Sydney)	ami-788a5b1a	ami-958b5af7	ami-ce8a5bac
ap-south-1	Asia Pacific (Mumbai)	ami-d06e43bf	ami-ca6b46a5	ami-5169443e

Images for PAN-OS 7.1.11

List of AMI IDs for PAN-OS 7.1.11 with the different licensing options: BYOL, and PAYG bundle 1 and 2. See Use the AWS CLI to get the AMI IDs to find the AMI IDs for different versions and across all supported regions.

AWS Regions		PAN-OS 7.1.11 AMI IDs that correspond to the licensing options		
		BYOL	PAYG Bundle 2	PAYG Bundle 1
us-east-1	US East (N. Virginia)	ami-83f1a3f8	ami-6ff0a214	ami-19f3a162
us-east-2	US East (Ohio)	ami-d15e7eb4	ami-a72101c2	ami-ba5e7edf
us-west-1	US West (N. California)	ami-0189a061	ami-0089a060	ami-4f88a12f
us-west2	US West (Oregon)	ami-0a829973	ami-d28398ab	ami-788e9501
sa-east-1	South America (Sao Paulo)	ami-3d631451	ami-c26413ae	ami-3c631450
eu-west-1	EU (Ireland)	ami-6a21c913	ami-1c21c965	ami-2920c850
eu-west-2	EU (London)	ami-176e7f73	ami-166e7f72	ami-b31302d7
eu-central-1	EU (Frankfurt)	ami-80f35fef	ami-1ecc6071	ami-4acc6025
ca-central-1	Canada (Central)	ami-1c02bd78	ami-440eb120	ami-1303bc77

AWS Regions		PAN-OS 7.1.11 AMI IDs that correspond to the licensing options		
ap-northeast-1	Asia Pacific (Tokyo)	ami-750dee13	ami-220eed44	ami-710cef17
ap-northeast-2	Asia Pacific (Seoul)	ami-06ba6368	ami-74bc651a	ami-96ba63f8
ap-southeast-1	Asia Pacific (Singapore)	ami-cc9a08af	ami-e2950781	ami-ae9a08cd
ap-southeast-2	Asia Pacific (Sydney)	ami-10d3cc73	ami-13d3cc70	ami-42d3cc21
ap-south-1	Asia Pacific (Mumbai)	ami-d4fe86bb	ami-2dfc8442	ami-a5fe86ca

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 ID by PAN-OS version for VM-Series Firewall on AWS GovCloud	BYOL	PAYG Bundle 2	PAYG Bundle 1
9.0.0	ami-acaac2cd	ami-7fa8c01e	ami-09553d68
8.1.0	ami-82ae24e3	ami-d4a923b5	ami-ccae24ad
8.0.13	ami-80bdd8e1	ami-f6b4d197	ami-a7bcd9c6
8.0.9	ami-ffcc5a9e	ami-d8cd5bb9	ami-c7ca5ca6
8.0.8	ami-c4109ba5	ami-ad159ecc	ami-682aa109
7.1.20	ami-aeab30cf	ami-afab30ce	ami-3fb3285e

Panorama

This section includes information on Panorama and compatible versions for devices that Panorama can manage, and on plugins available for Panorama.

- Plugins
- Panorama Hypervisor Support

Panorama Plugins

Palo Alto Networks introduced support for the extensible plugin architecture in Panorama 8.0. The following tables describe the features and functionality introduced with the Panorama plugins.

- VMware NSX
- Cloud Services
- Interconnect
- Public Cloud-AWS, Azure, GCP
- Cisco ACI
- VMware vCenter
- Cisco TrustSec
- Nutanix
- SD-WAN

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.

Plugin Version	Minimum Panorama Version	New Features or Changes
2.0.1	8.1.0	Introduces fixes for known issues. Minimum required plugin version for Panorama 8.1.
2.0.2	8.1.0	Introduces fixes for known issues.
2.0.3	8.1.0	Introduces fixes for known issues.
2.0.4	8.1.0	Introduces the Automated Full Dynamic Address Group Sync feature.
2.0.5	8.1.0	Introduces Proxy Bypass Support and Curl Call Timeout features.
3.0.0	9.0.3	Introduces the VM-Series firewall on VMware NSX-T for North-South traffic protection. *Panorama Plugin for VMware NSX 3.0.0 supports VMware NSX-T deployments only. Do not use the Panorama plugin for*

Plugin Version	Minimum Panorama Version	New Features or Changes
		VMware NSX 3.0.0 to manage the VM-Series firewall on NSX-V.
3.0.1	9.0.5	Supports upgrade from Panorama plugin NSX 2.0.5 for VMware NSX-V deployment.
3.1.0	9.1.0	Introduces the VM-Series firewall on VMware NSX-T for East-West traffic protection.

Cloud Services

The Cloud Services plugin supports Prisma Access and Cortex Data Lake. The minimum Panorama and plugin version depends on whether you use the Cloud Services plugin for Cortex Data Lake and Prisma Access, or if you use the plugin for Cortex Data Lake only.

Panorama or PAN-OS Minimum Version	Cloud Services Plugin Minimum Version
• If you use the Cloud Services plugin for Prisma Access and Cortex Data Lake—9.0.4 or later ***You must upgrade your Panorama to a minimum version of 9.0.4*** *before installing the 1.5 Cloud Services plugin or upgrading to 1.5 from an earlier version of the Cloud Services plugin. The Cloud Services plugin 1.5 and later require Panorama version 9.0.4 or later. Installing the 1.5 plugin with a Panorama running 8.1 or earlier will result in an unsupported configuration and data loss.* • If you use the Cloud Services plugin for Cortex Data Lake only—9.0.4 if your firewalls are managed by Panorama, 8.1.12 if your firewalls are not managed by Panorama.	• If you use the Cloud Services plugin for Prisma Access and Cortex Data Lake—1.5 • If you use the Cloud Services plugin for Cortex Data Lake only—1.2.0-h2

Interconnect

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

Plugin Version	Minimum Panorama Version	New Features or Changes
1.0.0	8.1.3	First plugin introduced to support a two-tier Panorama deployment for a horizontal scale-out architecture.

Public Cloud-AWS, Azure, GCP

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

Public Cloud Platform	AWS Plugin Version	Panorama Version (Minimum)	VM-Series Plugin Version (Minimum)	Features
AWS	1.0.0	8.1.x (8.1.3) 9.0.x	N/A	Enables support for VM Monitoring to monitor the virtual machine inventory within your AWS VPCs so that you can consistently enforce Security policy that automatically adapts to changes within your AWS deployment.
	1.0.1	8.1.x (8.1.3) 9.0.x	N/A	Introduces fixes for known issues.
	2.0.0	9.0.0 (9.0.6)	1.0.4	Enables support for: • VM Monitoring • Secure Kubernetes Services in an EKS Cluster
	2.0.1	9.0.0 (9.0.6)	1.0.4	Introduces a fix for a known issue.

Public Cloud Platform	Azure Plugin Version	Panorama Version (Minimum)	VM-Series Plugin Version (Minimum)	Features
Azure	1.0.0	8.1.x (8.1.3) 9.0.x	N/A	Enables support for VM Monitoring from Panorama. Configure the Panorama plugin for Azure to monitor the virtual machine inventory within your Azure subscription.
	2.0.0	8.1.x (8.1.8)	N/A	Enables support for: • Auto Scaling—Template v1.0

Public Cloud Platform	Azure Plugin Version	Panorama Version (Minimum)	VM-Series Plugin Version (Minimum)	Features
				• Azure Kubernetes Service (AKS) Cluster—Template v1.0
		9.0.x (9.0.3)	1.0.4	Enables support for: • Auto Scaling—Template v1.0 • Azure Kubernetes Service (AKS) Cluster—Template v1.0
	2.0.1	8.1.x (8.1.11) 9.0.x (9.0.5)	1.0.4	Introduces fixes for known issues.
	2.0.2	8.1.x (8.1.11) 9.0.x (9.0.5)	1.0.4	Introduces fixes for known issues.

Public Cloud Platform	GCP Plugin Version	Minimum Panorama Version	VM-Series Plugin Version	Features
GCP	1.0.0	8.1.x (8.1.3) 9.0.x	N/A	Enables you to secure Kubernetes services in a Google Kubernetes Engine (GKE) cluster and learn about the services that are exposed to the internet.

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.

Plugin Version	Minimum Panorama Version	Features
1.0.1	8.1.6	Introduces support for multiple IP addresses per endpoint and Cisco ACI 4.0 and later.
1.0.0	8.1.6	Enables support for Endpoint Monitoring from Panorama. Configure the Panorama plugin for Cisco ACI to monitor endpoints so that you can consistently enforce security

Plugin Version	Minimum Panorama Version	Features
		policy that automatically adapts to changes within your ACI deployment.

VMware vCenter

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

Plugin Version	Minimum Panorama Version	Features
1.0.0	9.0.2	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.

Cisco TrustSec

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

Plugin Version	Minimum Panorama Version	Features
1.0.0	9.0.3	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.

Nutanix

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

Plugin Version	Minimum Panorama Version	Features
1.0.0	9.0.4	Enables support for VM Monitoring from Panorama. Configure the Panorama plugin for Nutanix to monitor VM workloads so that you can consistently enforce security

Plugin Version	Minimum Panorama Version	Features
		policy that automatically adapts to changes within your Nutanix environment.

SD-WAN

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

Plugin Version	Minimum Panorama Version	Features
1.0.1	9.1.1	Improves monitoring experience and search filtering, and adds an option to display HA peers consecutively.
1.0.0	9.1.0	Enables support for SD-WAN from Panorama. Configure the Panorama plugin for SD-WANto 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.

Panorama Hypervisor Support

Before you install Panorama on a VMware ESXi, Hyper-V or KVM server, verify that the hypervisor meets the minimum version requirements to deploy Panorama.

Panorama Version	VMware ESXi Compatibility	KVM Compatibility	Hyper-V Compatibility	Public Cloud/ Partner IntegraCompatibility
PAN-OS 7.1	64-bit kernel-based VMware ESXi 5.1, 5.5, 6.0, or 6.5. The minimum supported version of the virtual hardware family type (also known as the VMware virtual hardware version) on the ESXi server is vmx-09. ESXi 5.5 and later versions supports a virtual disk of up to8TB. ESXi versions support one disk of up to 2TB.	Not Available	Not Available	Not Available
PAN-OS 8.1	64-bit kernel-based VMware ESXi 5.1, 5.5, 6.0, or 6.5. The supported version of the virtual hardware family type (also known as the VMware virtual hardware version) on the ESXi server is vmx-09. ESXi 5.5 and later versions supports one disk of up to 8TB. Earlier ESXi versions support one disk of up to 2TB.	(8.1.2) Ubuntu version 16.04 or CentOS7	(8.1.3) Windows Server 2016 with Hyper-V role or Hyper-V 2016	• Amazon AWS • Microsoft Azure • (8.1.1) Google Cloud Platform • (8.1.3) Amazon AWS GovCloud

Panorama Version	VMware ESXi Compatibility	KVM Compatibility	Hyper-V Compatibility	Public Cloud/ Partner IntegraCompatibility
PAN-OS 9.0	64-bit kernel-based VMware ESXi 5.1, 5.5, 6.0,6.5, or 6.7. The supported version of the virtual hardware family type (also known as the VMware virtual hardware version) on the ESXi server is vmx-09. ESXi 5.5 and later versions supports one disk of up to 8TB. Earlier ESXi versions support one disk of up to 2TB.	Ubuntu version 16.04 or CentOS7	Windows Server 2016 with Hyper-V role or Hyper-V 2016	• Amazon AWS • Microsoft Azure • Google Cloud Platform • Amazon AWS GovCloud • Nutanix AOS Version—5.10 Nutanix AOS Version—20170830.185 To manage VM-Series firewalls running supported versions of AHV. See VM-Series for Nutanix.
PAN-OS 9.1	64-bit kernel-based VMware ESXi 5.1, 5.5, 6.0, 6.5, or 6.7. The supported version of the virtual hardware family type (also known as the VMware virtual hardware version) on the ESXi server is vmx-09. ESXi 5.5 and later versions supports one disk of up to 8TB. Earlier ESXi versions support one disk of up to 2TB.	Ubuntu version 16.04 or CentOS7	Windows Server 2016 with Hyper-V role or Hyper-V 2016	• Amazon AWS • Microsoft Azure • Google Cloud Platform • Amazon AWS GovCloud • Nutanix AOS Version—5.10 Nutanix AOS Version—20170830.185 To manage VM-Series firewalls running supported versions of AHV. See VM-Series for Nutanix.

MFA Vendor Support

MFA Vendor Support

Palo Alto Networks® next-generation firewalls and Panorama™ appliances can integrate with multi-factor authentication (MFA) vendors using RADIUS and, in PAN-OS® 8.1 and later releases, using SAML.

Additionally, firewalls running a PAN-OS 8.1 or later release can 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	✓	✓	✓ PAN-OS 8.1 & later	–
Next-Generation Firewall and Panorama Administrator CLI	✓	✓	–	–
GlobalProtect™ Portal and Gateway Authentication	✓	✓	✓ PAN-OS 8.1 & later	–
Authentication Policy (Formerly Captive Portal Policy)	✓	✓	✓ PAN-OS 8.1 & later	✓ PAN-OS 8.1 & later **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® release.

- Cipher Suites Supported in PAN-OS 9.1
- Cipher Suites Supported in PAN-OS 9.0
- Cipher Suites Supported in PAN-OS 8.1
- Cipher Suites Supported in PAN-OS 7.1

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

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*.*

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 • RSA-CAMELLIA-128-SHA • RSA-CAMELLIA-256-SHA • RSA-3DES-SHA • RSA-AES-128-SHA • RSA-AES-256-SHA • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-SEED-SHA • DHE-RSA-AES-128-SHA • DHE-RSA-AES-256-SHA • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
	• ECDHE-RSA-AES-128-SHA • ECDHE-RSA-AES-256-SHA • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-128-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA • ECDHE-ECDSA-AES-256-SHA • 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 • AES-128-GCM-HMAC-SHA • AES-256-GCM-HMAC-SHA
GlobalProtect Portal—Browser Access	• SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA • RSA-CAMELLIA-128-SHA • RSA-CAMELLIA-256-SHA • RSA-3DES-SHA • RSA-AES-128-SHA • RSA-AES-256-SHA • 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 • DHE-RSA-AES-128-SHA • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA • ECDHE-ECDSA-AES-128-SHA • ECDHE-ECDSA-AES-256-SHA • 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 • 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 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*.*

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
IKE Certificate Support	• RSA • Keys—512-, 1024-, 2048-, and 3072-bit keys

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases

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

IKE—Encryption	• DES • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC
IKE—Message Authentication	• HMAC-MD5 • HMAC-SHA • 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-, 1024-, 2048-, 3072- and 4096-bit keys
	  • Digital signature algorithms—SHA, SHA-256, SHA-384, or SHA-512
	• ECDSA
	  • Keys—256- 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 (SSHv2 only)—Encryption
- SSH Decryption (SSHv2 only)—Message Authentication
- SSH Decryption (SSHv2 only)—Message Authentication
- 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 (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-96 • HMAC-RIPEMD-160 • HMAC-SHA
SSL/TLS Decryption	• SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA 512-, 1024-, 2048-, 3072-, 4096-, 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 • RSA-3DES-EDE-CBC-SHA • RSA-AES-128-CBC-SHA • RSA-AES-256-CBC-SHA • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384
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*	• DHE-RSA-3DES-EDE-CBC-SHA • DHE-RSA-AES-128-CBC-SHA • DHE-RSA-AES-256-CBC-SHA • 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 • ECDHE-RSA-AES-256-CBC-SHA • ECDHE-RSA-AES-128-CBC-SHA-256 • ECDHE-RSA-AES-256-CBC-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
decryption, you can use a hardware security module (HSM) to store the private keys used for SSL Inbound Inspection.	• ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-CBC-SHA • ECDHE-ECDSA-AES-256-CBC-SHA • 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 • RSA-CAMELLIA-128-SHA • RSA-CAMELLIA-256-SHA • RSA-3DES-SHA • RSA-AES-128-SHA • RSA-AES-256-SHA • RSA-AES-256-CBC-SHA • 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 • 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 • ECDHE-ECDSA-AES-256-SHA

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
	• ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
Administrative Sessions to CLI (SSH)—Encryption	• 3DES • ARCFOUR128 • ARCFOUR256 • BLOWFISH • CAST128 • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR • AES-256-CTR • AES-128-GCM • AES-256-GCM
Administrative Sessions to CLI (SSH)—Message Authentication	• UMAC-64 • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-96 • HMAC-RIPEMD-160 • HMAC-SHA • HMAC-SHA-256 • HMAC-SHA-512
Administrative Sessions to CLI (SSH)—Server Host Key Types	• RSA keys—2048-, 3072-, and 4096-bit keys • ECDSA keys—256-, 384-, and 521-bit keys
Administrative Sessions to CLI (SSH)—Key Exchange Algorithms	• diffie-hellman-group1-sha1 • diffie-hellman-group14-sha1 • diffie-hellman-group-exchange-sha1 • diffie-hellman-group-exchange-sha256 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-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 • 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 • RSA-3DES-SHA • RSA-SEED-SHA • RSA-CAMELLIA-128-SHA • RSA-CAMELLIA-256-SHA • RSA-AES-128-SHA • RSA-AES-128-SHA-256 • RSA-AES-256-SHA • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-SHA • DHE-RSA-AES-256-SHA

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.

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

Functions	Standards	Certificates
Asymmetric key generation		

Functions	Standards	Certificates
FFC key pair generation (key size 2048 bits)	FIPS PUB 186-4	**Appliances:** #[TBD] **VMs:** #[TBD]
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		
ECDSA-based key establishment	NIST SP 800-56A Revision 2	**Appliances:** #[TBD] **VMs:** #[TBD]
FFC-based key establishment	NIST SP 800-56A Revision 2	**Appliances:** #[TBD] **VMs:** #[TBD]
AES Data Encryption/Decryption		

Functions	Standards	Certificates
• 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 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:** #[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 curves" P-256, P-384, ISO/IEC 14888-3, Section 6.4	**Appliances:** #[TBD] **VMs:** #[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	**Appliances:**

Functions	Standards	Certificates
	NIST SP 800-90A	#[TBD] **VMs:** #[TBD]

Cipher Suites Supported in PAN-OS 9.0

The following topics list cipher suites that are supported on firewalls running a PAN-OS 9.0 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 9.0 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 9.0 GlobalProtect Cipher Suites
- PAN-OS 9.0 HA1 SSH Cipher Suites
- PAN-OS 9.0 IPSec Cipher Suites
- PAN-OS 9.0 IKE and Web Certificate Cipher Suites
- PAN-OS 9.0 Decryption Cipher Suites
- PAN-OS 9.0 Administrative Session Cipher Suites
- PAN-OS 9.0 PAN-OS-to-Panorama Connection Cipher Suites

PAN-OS 9.0 GlobalProtect Cipher Suites

The following table lists cipher suites for GlobalProtect™ supported on firewalls running a PAN-OS® 9.0 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 9.0 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 9.0 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 • RSA-CAMELLIA-128-SHA • RSA-CAMELLIA-256-SHA • RSA-3DES-SHA • RSA-AES-128-SHA • RSA-AES-256-SHA • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-SEED-SHA • DHE-RSA-AES-128-SHA • DHE-RSA-AES-256-SHA • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA

Feature or Function	Ciphers Supported in PAN-OS 9.0 Releases
	• ECDHE-RSA-AES-128-SHA • ECDHE-RSA-AES-256-SHA • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-128-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA • ECDHE-ECDSA-AES-256-SHA • 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 • AES-128-GCM-HMAC-SHA • AES-256-GCM-HMAC-SHA
GlobalProtect Portal—Browser Access	• SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA • RSA-CAMELLIA-128-SHA • RSA-CAMELLIA-256-SHA • RSA-3DES-SHA • RSA-AES-128-SHA • RSA-AES-256-SHA • 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 • DHE-RSA-AES-128-SHA • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA • ECDHE-ECDSA-AES-128-SHA • ECDHE-ECDSA-AES-256-SHA • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384

PAN-OS 9.0 IPSec Cipher Suites

The following table lists the cipher suites for IPSec that are supported on firewalls running a PAN-OS® 9.0 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 9.0 Cipher Suites Supported in FIPS-CC Mode*.*

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

Feature or Function	Ciphers Supported in PAN-OS 9.0 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 • 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 19 (256-bit elliptic curve group) with PFS enabled • Group 20 (384-bit elliptic curve group) with PFS enabled

PAN-OS 9.0 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 9.0 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 9.0 Cipher Suites Supported in FIPS-CC Mode*.*

Feature or Function	Ciphers Supported in PAN-OS 9.0 Releases
IKE Certificate Support	• RSA • Keys—512-, 1024-, 2048-, and 3072-bit keys

Feature or Function	Ciphers Supported in PAN-OS 9.0 Releases

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

IKE—Encryption	• DES • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC
IKE—Message Authentication	• HMAC-MD5 • HMAC-SHA • 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-, 1024-, 2048-, 3072- and 4096-bit keys
	  • Digital signature algorithms—SHA, SHA-256, SHA-384, or SHA-512
	• ECDSA
	  • Keys—256- and 384-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

PAN-OS 9.0 Decryption Cipher Suites

The following table lists cipher suites for decryption that are supported on firewalls running a PAN-OS® 9.0 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 9.0 Cipher Suites Supported in FIPS-CC Mode.

- 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 9.0 Releases
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-96 • HMAC-RIPEMD-160 • HMAC-SHA
SSL/TLS Decryption	• SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA 512-, 1024-, 2048-, 3072-, 4096-, 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 • RSA-3DES-EDE-CBC-SHA • RSA-AES-128-CBC-SHA • RSA-AES-256-CBC-SHA • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384
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*	• DHE-RSA-3DES-EDE-CBC-SHA • DHE-RSA-AES-128-CBC-SHA • DHE-RSA-AES-256-CBC-SHA • 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 • ECDHE-RSA-AES-256-CBC-SHA • ECDHE-RSA-AES-128-CBC-SHA-256 • ECDHE-RSA-AES-256-CBC-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 9.0 Releases
decryption, you can use a hardware security module (HSM) to store the private keys used for SSL Inbound Inspection.	• ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-CBC-SHA • ECDHE-ECDSA-AES-256-CBC-SHA • 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 9.0 Administrative Session Cipher Suites

The following table lists the cipher suites for administrative sessions that are supported on firewalls running a PAN-OS® 9.0 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 9.0 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 9.0 Releases
Administrative Sessions to Web Interface	• TLSv1.1 and TLSv1.2 cipher suites • RSA-SEED-SHA • RSA-CAMELLIA-128-SHA • RSA-CAMELLIA-256-SHA • RSA-3DES-SHA • RSA-AES-128-SHA • RSA-AES-256-SHA • RSA-AES-256-CBC-SHA • 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 • 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 • ECDHE-ECDSA-AES-256-SHA

Feature or Function	Ciphers Supported in PAN-OS 9.0 Releases
	• ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
Administrative Sessions to CLI (SSH)—Encryption	• 3DES • ARCFOUR128 • ARCFOUR256 • BLOWFISH • CAST128 • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR • AES-256-CTR • AES-128-GCM • AES-256-GCM
Administrative Sessions to CLI (SSH)—Message Authentication	• UMAC-64 • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-96 • HMAC-RIPEMD-160 • HMAC-SHA • HMAC-SHA-256 • HMAC-SHA-512
Administrative Sessions to CLI (SSH)—Server Host Key Types	• RSA keys—2048-, 3072-, and 4096-bit keys • ECDSA keys—256-, 384-, and 521-bit keys
Administrative Sessions to CLI (SSH)—Key Exchange Algorithms	• diffie-hellman-group1-sha1 • diffie-hellman-group14-sha1 • diffie-hellman-group-exchange-sha1 • diffie-hellman-group-exchange-sha256 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521

PAN-OS 9.0 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 9.0 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 9.0 Cipher Suites Supported in FIPS-CC Mode.

Feature or Function	Ciphers Supported in PAN-OS 9.0 Releases
HA1 SSH	• AES 128-bit cipher with Cipher Block Chaining • AES 128-bit cipher with Counter Mode • 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 9.0 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 9.0 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 9.0 Cipher Suites Supported in FIPS-CC Mode.

Feature or Function	Ciphers Supported in PAN-OS 9.0 Releases
PAN-OS to Panorama Connection	• RSA-RC4-128-SHA • RSA-3DES-SHA • RSA-SEED-SHA • RSA-CAMELLIA-128-SHA • RSA-CAMELLIA-256-SHA • RSA-AES-128-SHA • RSA-AES-128-SHA-256 • RSA-AES-256-SHA • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-SHA • DHE-RSA-AES-256-SHA

PAN-OS 9.0 Cipher Suites Supported in FIPS-CC Mode

The following table lists cipher suites that are supported on firewalls running a PAN-OS® 9.0 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 9.0

Functions	Standards	Certificates
Asymmetric key generation		

Functions	Standards	Certificates
FFC key pair generation (key size 2048 bits)	FIPS PUB 186-4	**Appliances:** #C1005 **VMs:** #C999
ECC key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	**Appliances:** #C1005 **VMs:** #C999
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	**Appliances:** #C1005 **VMs:** #C999
Cryptographic Key Generation (for IKE Peer Authentication)		
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	**Appliances:** #C1005 **VMs:** #C999
ECDSA key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	**Appliances:** #C1005 **VMs:** #C999
Cryptographic Key Establishment		
ECDSA-based key establishment	NIST SP 800-56A Revision 2	**Appliances:** #C1005 **VMs:** #C999
FFC-based key establishment	NIST SP 800-56A Revision 2	**Appliances:** #C1005 **VMs:** #C999
AES Data Encryption/Decryption		

Functions	Standards	Certificates
• 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:** #C1005 **VMs:** #C999
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:** #C1005 **VMs:** #C999
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	**Appliances:** #C1005 **VMs:** #C999
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:** #C1005 **VMs:** #C999
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:** #C1005 **VMs:** #C999
Random bit generation		
CTR_DRBG (AES-256)	ISO/IEC 18031:2011	**Appliances:**

Functions	Standards	Certificates
	NIST SP 800-90A	#C1005 **VMs:** #C999

Cipher Suites Supported in PAN-OS 8.1

The following topics list cipher suites that are supported on firewalls running a PAN-OS 8.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 8.1 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 8.1 GlobalProtect Cipher Suites
- PAN-OS 8.1 HA1 SSH Cipher Suites
- PAN-OS 8.1 IPSec Cipher Suites
- PAN-OS 8.1 IKE and Web Certificate Cipher Suites
- PAN-OS 8.1 Decryption Cipher Suites
- PAN-OS 8.1 Administrative Session Cipher Suites
- PAN-OS 8.1 PAN-OS-to-Panorama Connection Cipher Suites

PAN-OS 8.1 GlobalProtect Cipher Suites

The following table lists cipher suites for GlobalProtect™ supported on firewalls running a PAN-OS® 8.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 8.1 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 8.1 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 • RSA-CAMELLIA-128-SHA • RSA-CAMELLIA-256-SHA • RSA-3DES-SHA • RSA-AES-128-SHA • RSA-AES-256-SHA • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-SEED-SHA • DHE-RSA-AES-128-SHA • DHE-RSA-AES-256-SHA • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
	• ECDHE-RSA-AES-128-SHA • ECDHE-RSA-AES-256-SHA • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-128-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA • ECDHE-ECDSA-AES-256-SHA • 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 • AES-128-GCM-HMAC-SHA • AES-256-GCM-HMAC-SHA
GlobalProtect Portal—Browser Access	• SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA • RSA-CAMELLIA-128-SHA • RSA-CAMELLIA-256-SHA • RSA-3DES-SHA • RSA-AES-128-SHA • RSA-AES-256-SHA • 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 • DHE-RSA-AES-128-SHA • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA • ECDHE-ECDSA-AES-128-SHA • ECDHE-ECDSA-AES-256-SHA • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384

PAN-OS 8.1 IPSec Cipher Suites

The following table lists the cipher suites for IPSec that are supported on firewalls running a PAN-OS® 8.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 8.1 Cipher Suites Supported in FIPS-CC Mode.

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

Feature or Function	Ciphers Supported in PAN-OS 8.1 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 • 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 19 (256-bit elliptic curve group) with PFS enabled • Group 20 (384-bit elliptic curve group) with PFS enabled

PAN-OS 8.1 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 8.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 8.1 Cipher Suites Supported in FIPS-CC Mode.

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
IKE Certificate Support	• RSA • Keys—512-, 1024-, 2048-, and 3072-bit keys

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases

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

IKE—Encryption	• DES • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC
IKE—Message Authentication	• HMAC-MD5 • HMAC-SHA • 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-, 1024-, 2048-, 3072- and 4096-bit keys
	  • Digital signature algorithms—SHA, SHA-256, SHA-384, or SHA-512
	• ECDSA
	  • Keys—256- and 384-bit keys
	  • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

PAN-OS 8.1 Decryption Cipher Suites

The following table lists cipher suites for decryption that are supported on firewalls running a PAN-OS® 8.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 8.1 Cipher Suites Supported in FIPS-CC Mode.

- 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 8.1 Releases
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-96 • HMAC-RIPEMD-160 • HMAC-SHA
SSL/TLS Decryption	• SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA 512-, 1024-, 2048-, 3072-, 4096-, 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 2048-bit RSA keys.* • RSA-RC4-128-MD5 • RSA-RC4-128-SHA • RSA-3DES-EDE-CBC-SHA • RSA-AES-128-CBC-SHA • RSA-AES-256-CBC-SHA • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384
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*	• DHE-RSA-3DES-EDE-CBC-SHA • DHE-RSA-AES-128-CBC-SHA • DHE-RSA-AES-256-CBC-SHA • 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 • ECDHE-RSA-AES-256-CBC-SHA • ECDHE-RSA-AES-128-CBC-SHA-256 • ECDHE-RSA-AES-256-CBC-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
decryption, you can use a hardware security module (HSM) to store the private keys used for SSL Inbound Inspection.	• ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-CBC-SHA • ECDHE-ECDSA-AES-256-CBC-SHA • 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 8.1 Administrative Session Cipher Suites

The following table lists the cipher suites for administrative sessions that are supported on firewalls running a PAN-OS® 8.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 8.1 Cipher Suites Supported in FIPS-CC Mode.

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
Administrative Sessions to Web Interface	• TLSv1.1 and TLSv1.2 cipher suites • RSA-SEED-SHA • RSA-CAMELLIA-128-SHA • RSA-CAMELLIA-256-SHA • RSA-3DES-SHA • RSA-AES-128-SHA • RSA-AES-256-SHA • RSA-AES-256-CBC-SHA • 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 • 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 • ECDHE-ECDSA-AES-256-SHA

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
	• ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
Administrative Sessions to CLI (SSH)—Encryption	• 3DES • ARCFOUR128 • ARCFOUR256 • BLOWFISH • CAST128 • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR • AES-256-CTR • AES-128-GCM • AES-256-GCM
Administrative Sessions to CLI (SSH)—Message Authentication	• UMAC-64 • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-96 • HMAC-RIPEMD-160 • HMAC-SHA • HMAC-SHA-256 • HMAC-SHA-512
Administrative Sessions to CLI (SSH)—Server Host Key Types	• RSA keys—2048-, 3072-, and 4096-bit keys • ECDSA keys—256-, 384-, and 521-bit keys
Administrative Sessions to CLI (SSH)—Key Exchange Algorithms	• diffie-hellman-group1-sha1 • diffie-hellman-group14-sha1 • diffie-hellman-group-exchange-sha1 • diffie-hellman-group-exchange-sha256 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521

PAN-OS 8.1 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 8.1 release in normal (non-FIPS-CC) or FIPS-CC operational mode.

Feature or Function	Ciphers Supported in PAN-OS 8.1 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 8.1 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 8.1 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 8.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of PAN-OS 8.1 Cipher Suites Supported in FIPS-CC Mode.

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
PAN-OS to Panorama Connection	• RSA-RC4-128-SHA • RSA-3DES-SHA • RSA-SEED-SHA • RSA-CAMELLIA-128-SHA • RSA-CAMELLIA-256-SHA • RSA-AES-128-SHA • RSA-AES-128-SHA-256 • RSA-AES-256-SHA • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-SHA • DHE-RSA-AES-256-SHA

PAN-OS 8.1 Cipher Suites Supported in FIPS-CC Mode

The following table lists cipher suites that are supported on firewalls running a PAN-OS® 8.1 release in FIPS-CC mode.

If your firewall is running in normal (non-FIPS-CC) operational mode, see Cipher Suites Supported in PAN-OS 8.1

Functions	Standards	Certificates
Asymmetric key generation		
FFC key pair generation (key size 2048 bits)	FIPS PUB 186-4	**Appliances:** DSA #1485 **VMs:**

Functions	Standards	Certificates
		DSA #1497
ECC key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	**Appliances:** ECDSA #1570 **VMs:** ECDSA #1575
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	**Appliances:** RSA #3086 **VMs:** RSA #3090
Cryptographic Key Generation (for IKE Peer Authentication)		
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	**Appliances:** RSA #3086 **VMs:** RSA #3090
ECDSA key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	**Appliances:** ECDSA #1570 **VMs:** ECDSA #1575
Cryptographic Key Establishment		
ECDSA-based key establishment	NIST SP 800-56A Revision 2	**Appliances:** CVL #2119 **VMs:** CVL #2128
FFC-based key establishment	NIST SP 800-56A Revision 2	**Appliances:** CVL #2119 **VMs:** CVL #2128
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	**Appliances:** AES #5890 **VMs:**

Functions	Standards	Certificates
	• GCM as specified in ISO 19772 • NIST SP 800-38A/C/D/F • FIPS PUB 197	AES #5902
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:** RSA #3086 **VMs:** RSA #3090
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	**Appliances:** RSA #1570 **VMs:** RSA #1575
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:** SHS #4641 **VMs:** SHS #4658
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:** HMAC #3865 **VMs:** HMAC #3882
Random bit generation		
CTR_DRBG (AES-256)	ISO/IEC 18031:2011 NIST SP 800-90A	**Appliances:** DRBG #2451 **VMs:** DRBG #2464

Cipher Suites Supported in PAN-OS 7.1

The following topics list cipher suites that are supported on firewalls running a PAN-OS® 7.1 release in normal (non-FIPS-CC) operational mode.

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

PAN-OS 7.1 GlobalProtect Cipher Suites

The following table lists cipher suites for GlobalProtect™ that are supported on firewalls running a PAN-OS® 7.1 release in normal (non-FIPS-CC) operational mode.

Feature or Function	Ciphers Supported in PAN-OS 7.1 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 • RSA-CAMELLIA-128-SHA • RSA-CAMELLIA-256-SHA • RSA-3DES-SHA • RSA-AES-128-SHA • RSA-AES-256-SHA • DHE-RSA-AES-128-SHA • DHE-RSA-AES-256-SHA • EDH-RSA-3DES-SHA • ECDHE-ECDSA-AES-128-SHA • ECDHE-ECDSA-AES-256-SHA • 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 • AES-128-GCM-HMAC-SHA • AES-256-GCM-HMAC-SHA
GlobalProtect Portal—Browser Access	• SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA • RSA-CAMELLIA-128-SHA • RSA-CAMELLIA-256-SHA • RSA-3DES-SHA

Feature or Function	Ciphers Supported in PAN-OS 7.1 Releases
	• RSA-AES-128-SHA • RSA-AES-256-SHA • 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 • DHE-RSA-AES-128-SHA • EDH-RSA-3DES-SHA • ECDHE-ECDSA-AES-128-SHA • ECDHE-ECDSA-AES-256-SHA • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384

PAN-OS 7.1 IPSec Cipher Suites

The following table lists cipher suites for IPSec that are supported on firewalls running a PAN-OS® 7.1 release in normal (non-FIPS-CC) operational mode.

Feature or Function	Ciphers Supported in PAN-OS 7.1 Releases
IPSec—Encryption	• 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 • 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

Feature or Function	Ciphers Supported in PAN-OS 7.1 Releases
	• Group 19 (256-bit elliptic curve group) with PFS enabled • Group 20 (384-bit elliptic curve group) with PFS enabled

PAN-OS 7.1 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 7.1 release in normal (non-FIPS-CC) operational mode.

Feature or Function	Ciphers Supported in PAN-OS 7.1 Releases

IKE Certificate Support	• RSA
	  • Keys—512-, 1024-, 2048-, and 3072-bit keys
	  • Digital signature algorithms—SHA, SHA-256, SHA-384, or SHA-512
	• ECDSA
	  • Keys—256- 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
IKE—Message Authentication	• HMAC-MD5 • HMAC-SHA • 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-, 1024-, 2048-, 3072- and 4096-bit keys
	  • Digital signature algorithms—SHA, SHA-256, SHA-384, or SHA-512

Feature or Function	Ciphers Supported in PAN-OS 7.1 Releases

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

PAN-OS 7.1 Decryption Cipher Suites

The following table lists cipher suites for decryption that are supported on firewalls running a PAN-OS® 7.1 release in normal (non-FIPS-CC) operational mode.

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

Feature or Function	Ciphers Supported in PAN-OS 7.1 Releases
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-96 • HMAC-RIPEMD-160 • HMAC-SHA
SSL/TLS Decryption *Firewalls do not decrypt sessions where Diffie-Hellman key exchange is used for Forward Proxy Decryption in PAN-OS 7.1 and earlier releases.*	• SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA keys—512-, 1024-, 2048-, 3072-, 4096-, 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 2048-bit RSA keys.* • RSA-RC4-128-MD5 • RSA-RC4-128-SHA • RSA-3DES-EDE-CBC-SHA • RSA-AES-128-CBC-SHA • RSA-AES-256-CBC-SHA • 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 7.1 Releases
SSL/TLS Elliptical Curves	PAN-OS 7.1 does not support elliptical curve cryptography (ECC) certificates for SSL/TLS decryption.
SSL/TLS Decryption—Perfect Forward Secrecy (PFS) Ciphers (SSL Forward Proxy Decryption only)	• DHE-RSA-3DES-EDE-CBC-SHA • DHE-RSA-AES-128-CBC-SHA • DHE-RSA-AES-256-CBC-SHA • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-CBC-SHA • ECDHE-RSA-AES-256-CBC-SHA • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 Additional ciphers supported in PAN-OS 7.1.13 and later PAN-OS 7.1 releases: • DHE-RSA-AES-128-CBC-SHA-256 • DHE-RSA-AES-256-CBC-SHA-256 • ECDHE-RSA-AES-128-CBC-SHA-256 • ECDHE-RSA-AES-256-CBC-SHA-384

PAN-OS 7.1 Administrative Session Cipher Suites

The following table lists the cipher suites for administrative sessions that are supported on firewalls running a PAN-OS® 7.1 release in normal (non-FIPS-CC) operational 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 7.1 Releases
Administrative Sessions to Web Interface	• SSLv3, TLSv1.0, TLSv1.1 and TLSv1.2 cipher suites • RSA-3DES-EDE-CBC-SHA • RSA-SEED-CBC-SHA • RSA-CAMELLIA-128-CBC-SHA • RSA-CAMELLIA-256-CBC-SHA • RSA-AES-128-SHA • RSA-AES-128-SHA256 • RSA-AES-256-SHA • RSA-AES-256-SHA256 • RSA-AES-128-GCM-SHA256 • RSA-AES-256-GCM-SHA384 • DHE-RSA-3DES-EDE-SHA • DHE-RSA-AES-128-SHA • DHE-RSA-AES-256-SHA

Feature or Function	Ciphers Supported in PAN-OS 7.1 Releases
	• ECDHE-ECDSA-AES-128-SHA • ECDHE-ECDSA-AES-256-SHA • ECDHE-ECDSA-AES-128-GCM-SHA256 • ECDHE-ECDSA-AES-256-GCM-SHA384
Administrative Sessions to CLI (SSH)—Encryption	• 3DES • ARCFOUR128 • ARCFOUR256 • BLOWFISH • CAST128 • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR • AES-256-CTR • AES-128-GCM • AES-256-GCM
Administrative Sessions to CLI (SSH)—Message Authentication	• UMAC-64 • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-96 • HMAC-RIPEMD-160 • HMAC-SHA • HMAC-SHA-256 • HMAC-SHA-512
Administrative Sessions to CLI (SSH)—Server Host Key Types	• RSA keys—2048-bit keys • DSA keys—1024-bit keys
Administrative Sessions to CLI (SSH)—Key Exchange Algorithms	• diffie-hellman-group1-sha1 • diffie-hellman-group14-sha1 • diffie-hellman-group-exchange-sha1 • diffie-hellman-group-exchange-sha256 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521

PAN-OS 7.1 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 7.1 release in normal (non-FIPS-CC) operational mode.

Feature or Function	Ciphers Supported in PAN-OS 7.1 Releases
PAN-OS to Panorama Connection	• RSA-RC4-128-SHA • RSA-3DES-SHA • RSA-SEED-SHA • RSA-CAMELLIA-128-SHA • RSA-CAMELLIA-256-SHA • RSA-AES-128-SHA • RSA-AES-128-SHA-256 • RSA-AES-256-SHA • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-SHA • DHE-RSA-AES-256-SHA

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 table shows operating systems on which you can install each release of the GlobalProtect app:

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

Operating System	Release 4.1	Release 5.0	Release 5.1
Apple iOS and iPadOS (Installation instructions for 5.0 and 5.1.)			
iOS 8	–	–	–
iOS 9	–	–	–
iOS 10	✓ (64-bit devices only)	✓ (64-bit devices only)	✓ (64-bit devices only)
iOS 11	✓ (64-bit devices only)	✓ (64-bit devices only)	✓ (64-bit devices only)
iOS 12	–	✓ (64-bit devices only)	✓ (64-bit devices only)
iOS 13	–	✓ *5.0.8 & later (64-bit devices only)	✓ *5.0.8 & later (64-bit devices only)
Apple Mac (Installation instructions for 4.1, 5.0, and 5.1.)			
Mac OS X 10.5 (64-bit only)	–	–	–
Mac OS X 10.6	–	–	–
Mac OS X 10.7	–	–	–

Operating System	Release 4.1	Release 5.0	Release 5.1
Mac OS X 10.8	–	–	–
Mac OS X 10.9	–	–	–
Mac OS X 10.10	✓	–	–
macOS 10.11	✓	✓	✓
macOS 10.12	✓	✓	✓
macOS 10.13	✓	✓	✓
macOS 10.14	✓ *4.1.5 & later	✓	✓
macOS 10.15	–	✓ *5.0.4 & later	✓ *5.0.4 & later
Google Android (Installation instructions for 5.0 and 5.1.)			
Google Android 4.4	✓	✓	✓
Google Android 5.x	✓	✓	✓
Google Android 6.x	✓	✓	✓
Google Android 7.x	✓	✓	✓
Google Android 8.x	✓	✓	✓
Google Android 9.x	✓ *4.1.5 & later	✓	✓
Chrome OS Systems Supporting Android Apps	–	✓	✓
Google Chrome (Installation instructions for 4.1, 5.0, and 5.1.)			
Google Chrome OS 45 and later releases	✓		
Chrome OS Systems Supporting Android Apps	–	✓	✓

Operating System	Release 4.1	Release 5.0	Release 5.1
Internet of Things (IoT) (Installation instructions for 5.1 and supported features list.)			
Android	–	–	✓
Raspbian	–	–	✓
Ubuntu	–	–	✓
Windows IoT Enterprise	–	–	✓
Linux (Installation instructions for 4.1, 5.0, and 5.1.)			
CentOS 7.7	✓	✓	✓ CLI-based and GUI-based GlobalProtect app
CentOS 7.6	✓	✓	✓ CLI-based and GUI-based GlobalProtect app
CentOS 7.5	✓	✓	✓ CLI-based and GUI-based GlobalProtect app
CentOS 7.4	✓	✓	✓ CLI-based and GUI-based GlobalProtect app
CentOS 7.3	✓	✓	✓ CLI-based and GUI-based GlobalProtect app
CentOS 7.2	✓	✓	✓ CLI-based and GUI-based GlobalProtect app
CentOS 7.1	✓	✓	✓ CLI-based and GUI-based GlobalProtect app
CentOS 7.0	✓	✓	✓

Operating System	Release 4.1	Release 5.0	Release 5.1
			CLI-based and GUI-based GlobalProtect app
Red Hat Enterprise Linux (RHEL) 7.0 through 7.7	✓	✓	✓ Releases 7.0 through 7.6: CLI-based GlobalProtect app only
Ubuntu 19.04	✓	✓	✓ CLI-based and GUI-based GlobalProtect app
Ubuntu 18.04 2 LTS	✓	✓	✓ CLI-based and GUI-based GlobalProtect app
Ubuntu 18.04 1 LTS	✓	✓	✓ CLI-based and GUI-based GlobalProtect app
Ubuntu 18.04 LTS	✓	✓	✓ CLI-based and GUI-based GlobalProtect app
Ubuntu 16.04 LTS	✓	✓	✓ CLI-based and GUI-based GlobalProtect app
Ubuntu 14.04	✓	✓	✓ CLI-based and GUI-based GlobalProtect app
Microsoft Windows (Installation instructions for 4.1, 5.0, and 5.1.)			
Windows XP (32-bit only)	–	–	–
Windows Vista	–	–	–
Windows 7	✓	✓	✓
Windows 8	✓	✓	✓

Operating System	Release 4.1	Release 5.0	Release 5.1
Windows 8.1	✓	✓	✓
Windows 10	✓	✓	✓
Windows 10 UWP	✓ Intel devices only	✓ Intel devices only	✓ Intel and ARM devices

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®.

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 Release Version
iOS built-in IPSec client	7.1
Android built-in IPSec client	7.1
VPNC on Ubuntu Linux 10.04 and later versions and CentOS 6 and later versions	7.1
strongSwan on Ubuntu Linux and CentOS*	7.1
* To set up authentication for strongSwan Ubuntu and CentOS clients for PAN-OS 7.1 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 Certificates or User Credentials	✓	✓	✓	✓

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
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-7050	2000
PA-5250	2000
PA-5050	1000
PA-5020	1000
PA-3250	1500
PA-3050	1000
VM-Series Firewalls	
VM-700	1000
VM-500	500
VM-300	500
VM-200	500
VM-100	500

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

What Features Does GlobalProtect Support?

The following table lists the features supported on GlobalProtect by 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?.

Feature	Android	iOS	Chrome If you are using 4.1.0, to avail of new features use the Android App 5.0 or later	Windows	Windows 10 UWP	Mac	Linux
Authentication							
App Login Enhancements	4.0.0	4.0.0	—	4.0.0	—	4.0.0	—
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	—	4.0.0	5.1
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	—	—	—

Feature	Android	iOS	Chrome If you are using 4.1.0, to avail of new features use the Android App 5.0 or later	Windows	Windows 10 UWP	Mac	Linux
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
Pre-Logon Followed by Two-Factor Authentication	–	–	–	4.1.0	–	4.1.0	–
Pre-Logon Followed by SAML Authentication	–	–	–	4.1.0	–	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	–	–	–	–	–	–
VPN Connections							
IPSec	1.3.0	1.3.0	3.1.1	1.0.0	–	1.0.0	4.1.0
SSL	1.3.0	1.3.0	3.1.1	1.0.0	3.1.3	1.0.0	4.1.0
SSL Tunnel Enforcement	5.1.0	5.1.0	–	5.1.0	–	5.1.0	5.0.6 (CLI) 5.1.0 (GUI)

Feature	Android	iOS	Chrome If you are using 4.1.0, to avail of new features use the Android App 5.0 or later	Windows	Windows 10 UWP	Mac	Linux
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)	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	1.0.0	4.1.0
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							

Feature	Android	iOS	Chrome If you are using 4.1.0, to avail of new features use the Android App 5.0 or later	Windows	Windows 10 UWP	Mac	Linux
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
Networking							
IPv4 Addressing	1.3.0	1.3.0	3.1.1	1.0.0	3.1.3	1.0.0	4.1
IPv6 Addressing	4.0.0	4.0.0	4.0.0	4.0.0	4.0.0	4.0.0	4.1
Split Tunnel to Exclude by Access Route	—	4.0.0	4.0.0	4.0.0	4.0.0	4.0.0	4.1
Optimized Split Tunneling for GlobalProtect	—	—	—	4.1.0	—	4.1.0	—
Customization							
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	-	-	-	4.1.0	-	4.1.0	-

Feature	Android	iOS	Chrome If you are using 4.1.0, to avail of new features use the Android App 5.0 or later	Windows	Windows 10 UWP	Mac	Linux
of Web Browser in Captive Portal Environment							
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 New Endpoint Attributes	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0
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	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 If you are using 4.1.0, to avail of new features use the Android App 5.0 or later	Windows	Windows 10 UWP	Mac	Linux
and Authentication Cookie Usage Restrictions							
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 Deployments	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0
FIPS-CC Mode for GlobalProtect	–	–	–	5.0.0	–	5.0.0	–
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	–
GlobalProtect Credentials Provier Pre-Logon Connection Status	–	–	–	4.1.0	–	–	–

Feature	Android	iOS	Chrome If you are using 4.1.0, to avail of new features use the Android App 5.0 or later	Windows	Windows 10 UWP	Mac	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-	3.1.0	—

Feature	Android	iOS	Chrome If you are using 4.1.0, to avail of new features use the Android App 5.0 or later	Windows	Windows 10 UWP	Mac	Linux
					party MDM)		
Certificate selection by OID	—	—	—	3.0.0	—	3.0.0	—
Deployment of SSL Forward Proxy CA certificates in the trust store	—	—	—	3.0.0	—	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)	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	—	—	—	2.2.0	—	2.2.0	4.1.0
Welcome and help pages	1.3.0	1.3.0	3.0.0	1.0.0	—	1.0.0	—
Other							
Support for 100 Manual Gateways	5.0.3	5.0.7	-	5.0.3	-	5.0.3	5.0.3

Feature	Android	iOS	Chrome If you are using 4.1.0, to avail of new features use the Android App 5.0 or later	Windows	Windows 10 UWP	Mac	Linux
User Location Visibility on GlobalProtect Gateways and Portals	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0
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	—	—	—	—

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 domain, client process, and video streaming application	–	–	–	✓

Feature	Android	Raspbian	Ubuntu	Windows IoT Enterprise
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	—	—	—	✓
Multi-factor authentication	—	—	—	✓
SAML authentication	—	—	—	✓
Expired Active Directory password change for remote users	—	—	—	✓
Active Directory password change using the GlobalProtect	—	—	—	✓

Feature	Android	Raspbian	Ubuntu	Windows IoT Enterprise
Credential Provider				
SSO (Credential Provider)	—	—	—	✓
Kerberos SSO	—	—	—	✓
Welcome and help pages	—	—	—	✓
Headless-mode without icon, pop-up, dialogs, 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 – indicates the feature is not supported.

Feature	AirWatch	Microsoft Intune	MobileIron	Google Admin Console
GlobalProtect app deployment	✓	✓	✓	✓
Always on VPN Configuration	✓	✓ (Android, iOS, and Windows 10 UWP only)	✓ (iOS and Android only)	–
Remote access VPN configuration	✓	✓ (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:

- **Panorama Managed Prisma Access**—If you are already using Panorama to manage your next-gen firewalls, you can use Panorama to deploy Prisma Access and leverage your existing configurations. You'll need the Cloud Services plugin to use Panorama for Prisma Access.
- **Cloud Managed Prisma Access**—If you aren't using Panorama, the Prisma Access app on the hub gives you a simplified way onboard and manage Prisma Access.

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've activated your Prisma Access license. This means you must decide how you want to manage Prisma Access before begin setting up the product. See Features in Panorama Managed Prisma Access to select your management interface.

For a description of the features that are supported in GlobalProtect, see What Features Does GlobalProtect Support?

Features in Panorama Managed Prisma Access

Feature	Prisma Access (Panorama-Managed)	Prisma Access (Cloud-Managed)
Authentication		
Multi-factor (MFA) authentication policy	✓	Supports only SAML and local authentication
On-Premise LDAP Authentication	✓	
Certificate-based authentication	✓ Supported for both IPSec and Remote Access.	
Single Sign-On (SSO)		
SSO (Credential Provider)	✓	Supports only SAML and local authentication
Kerberos SSO	✓ Kerberos is supported for Windows clients only.	
Security Features		
SaaS Application Hosting Characteristics	✓	—

Feature	Prisma Access (Panorama-Managed)	Prisma Access (Cloud-Managed)
	This feature has the following Logging Service-based limitations: • **Saas Application Usage** report (**Monitor** > **PDF Reports** > **SaaS Application Usage**): **Include user group information in the report** not available • **Custom Report** (**Monitor** > **Manage Custom Reports**): **Detailed Logs (Slower)** not available in **Database** area • Scheduled and pre-defined reports are not supported.	
Simplified App-ID	✓	
HTTP Header Insertion and Modification	✓	
Service-Based Session Timeouts	✓	
Automatic SAN Support for SSL Decryption	✓	
WildFire Script Sample Analysis	✓	✓
Management Features		
Rule Usage Tracking	✓	–
Configuration Table Export	✓	
Reporting Engine Enhancements	✓	
Enhanced Application Logging	✓	✓
Administratively logout mobile users	✓ This feature is introduced in version 1.4.	–
Mobile Features		
Optimized Split Tunneling for GlobalProtect	✓	–

Feature	Prisma Access (Panorama-Managed)	Prisma Access (Cloud-Managed)
Extensible Authentication Protocol (EAP) Support for RADIUS	✓	
Support for Multiple Username Formats	✓	
Content Inspection Features		
New Scheduling Options for Application and Threat Content Updates	Managed by Palo Alto Networks.	Managed by Palo Alto Networks.
Five-Minute Updates for PAN-DB Malware and Phishing URL Categories	Managed by Palo Alto Networks.	Managed by Palo Alto Networks.
Routing Features		
Static Routing	✓	✓
Dynamic Routing (BGP)	✓	✓
Dynamic Routing (OSPF)	–	–
VPN Connections		
IPSec tunnels See Prisma Access IPSec Tunnel Configuration Parameters for a list of the supported IPSec tunnel parameters.	✓	✓
SSL SSL is supported only for Remote Access, not for site-to-site VPNs.	✓	✓
Clientless VPN	✓	✓
Hybrid Deployments		
Hybrid Deployments	✓ Using on-premise gateways with Prisma Access gateways is supported.	–
Prisma Access gateway priority	✓	–

Feature	Prisma Access (Panorama-Managed)	Prisma Access (Cloud-Managed)
	Supported for deployments that have on-premise GlobalProtect gateways. You can set a priority separately for on-premise gateways and collectively for all gateways in Prisma Access. You can also specify source regions for on-premise gateways.	
Manual gateway selection	✓ Users can manually select a cloud gateway from their client machines using the GlobalProtect app.	✓ Users can manually select a cloud gateway from their client machines using the GlobalProtect app.
GlobalProtect Gateway Modes		
External mode	✓	✓
Internal mode	– You cannot configure Prisma Access gateways as internal gateways; however, you can add one or more on-premise gateways and configure them as internal gateways.	–
GlobalProtect App Connect Methods		
User-logon (always on)	✓	Supports user-logon (always on) only
Pre-logon (always-on)	✓	
Pre-logon (then on-demand)	✓	
On-demand	✓	
Security Profiles		
Security profiles scan traffic for and protect against threats, attacks, misuse, and abuse:	✓	✓ Supports predefined security profiles only
Networking		
IPv4 addressing	✓	✓

Feature	Prisma Access (Panorama-Managed)	Prisma Access (Cloud-Managed)
IPv6 addressing	–	–
Split tunnel based on access route	✓	–
Split tunnel based on destination domain, client process, and video streaming application	✓	
NetFlow	–	–
QoS Prisma Access uses the same security policies and QoS profiles and supports the same Differentiated Services Code Point (DSCP) markings as next-generation Palo Alto Networks firewalls.	✓	✓
NAT Prisma Access automatically manages outbound NAT; you cannot the configure the settings.	✓	✓
SSL VPN connections	✓	✓
Policies		
Policy-Based Forwarding	–	–
Policy Optimizer	–	–
DoS Protection	✓ The Prisma Access infrastructure manages DoS protection.	✓
User and Group-Based Policy with Directory Sync		✓
Dynamic Address Groups		✓
MDM	✓	–
MDM integration with HIP	✓ Prisma Access does not support AirWatch MDM HIP service	–

Feature	Prisma Access (Panorama-Managed)	Prisma Access (Cloud-Managed)
	integration; however, you can use the GlobalProtect App for iOS and Android MDM Integration for HIP-Based Policy Enforcement.	
Virtual Routers	–	–
Policy rule hit count	✓	–
HIP Reports		
HIP	✓	✓
HIP match log	✓	✓
HIP-based security policy	✓	✓
HIP notification	✓	–
HIP report submission	✓	✓
HIP Checks	✓	✓
HIP Objects and Profiles	✓	✓
HIP report viewing	✓ This feature is introduced in version 1.5.	–
HIP redistribution	✓ This feature is introduced in version 1.5.	–
Tunnel Monitoring		
Dead Peer Detection (DPD)	✓	✓
ICMP	✓	✓
Bidirectional Forwarding Detection (BFD)	–	–
App-ID		

Feature	Prisma Access (Panorama-Managed)	Prisma Access (Cloud-Managed)
App-ID	✓ Any applications that are supported by VM-Series firewalls are supported by Prisma Access.	✓
High Availability		
High Availability	✓	–
Logging		
Log Settings	✓	–
Cortex Data Lake Log Storage	✓	✓
Log Forwarding app Forward logs stored in Cortex Data Lake to syslog and/or email destinations.	✓	✓
Monitoring		
SNMP Use Tunnel Monitoring instead of SNMP to monitor the tunnels in Prisma Access.	–	–

Prisma Access IPSec Tunnel Configuration Parameters

The following table describes the supported IPSec tunnel configuration parameters in Prisma Access. A check mark indicates that the parameter is supported; a dash (—) indicates that the parameter is not supported.

Instead of creating IPSec and IKE crypto profiles and gateways from scratch, you can use one of the predefined IPSec and IKE templates for common IPSec and SD-WAN devices, which simplify the onboarding of service connections that use one of the devices to terminate the connection.

Feature	Support
IPSec Tunnel	✓
GRE Tunnel	—
IKE Versions	
IKE v1	✓
IKE v2	✓
IPSec Phase 1 DH-Group	
Group 1	✓
Group 2	✓ (Default)
Group 5	✓
Group 14	✓
Group 19	✓
Group 20	✓
IPSec Phase 1 Auth	
MD5	✓
SHA1	✓ (Default)

Feature	Support
SHA256	✓
SHA384	✓
SHA512	✓
IPSec Phase 1 Encryption	
DES	✓
3DES	✓ (Default)
AES-128-CBC	✓ (Default)
AES-192-CBC	✓
AES-256-CBC	✓
IPSec Phase 1 Key Lifetime Default	
IPSec Phase 1 Key Lifetime Default	✓ (8 Hours)
IPSec Phase 1 Peer Authentication	
Pre-Shared Key	✓
Certificate	✓
IKE Peer Identification	
FQDN	✓
IP Address	✓
User FQDN	✓
IKE Peer	
As Static Peer	✓
As Dynamic Peer	✓

Feature	Support
Options	
NAT Traversal	✓
Passive Mode	✓
Ability to Negotiate Tunnel	
Per Subnet Pair	✓
Per Pair of Hosts	✓
Per Gateway Pair	✓
IPSec Phase 2 DH-Group	
Group 1	✓
Group 2	✓ (Default)
Group 5	✓
Group 14	✓
Group 19	✓
Group 20	✓
No PFS	✓
IPSec Phase 2 Auth	
MD5	✓
SHA1	✓ (Default)
SHA256	✓
SHA384	✓
SHA512	✓

Feature	Support
None	✓
IPSec Phase 2 Encryption	
DES	✓
3DES	✓ (Default)
AES-128-CBC	✓ (Default)
AES-192-CBC	✓
AES-256-CBC	✓
AES-128-CCM	✓
AES-128-GCM	✓
AES-256-GCM	✓
NULL	✓
IPSec Protocol	
ESP	✓
AH	✓
IPSec Phase 2 Key Lifetime Default	
IPSec Phase 2 Key Lifetime Default	✓ (1 Hour)

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?
- Which Servers Can the User-ID Agent Monitor?
- Where Can I Install the User-ID Credential Service?

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.

Operating System	Release 7.0	Release 8.1	Release 9.0	Release 9.1
Windows Server 2008 and 2008 R2	✓	✓	✓	✓
Windows Server 2012 and 2012 R2	✓	✓	✓	✓
Windows Server 2016	–	✓	✓	✓
Windows Server 2019	–	–	✓ *9.0.2 & later	✓

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—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 9.1 (all releases)
	  • PAN-OS 9.0.2 and later PAN-OS 9.0 releases
	  • PAN-OS 8.1.8 and later PAN-OS 8.1 releases
	  • PAN-OS 7.1.23 and later PAN-OS 7.1 releases
	• 2016—with Windows User-ID agent 8.0.5 and later releases or with PAN-OS integrated User-ID agents running the following PAN-OS releases:
	  • PAN-OS 9.1 (all releases)
	  • PAN-OS 9.0 (all releases)
	  • PAN-OS 8.1 (all releases)
	  • PAN-OS 7.1.12 and later PAN-OS 7.1 releases
	• 2013

Microsoft Windows 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 9.1 (all releases)
	  • PAN-OS 9.0.2 and later PAN-OS 9.0 releases
	  • PAN-OS 8.1.8 and later PAN-OS 8.1 releases
	  • PAN-OS 7.1.23 and later PAN-OS 7.1 releases
	• 2016—only with Windows User-ID agent 8.1 and later releases or with PAN-OS integrated User-ID agents running the following PAN-OS releases:
	  • PAN-OS 9.1 (all releases)
	  • PAN-OS 9.0 (all releases)
	  • PAN-OS 8.1 (all releases)
	  • PAN-OS 7.1.12 and later PAN-OS 7.1 releases
	• 2012 and 2012 R2
	• 2008 and 2008 R2

Novell eDirectory Server	8.8

Where Can I Install the User-ID Credential Service?

The following table shows the Read-Only Domain Controllers (RODCs) on which you can install each release of the Windows-based User-ID™ agent with the User-ID credential service to detect credential submissions.

Operating System	Release 8.1	Release 9.0	Release 9.1
Windows Server 2012 and 2012 R2	✓	✓	✓

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?
> How Many TS Agents Does My Firewall Model Support?

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 TS agent.

Operating System	TS agent 7.0 Release	TS agent 8.1 Release	TS agent 9.0 Release	TS agent 9.1 Release
Windows Server 2008 and 2008 R2	✓	✓	✓	✓
Windows Server 2012 R2	✓	✓	✓	✓
Windows Server 2016	–	✓ *8.1.1 & later	✓	✓
Windows Server 2019	–	–	✓	✓
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 Model 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 8.1 and earlier PAN-OS Releases	PAN-OS 9.0 Release	PAN-OS 9.1 Release
PA-7000 Series	1000	2000	2000
PA-7050 SMC-B	not applicable	2500	2500
PA-5200 Series	1000	2500	2500
PA-3200 Series	400	2000	2000
PA-3000 Series	400	400	400
PA-800 Series	400	1000	1000
PA-220R	400	400	400
PA-220	400	400	400
VM-700	1000	2500	2500
VM-300	400	400	400
VM-100	400	400	400
VM-50 Lite	400	400	400

Cortex XDR

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. The topics below reflect support for both the new Cortex XDR agent and earlier Traps releases.

Palo Alto Networks strives to support the latest major operating systems. After a new operating system is available, there can be a short delay in our support of the operating system as we test interoperability with the production release.

Palo Alto Networks supports operating systems until they reach end-of-life except where noted in each table.

You can install the agent on supported physical and virtual endpoints:

- Agent Versions Supported with Cortex XDR
- Mobile Operating Systems Supported with Cortex XDR and Traps
- Endpoint Operating Systems Supported with Cortex XDR and Traps
- Virtual Applications Supported with Cortex XDR and Traps
- Cortex XDR and Traps Compatibility with Third-Party Security Products

Agent Versions Supported with Cortex XDR

The following table displays the minimum agent versions supported with Cortex XDR:

Agent Version	Minimum Supported
Traps agent 5.0	5.0.8
Traps agent 6.0	—
Traps agent 6.1	6.1.4
Cortex XDR agent 7.0	7.0.0

Mobile Operating Systems Supported with Cortex XDR and Traps

The following table shows the mobile operating systems on which you can install each release of the agent.

Endpoint Operating System	Traps 5.0	Traps 6.0	Cortex XDR 7.0
Android			
5	✓	✓	✓
6	✓	✓	✓
7	✓	✓	✓

Endpoint Operating System	Traps 5.0	Traps 6.0	Cortex XDR 7.0
8	✓	✓	✓
9	✓	✓	✓
10	–	✓	✓

Endpoint Operating Systems Supported with Cortex XDR and Traps

The following table shows the endpoint operating systems on which you can install each release of the agent. These operating systems are also supported with supported Citrix and VMware virtual applications (see Virtual Applications Supported with Traps).

Endpoint Operating System	Traps 4.2	Traps 5.0	Traps 6.0	Traps 6.1	Cortex XDR 7.0
Linux (x86 64-bit only)					
Amazon Linux 2 LTS Candidate (2017.12)	✓ *4.2.1 & later	✓ *5.0.1 & later	✓	✓	✓
Amazon Linux 2 LTS Candidate 2	✓ *4.2.1 & later	✓ *5.0.1 & later	✓	✓	✓
Amazon Linux AMI 2017.03	–	–	✓	✓	✓
Amazon Linux AMI 2017.09	–	–	✓	✓	✓
Amazon Linux AMI 2018.03	–	–	✓	✓	✓
CentOS 6	✓	✓	✓	✓	✓
CentOS 7	✓	✓	✓	✓	✓
CentOS 8	–	–	–	–	✓ *7.0.1 only and with UEFI

Endpoint Operating System	Traps 4.2	Traps 5.0	Traps 6.0	Traps 6.1	Cortex XDR 7.0
					secure boot disabled
Debian 8	✓	✓ *5.0.1 & later	✓	✓	✓
Debian 9	✓	✓ *5.0.1 & later	✓	✓	✓
Oracle 6	✓	✓ *5.0.1 & later	✓	✓	✓
Oracle 7	✓	✓ *5.0.1 & later	✓	✓	✓
Oracle 8	–	–	–	–	✓ *7.0.1 only, and with UEFI secure boot disabled
Red Hat Enterprise Linux 6	✓	✓	✓	✓	✓
Red Hat Enterprise Linux 7	✓	✓	✓	✓	✓
Red Hat Enterprise Linux 8	–	–	–	–	✓ *7.0.1 release only, and with UEFI secure boot disabled
SUSE Linux Enterprise Server 12	✓	✓	✓	✓	✓
Ubuntu Server 12	✓	✓	✓	✓	✓
Ubuntu Server 14	✓	✓	✓	✓	✓

Endpoint Operating System	Traps 4.2	Traps 5.0	Traps 6.0	Traps 6.1	Cortex XDR 7.0
Ubuntu Server 16	✓	✓	✓	✓	✓
Ubuntu Server 18	–	–	✓	✓	✓
Mac					
OS X 10.10	–	–	–	–	–
OS X 10.11	✓	✓	✓	✓	–
macOS 10.12	✓	✓	✓	✓	✓
macOS 10.13	✓	✓	✓	✓	✓
macOS 10.14	✓ *4.2.1-h3 & later	✓ *5.0.3-h1 & later	✓	✓	✓
macOS 10.15	✓ *4.2.6 & later	–	–	✓ *6.1.2 & later	✓
Windows					
Windows 2000 and below	–	–	–	–	–
Windows XP (32-bit) (SP2 & earlier)	–	–	–	–	–
Windows XP (32-bit) (SP3 & later)	✓	✓ Supported until Traps 5.0 end-of-life	–	–	–
Windows XP (64 bit)	–	–	–	–	–
Windows Vista (SP1 & later; FIPS mode)	✓	✓	–	–	–

Endpoint Operating System	Traps 4.2	Traps 5.0	Traps 6.0	Traps 6.1	Cortex XDR 7.0
		Supported until Traps 5.0 end-of-life			
Windows 7 (RTM and SP1; FIPS mode; all editions except Home) SHA2 code signing supported with Microsoft Security Advisory 3033929	✓	✓	✓	✓	✓
Windows Embedded 7 (Standard and POSReady)	✓	✓	–	–	–
Windows Embedded 7 SP1 (Standard and POSReady)	✓	✓	✓	✓	✓
Windows 8.1 (and with FIPS mode)	✓	✓	✓	✓	✓
Windows Embedded 8.1 Professional	✓	✓	✓	✓	✓
Windows Embedded POSReady 2009	✓	✓	✓	✓	✓
Windows 10 Education	–	✓ *5.0.4 & later	✓	✓	✓
Windows 10 Pro	✓	✓	✓	✓	✓

Endpoint Operating System	Traps 4.2	Traps 5.0	Traps 6.0	Traps 6.1	Cortex XDR 7.0
(CB and CBB)					
Windows 10 Enterprise (CB, CBB, and LTSB)	✓	✓	✓	✓	✓
Windows 10 Fall Creators Update 1709	✓	✓	✓	✓	✓
Windows 10 Update 1803	✓	✓	✓	✓	✓
Windows 10 Update 1809 (Standard, Enterprise, Professional)	✓ *4.2.3 & later	✓ *5.0.4 & later	✓	✓	✓
Windows 10 RS6 Update 1903 (Standard, Enterprise, Professional)	✓ *4.2.5 & later	✓	✓	✓	✓
Windows 10 Update 1909 (Standard, Enterprise, Professional)	✓ *4.2.6 & later	✓	✓	✓ *6.1.3 & later	✓
Windows 10 Enterprise 2019 LTSC	✓ *4.2.3 & later	✓ *5.0.4 & later	✓	✓	✓
Windows Server 2003 (SP1 & earlier)	–	–	–	–	–
Windows Server 2003 (32-bit) (SP2 & later)	✓	✓ Supported until Traps 5.0 end-of-life	–	–	–

Endpoint Operating System	Traps 4.2	Traps 5.0	Traps 6.0	Traps 6.1	Cortex XDR 7.0
Windows Server 2003 (64-bit)	–	–	–	–	–
Windows Server 2003 R2 (32-bit) (SP2 & later)	✓	✓ Supported until Traps 5.0 end-of-life	–	–	–
Windows Server 2003 R2 (64 bit)	–	–	–	–	–
Windows Server 2008 (All editions; FIPS mode)	✓	✓ Supported until Traps 5.0 end-of-life	–	–	–
Windows Server 2008 R2 (All editions; FIPS mode)	✓	✓	✓ Supported until January 2023 (Microsoft EOL + 3 years)	✓ Supported until January 2023 (Microsoft EOL + 3 years)	✓ Supported until January 2023 (Microsoft EOL + 3 years)
Windows Server 2012 (All editions; FIPS mode)	✓	✓	✓	✓	✓
Windows Server 2012 R2 (All editions; FIPS mode)	✓	✓	✓	✓	✓
Windows Server 2016 (Standard edition; Server with Desktop Experience - previously known as	✓	✓	✓	✓	✓

Endpoint Operating System	Traps 4.2	Traps 5.0	Traps 6.0	Traps 6.1	Cortex XDR 7.0
Server with a GUI)					
Windows Server 2016 Datacenter edition	–	✓ *5.0.4 & later	✓	✓	✓
Windows Server 2019	✓ *4.2.6 & later	–	✓ *6.0.1 & later	✓	✓
Windows Server Core option (Windows Server 2012, 2012 R2, and 2016 only)	✓	✓	✓	✓	✓

Virtual Applications Supported with Cortex XDR and Traps

The following table shows the supported software vendors you can use to deploy virtual applications and the minimum software version supported with each release of the agent.

Product	Traps 4.2	Traps 5.0	Traps 6.0	Traps 6.1	Cortex XDR 7.0
Citrix					
Citrix Virtual Apps and Desktops (previously XenApp and XenDesktop)	7.6 and 7.15	7.15 & later	7.15 & later	7.13 & later	7.13 & later
Citrix App Layering (supports Traps installed on the OS layer)	4	4 & later	4 & later	4 & later *6.1.4 & later according to process detailed below	4 & later *7.0.0 & later read according to process detailed below
VMware					

Product	Traps 4.2	Traps 5.0	Traps 6.0	Traps 6.1	Cortex XDR 7.0
VMware AppVolumes	2.13.1	2.13.1 & later	2.13.1 & later	2.13.1 & later	2.13.1 & later
VMware ThinApp	5.2.2	5.2.2 & later	5.2.2 & later	5.2.2 & later	5.2.2 & later
Windows					
Windows Virtual PC	—	—	—	—	—

* Cirtix App Layering (previously Unidesk) - Due to a Citrix App Layering limitation, you must install the Cortex XDR agent on the OS layer according to this flow to enable the Cortex XDR agent provide full protection to your endpoints:

1. Install the Cortex XDR agent on OS layer during App Layering image preparation process, as a Terminal session, VDI or Standard installation.

   Cortex XDR agent installations on the Application layer or User layer are not supported.

2. Before you finalize the OS layer, stop the Cortex XDR agent with the **`Cytool runtime stop`** command.
3. Delete the **`c:\ProgramData\Cyvera\LocalSystem\Download\content`** folder.
4. Delete the **`c:\ProgramData\Cyvera\LocalSystem\Persistence\cloud_frontend_db`** folder.
5. Add the following entry to the Registry: **`HKLM\SYSTEM\CurrentControlSet\Services\Unirsd \ExcludeKey [REG_SZ] = "\Registry\Machine\System\Cyvera"`**
6. Do not boot up the OS layer before it is finalized.

Cortex XDR and Traps Compatibility with Third-Party Security Products

The Traps agent is now the Cortex XDR agent in Cortex XDR agent release 7.0 and later.

The following tables describe considerations related to third-party security software integration with Cortex XDR and Traps software. This includes security products that are tested and have known limitations or require additional action to integrate with Cortex XDR and Traps agents. Additional third-party apps may be compatible with Cortex XDR and Traps but are not tested and, so, are not included in the list of supported third-party applications.

Third-Party Windows Security Applications

Application Name	Limitations
AppVolumes	On endpoints running Windows 8.1 or a later release, the anti-ransomware malware protection module (MPM) collides with the AppVolumes writeable volume and AppStack features. As a result, running Traps anti-ransomware protection and AppVolumes in parallel is not supported on endpoints running Windows 8.1 or a later release. On endpoints running earlier Windows releases, AppVolumes collides with Traps injection mechanism. To address this limitation, configure AppVolumes to remove Traps registry keys and files that interfere with Traps injection. For more information, see KB-189193.
AVG	If a Cortex XDR or Traps agent component is suspected as a threat, we recommend excluding the component in the AVG management tools.
Avira AV	If a Cortex XDR or Traps agent component is suspected as a threat, we recommend excluding the component in the Avira management tools.
BeyondTrust PowerBroker	Running exploit protection and PowerBroker in parallel is not supported. All other malware protection functionality—such as local analysis, WildFire analysis, and restriction rules—works as expected.
Bitdefender Total Security	Running exploit protection and Bitdefender in parallel is not supported. All other malware protection functionality—such as local analysis,

Application Name	Limitations
	WildFire analysis, and restriction rules—works as expected.
Bufferzone	Not supported.
CylancePROTECT	Not supported.
Digital Guardian	Running exploit protection and Digital Guardian software in parallel is not supported. All other malware protection functionality—such as local analysis, WildFire analysis, and restriction rules—works as expected.
McAfee Solidcore/Solidifier	Running exploit protection and Solidcore/Solidifier in parallel is not supported. All other malware protection functionality—such as local analysis, WildFire analysis, and restriction rules—works as expected.
McAfee VirusScan	Enabling Agent Tampering Protection is not supported on Windows XP or Windows Server 2003 when McAfee VirusScan is installed in parallel.
Microsoft EMET	Running exploit protection and Microsoft EMET in parallel is not supported. All other malware protection functionality—such as local analysis, WildFire analysis, and restriction rules—works as expected.
Panda Antivirus	Running exploit protection and Panda Antivirus in parallel is not supported. All other malware protection functionality—such as local analysis, WildFire analysis, and restriction rules—works as expected.
Sandboxie	Running exploit protection and Sandboxie in parallel is not supported. All other malware protection functionality-such as local analysis, WildFire analysis, and restriction rules-works as expected.
Sophos Intercept	Running exploit protection and Sophos Intercept exploit mitigation features in parallel is not supported. All other malware protection functionality —such as local analysis, WildFire analysis, and restriction rules—works as expected. To enable exploit protection, disable the following **Runtime Protection** options in the server policy of the cloud server for Sophos Intercept: • Mitigate exploits in vulnerable applications • Protect processes

Application Name	Limitations
Trend Micro OfficeScan XG	To prevent Trend Micro OfficeScan XG from detecting malware in the process memory collected by the agent, disable the **Enable program inspection to detect and block compromised executable files** option in Behavior Monitoring Settings of Trend Micro.

Third-Party Mac Security Applications

Application Name	Limitations
Symantec Endpoint Protection (SEP)	Uninstalling or upgrading Traps 6.1 on Mac endpoints with SEP installed is not supported.

Third-Party Linux Security Applications

Application Name	Limitations
SELinux	Because SELinux collides with the agent injection mechanism, injection-based security modules (ROP Mitigation and Brute Force Protection) are disabled when SELinux is enabled. All other exploit and malware protection functionality works as expected. No user action is required.

Traps

You can install the Traps™ 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)?
> Where Can I Install the Traps Agent?
> Traps Compatibility with Third-Party Security Applications

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. You can install the ESM components on dedicated servers or install them on the same server as long as you install them on a supported operating system (OS).

Server Operating System	ESM 4.2
Windows Server 2008 R2	✓
Windows Server 2012	✓
Windows Server 2012 R2	✓
Windows Server 2016	✓
Windows Server 2019	✓ *4.2.6 & later

Where Can I Install the Traps Agent?

The Traps agent is now the Cortex XDR agent in Cortex XDR agent release 7.0 and later. For installation support for both the new Cortex XDR agent and earlier Traps releases, see Where Can I Install the Cortex XDR Agent?.

Traps Compatibility with Third-Party Security Applications

The Traps agent is now the Cortex XDR agent in Cortex XDR agent release 7.0 and later. For compatibility support for both the new Cortex XDR agent and earlier Traps releases, see Where Can I Install the Cortex XDR Agent?.

IPv6 Support by Feature

IPv6 Support by Feature

Use the following table to review PAN-OS® features (listed by category) that support IPv6 traffic.

PAN-OS Feature	PAN-OS 7.1	PAN-OS 8.1	PAN-OS 9.0	PAN-OS 9.1
Security				
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	✓	✓	✓	✓
DoS Rulebase	✓	✓	✓	✓
IPv6 access to PAN-DB	✓	✓	✓	✓
DNS Sinkhole	✓	✓	✓	✓
External Dynamic List (EDL)	✓	✓	✓	✓
Management & Panorama				

PAN-OS Feature	PAN-OS 7.1	PAN-OS 8.1	PAN-OS 9.0	PAN-OS 9.1
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	✓	✓	✓	✓
Reporting and Visibility into IPv6	✓	✓	✓	✓
IPv6 address objects	✓	✓	✓	✓
IPv6 FQDN address objects	✓	✓	✓	✓
Networking				
IPv6 static routes	✓	✓	✓	✓
PBF	✓	✓	✓	✓
PBF next hop monitor (v6 endpoint)	✓	✓	✓	✓

PAN-OS Feature	PAN-OS 7.1	PAN-OS 8.1	PAN-OS 9.0	PAN-OS 9.1
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	✓	✓	✓	✓
Tunnel Content Inspection	–	✓	✓	✓
Virtual wires	✓	✓	✓	✓
NPTv6 (stateless prefix translation)	✓	✓	✓	✓
NAT64 (IP-IPv6 protocol translation)	✓	✓	✓	✓
LLDP (Link Layer Discovery Protocol)	✓	✓	✓	✓
Bidirectional Forwarding Detection (BFD)	✓	✓	✓	✓
VPN				
GlobalProtect™	–	✓	✓	✓
IKE/IPSec	✓	✓	✓	✓
IKEv2	✓	✓	✓	✓
IPv6 over IPv4 IPSec tunnel	✓	✓	✓	✓
Large Scale VPN (LSVPN)	–	✓	✓	✓
Host Dynamic Address Configuration				

PAN-OS Feature	PAN-OS 7.1	PAN-OS 8.1	PAN-OS 9.0	PAN-OS 9.1
DHCPv6 relay	✓	✓	✓	✓
SLAAC (Router Advertisements)	✓	✓	✓	✓
SLAAC (Router Preference)	✓	✓	✓	✓
SLAAC (RDNSS)	–	✓	✓	✓
Device				
High Availability (HA) - Active/Active	✓	✓	✓	✓
High Availability (HA) - Active/Passive	✓	✓	✓	✓
High Availability (HA) - IPv6 transport for HA1 & HA2	✓	✓	✓	✓
High Availability (HA) Path Monitoring (IPv6 Endpoint)	✓	✓	✓	✓
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

Specific Palo Alto Networks firewall models support GTP and SCTP security and 3GPP Technical Standards:

- PAN-OS Releases by Model that Support GTP and SCTP Security
- 3GPP Technical Standard Support

PAN-OS Releases by Model that Support GTP and SCTP Security

The following firewall models support GTP Security and SCTP Security:

Firewall Model	PAN-OS 8.1 (GTP and SCTP)	PAN-OS 9.0 (GTP and SCTP)	PAN-OS 9.1 (GTP and SCTP)
VM-Series	✓	✓	✓
PA-5200 Series	✓	✓	✓
PA-7000 Series firewalls that use the PA-7000-100G-NPC card, and the PA-7050-SMC-B card or PA-7080-SMC-B card, and the PA-7000-LFC-A card (the firewall must use all three cards)*	—	✓	✓

** To verify that your PA-7000 Series firewall is installed with the cards that support GTP and SCTP, use the CLI operational command* ***`show chassis inventory`****. However, cards can be installed but not functional if their dependencies aren't met; refer to the PA-7000 Series Next-Gen Firewall Hardware Reference for installation instructions and the dependencies of each card.*

3GPP Technical Standard Support

GTP security on supported Palo Alto Networks firewalls supports the following releases of the 3GPP Technical Standards:

	Protocol	3GPP TS	3GPP TS Release
PAN-OS 9.0	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	GTPv2-C	29.274	Up to 13.4
	GTPv1-C	29.060	Up to 13.4
	GTP-U	29.281	Up to 13.0
PAN-OS 8.0.7 and Later 8.0 Releases	GTPv2-C	29.274	Up to 13.4
	GTPv1-C	29.060	Up to 13.4
	GTP-U	29.281	Up to 13.0
PAN-OS 8.0.4 to 8.0.6	GTPv2-C	29.274	Up to 11.10
	GTPv1-C	29.060	Up to 11.10
	GTP-U	29.281	Up to 11.6