Prisma SD-WAN Instant-On Network Device Specifications

The Prisma® SD-WAN Instant-On Network (ION) models of hardware and software devices enable the integration of a diverse set of wide area network (WAN) connection types. They deliver exceptional user experience, automate operations, enhance security and compliance, and reduce the overall cost and complexity of your WAN. Built with the intent to transform branch infrastructure, Prisma SASE powers the branch of the future with next-generation SD-WAN.

Enterprises have traditionally implemented rigid and complex solutions with multiple-point solutions, regularly needing to refresh hardware appliances. Traditional architectures hinder the ability to deliver application performance for all applications. They offer only network SLAs and basic caching techniques that fail to optimize performance for dynamic SaaS application content, resulting in a poor user experience and application resiliency. Most importantly, they don't accommodate a zero trust security architecture to protect employees holistically, diversifying apps and rapidly increasing internet of things (IoT) devices. The SD-WAN solution enables this network transformation and removes the limitations of legacy WAN architectures.

SD-WAN requires a networking solution with the capacity to:

- Deliver foundational capabilities for all applications by providing direct-to-app access. It must also ensure application assurance with SLAs and optimization techniques, like forward error correction (FEC), packet duplication, and application acceleration for exceptional user experience.
- Provide integrated and cloud-delivered security services (CDSS) to branch offices. It must have granular security (Layer 7) to enforce true least-privileged access and ensure only the right people can access only the information and assets they need. Plus, it should provide visibility to all your assets, including the rapidly growing IoT devices and AI applications, to ensure organizations can apply the right controls and policies to the entire network.
- Use the latest observability and AI or ML advancements built natively to help organizations automate complex IT and network operations center (NOC) functions with the power of AI or ML to increase productivity and reduce mean time to resolution (MTTR).

Key Benefits

Prisma SD-WAN ION devices offer:

- **End-to-end application performance for exceptional user experience**: Prisma SD-WAN with SASE addresses challenges that organizations face across the last, middle, and first mile. Our innovations address dynamic and transient application and network behaviors across these miles.
- **Improved security outcomes with integrated security**: Prisma SD-WAN enables native discovery of IoT devices and AI applications to apply the right segmentation policies, security policies, and controls to protect branches from all sophisticated threats with Precision AI®.
- **Operational resiliency and simplicity**: Prisma SD-WAN simplifies operations by delivering a unified policy across networking and security. It uses common policy constructs and native integration of Autonomous Digital Experience Management (ADEM) to provide segment-wise insights into application performance. And, it uses Strata Copilot™ so administrators can use natural language processing to run queries.

Prisma SD-WAN Features

Alongside these benefits, your organization can take advantage of the following features.

Application Acceleration

Prisma SD-WAN IONs seamlessly discover and establish robust, optimized path policies to the most optimal App Acceleration nodes in the SASE network. They accelerate the access of these SaaS applications from the branch. This eliminates the need for discrete and bespoke application acceleration and caching solutions. Otherwise, enterprise IT or their ISPs would need to additionally deploy at the branches, reducing capital investments to improve network and application performance.

Strata Copilot

The Strata Copilot for Prisma SD-WAN uses natural language processing that enables administrators to query based on natural language. It provides free-form and curated sets of questions based on the network's health. The copilot makes relevant suggestions, helps perform guided and automated network-centric actions, as well as provides access to product collateral, reducing the need for specialized training.

Application SLA Assurance Framework

The app-defined fabric in Prisma SD-WAN is enhanced with a policy-driven SLA framework to deliver application SLA assurance. It delivers the ability to measure, enforce, and alert, ensuring an exceptional user experience for all apps. With the ability to identify apps and measure SLAs, Prisma SD-WAN enables enforcement such as prioritization, switch flows, and link conditioning, like adaptive FEC. FEC can dynamically turn on or off for a specific application and control the number of recovery packets based on the performance SLAs.

Broadest Support for Network Segmentation

Prisma SD-WAN supports segmentation with network contexts and techniques like virtual routing and forwarding (VRF). It provides the simplicity of defining unique policy rules per segment for the same application using network contexts while supporting overlapping IP addresses with VRF.

SD-WAN with Integrated IoT Security

The industry's first SD-WAN features integrated security for IoT devices. Existing Prisma SD-WAN appliances provide visibility and help secure all IoT devices with Prisma Access. They act as sensors and control points, unlike other SD-WAN solutions that require deploying additional sensors in the network to gain visibility and prevent threats. These sensor and control points enable accurate detection and identification of all IoT devices and security controls from within the familiar cloud management for Prisma SASE.

On-Premises Controller for Prisma SD-WAN

Organizations can meet industry-specific security compliance requirements using the on-premises controller for Prisma SD-WAN. They can deploy Prisma SD-WAN using either the cloud management console or on-premises controller.

Command Center

Through the command center, Prisma SD-WAN provides AI-powered and segment-wise insights and always-on monitoring for network and applications for proactive problem resolution at the branch level. The dashboard on the comprehensive command center enables IT to gain visibility into organization-wide application experience and health, enabling expedited root cause analysis.

Integrated 5G

Prisma SD-WAN has expanded its lightweight appliance portfolio to include the ION 1200, ION 1200-S, and ION 3200H with integrated 5G. With this new appliance, organizations ensure optimal uptime with 5G used as a backup WAN transport for business-critical applications. Businesses with ATMs and kiosks that require cellular as their primary WAN can also deploy this appliance rapidly without the hassle of adding appliances to use 5G.

SD-Branch Capabilities

Prisma SD-WAN SD-branch capabilities extend to the local area network (LAN) with the ION 1200-S and the ION 3200. Integrated switching with Power over Ethernet (PoE) on these appliances fuels end devices—like IP phones and cameras, point-of-sale systems, and wireless access points—without additional switch appliances or power sources. Meanwhile, the built-in fiber optic ports provide flexibility to connect your LAN or WAN to high-speed and long-range fiber optic connections. They also provide power redundancy with a dual supply.

Advanced AIOps Capabilities

The AIOps capabilities in Prisma SD-WAN provide a rich telemetry of network insights, enabling admins to perform granular trend analysis, as well as create unique network conditions to automate tedious manual tasks. AIOps in Prisma SD-WAN can immediately identify a common parent event among all event alarms. Prisma SD-WAN also includes fault analytics capabilities and automated statistical analysis. Besides event correlation and analysis, admins gain greater control over events with automatic prioritization so they can easily pinpoint issues and reduce time to resolution.

Autonomous Digital Experience Management

Prisma SASE with ADEM capabilities extends to both mobile and branch users, enabling organizations to gain end-to-end visibility and segment-wise insights across the entire SASE service delivery path regardless of their users' location. ADEM on Prisma SD-WAN helps ensure the best digital experience for branches by providing observability in the cloud and across multiple WAN paths.

Organizations can use segment-wise insights from synthetic traffic analysis for remote networks to proactively isolate network and application performance issues.

CloudBlades

The CloudBlades platform enables seamless integration of branch services into the SASE fabric without needing to update your branch appliances or controllers, eliminating service disruptions and complexity. This API-based integration of the branch customer-premises equipment (CPE) provides a centralized platform for programming. It also includes an app-flow engine at the CPE, access to Prisma SD-WAN telemetry, and secure authenticated API access to Prisma SD-WAN CPE and systems. As a result, organizations can easily enable the cloud-delivered branch and simplify management and operations.

Zone-Based Firewall

Prisma SD-WAN ION devices include an application-based, zone-based firewall (ZBFW). It's configured using the same top-down, application-centric policies used for performance and path selection, ensuring compliance across different network circuits and interfaces. Our lightweight ZBFW security solution secures the WAN perimeter and segments traffic within a branch site. You can configure ION devices to use on-premises security devices or external, hosted security services to provide further security for remote offices.

Prisma SD-WAN DVR License

With this optional license, you can retain and access up to 90 days of statistics, policy, configuration, alarms, and alerts. Network DVR is licensed per ION device.

Prisma SD-WAN WCR Report License

With the inclusion of this optional license, users gain access to automatically generated and downloadable reports, offering comprehensive insights into different aspects of their Prisma SD-WAN fabric. These reports cover utilization trends and hotspots, empowering customers to make informed decisions about potential circuit upgrades or policy adjustments. Additionally, the license provides advanced AIOps capabilities, delivering actionable insights into the overall health and performance of WAN applications and links. This functionality aids in network planning, problem resolution, and analytics. Instant visibility into application performance enables users to enhance their understanding of network health and usage, facilitating more effective policy decisions.

High Availability

An ION device feature, high availability (HA) is the industry's only deployment model that can survive a device failure and still preserve 100% of WAN capacity at a branch site.

Branch Security Capabilities

The ION devices include intelligence to deliver Layer 7 security, especially for east-west and guest-traffic use cases. These services include:

- **Threat Prevention**: Provides comprehensive threat prevention services, including antispyware and vulnerability protection, to detect and block malicious traffic and attempts to exploit system flaws.
- **DNS Security**: Detects and protects against command-and-control (C2) threats, such as DNS tunneling, through cloud-based DNS request analysis.
- **URL Filtering**: Enables granular monitoring and control over web access by defining policies based on URL categories.

By extending protection through the cloud with Prisma Access as part of the unified Prisma SASE architecture, organizations can achieve a consistent, gap-free, and context-aware security posture across the entire network.

Modes of Operation

The multitenant Prisma SD-WAN cloud management portal enables your team to perform all aspects of configuration, management, and monitoring of ION hardware and software. This feature eliminates the need to individually configure devices at each location, without requiring any additional servers or storage.

Managed through the central cloud controller, ION devices include two modes of operation. In analytics mode, the solution provides end-to-end visibility and analytics of your applications and networks, operating independently of the full suite of Prisma SD-WAN capabilities. ION devices are deployed in the network at the WAN edge and automatically begin examining application data on the network to identify the application and measure several key performance indicators of each session. Statistics from your network are stored securely in the Prisma SD-WAN cloud management portal, which can be used to configure ION devices, define applications and sites, and monitor end-to-end application performance and availability.

In control mode, Prisma SD-WAN builds on the visibility and analytics foundation set by analytics mode and enables the ION devices to begin intelligently taking action based on policy for performance, compliance, and security. Routing functions, including path selection, prioritization, and security, can be integrated into the ION device to reduce the amount of hardware and operational expenses associated with each remote office.

Software Subscriptions

Each Prisma SD-WAN ION branch or data center device requires an accompanying subscription license for operational use. Prisma SD-WAN customers can choose from one of the following licensing models for their branch subscriptions to better align with their deployment needs:

- Per-device subscription (Small/Medium/Large)
- Per-branch site subscription (Small/Medium/Large)
- Aggregate bandwidth subscription (Mbps quantity)

You must purchase a data center subscription for each ION device (physical or virtual) that will be assigned to a data center site.

Hardware Model Specifications

Prisma SD-WAN ION devices come in both hardware and software form factors to meet the needs of any location and deployment scenario. All ION devices are built with FIPS 140-3 as a security baseline. Encryption keys are specific to each customer and device, with high-frequency key rotation occurring at a network level for a large-scale full-mesh, partial-mesh, or hub-and-spoke VPN network.

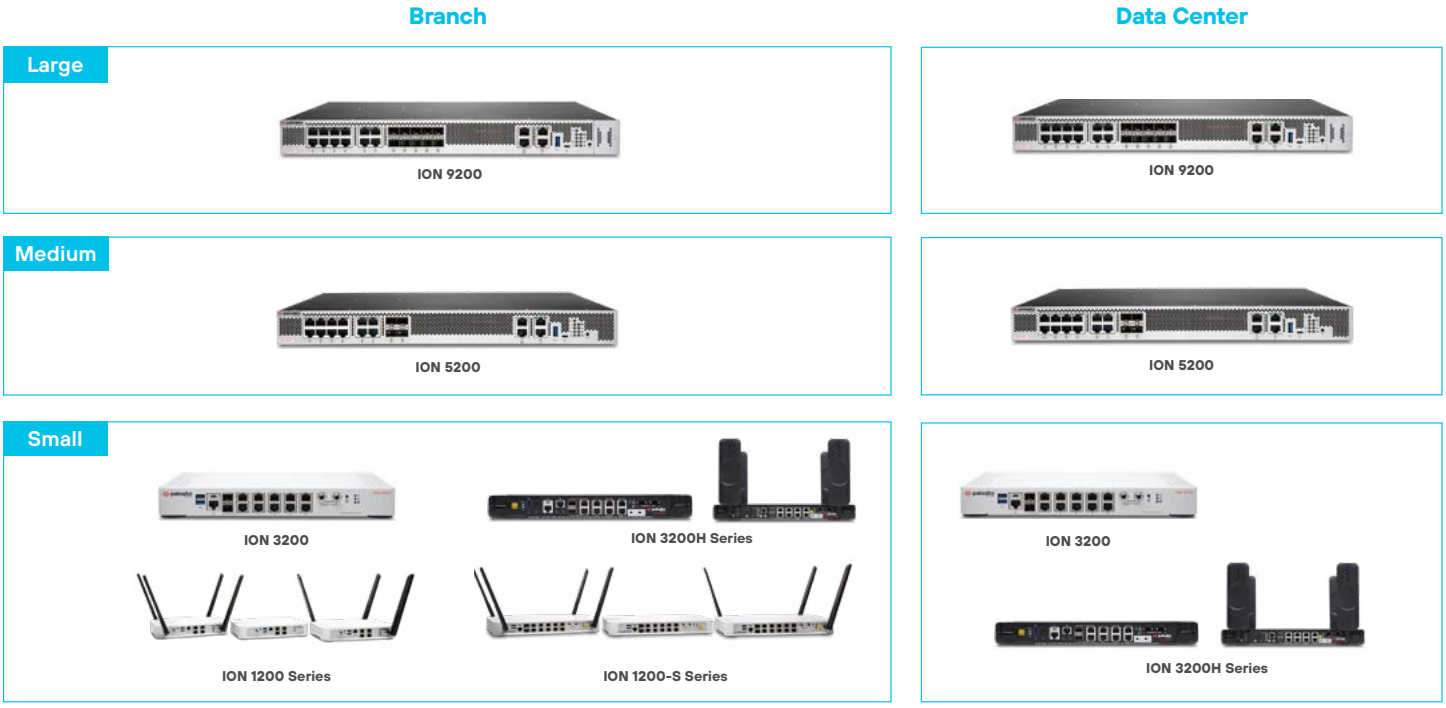

Figure 1. Prisma SD-WAN hardware portfolio

Table 1. Hardware Models

	ION 1200	ION 1200-S	ION 3200	ION 3200H	ION 5200	ION 9200	PA 5440
Use case	Enterprise small branch	Enterprise small branch	Enterprise small branch, data center	Enterprise small branch, data center with temperature hardened appliance (IP40 rating)	Enterprise large branch, data center	Multigigabit remote office data center and large campus	High throughput data center
Controller ports	N/A	N/A	N/A	N/A	N/A	NA	N/A
Console ports	RJ45 (1) console port	RJ45 (1) console port	RJ45 (1) console port	RJ45 (1) console port	RJ45 (1) console port	RJ45 (1) console port	RJ45 (1) console port
WAN/LAN/ Internet ports	10/100/1000 RJ45 (4)	1 GE RJ45 (6), 1 GE RJ45/ SFP Combo ports (2), 1 GE RJ45 bypass ports (2), PoE++ ports (4)	1 GE RJ45 (6), 1 GE RJ45/ SFP Combo ports (2), 1 GE RJ45 bypass ports (2), PoE++ ports (4)	1 GE RJ45 (5), 1 GE RJ45/ SFP Combo ports (2), 1 GE RJ45 bypass ports (2)	10 GE SFP+ (4) 10/100/1000 RJ45 (11) MGIG RJ45 (4 [1G/2.5G]) 1 GE RJ45 bypass ports (4), 802.3 bt PoE++ ports (4)	10 GE SFP+ (10) 10/100/1000 RJ45 (11) MGIG RJ45 (4 [1 G/2.5G/5]) 1 GE RJ45 bypass ports (8), 802.3 bt PoE++ ports (4)	10/100/1000/2500/5000/10000 RJ45 (8) 1/10 GE SFP/SFP+ (12) 40 Gbps/100 Gbps QSFP+/ QSFP28 (4) 10G HA RJ45 (2) 1G MGMT(1)
Cellular support	4G LTE/5G (variants of base product)	4G LTE/5G (variants of base product)	None	5G (variant of base product)	None	None	None
Bypass pairs	N/A	1 pair: Ports 3/4	1 pair: Ports 3/4	1 pair: Ports 3/4	2 pairs: Ports 1–2 and 3–4	4 pairs: Ports 1–2, 3–4, 5–6, and 7–8	N/A
Throughput* (encrypted 1,400 byte packets)	800 Mbps	800 Mbps	1.4 Gbps (DC) 1 Gbps (branch)	1.7 Gbps (DC) 1.3 Gbps (branch)	4 Gbps (DC) 3.2 Gbps (branch)	15 Gbps (DC) 7.5 Gbps (Branch)†	54 Gbps (DC)
Threat prevention (appmix)§	N/A	350 Mbps (Branch)	520 Mbps (Branch)	710 Mbps (Branch)	1.3 Gbps (Branch)	4.5 Gbps (Branch)	70 Gbps (DC)
Flows per second	1K	2K	6K (DC) 3.1K (Branch)	15K (DC) 4.7K (Branch)	16K (DC) 8.5K (Branch)	65K (DC) 20K (Branch)	390K (DC)
Concurrent flows	20K (Branch)	40K (Branch)	100K (DC) 100K (Branch)	100K (DC) 100K (Branch)	100K (DC) 100K (Branch)	1M (DC) 1M (Branch)	20M (DC)
DC VPN scale	N/A	N/A	500‡	2000	2000	5000‡	3000
Power and mechanical	25 W power adapter (noncellular) and 40 W power adaptor (cellular) (AC), 100–240 V, 50–60 Hz, fanless	2 PSU 150 W (AC), 100–240 V, 50–60 Hz, fanless	2 PSU 150 W (AC), 100-240 V, 50–60 Hz, fanless	2 PSU 270 W (AC), 100–240 V, 50–60 Hz, redundant DC, fanless	1+1 redundant PSU 450 W (AC), 100–240 V, 50–60 Hz, fixed fans (4)	1+1 redundant PSU 450 W (AC), 100–240 V, 50–60 Hz, fixed fans (4)	2 load-sharing, hot swappable 1200 W (AC or DC) Input (AC): 100–240 VAC, 50–60 Hz Input (DC): –48 to –60 VDC
Certifications	IEC 62368-1, cTUVus, FCC, CE B, RoHS, TEC	IEC 62368-1, cMETus, FCC, CE B, RoHS, TEC	IEC 62368-1, cMETus, FCC & CE Class A, TEC, KCC	UL 62368-1:2014, CSA C22.2 No. 62368-1:14, IEC/EN 62368-1:2014, IEC 62368-1:2018 FCC Class A, CE Class A, VCCI Class A	IEC 62368-1, cTUVus, FCC & CE Class A, TEC, KCC	IEC 62368-1, cTUVus, FCC & CE Class A, TEC, KCC	IEC 62368-1, cTUVus, FCC & CE Class A, TEC, KCC
Operating temperature	32°F–104°F (0°C–40°C)	32°F–104°F (0°C–40°C) 1200-S-C5G-WW (PoE disabled) operates 32°F–140°F (0°C–60°C)	32°F–104°F (0°C–40°C)	-40°F–158°F (-40°C–70°C) (DC power supply) 32°F–140°F (0°C–60°C) (AC power supply)	32°F–104°F (0°C–40°C)	32°F–104°F (0°C–40°C)	32°F–131°F (0°C–55°C)
Storage temperature	-4°F–158°F (-20°C–70°C)	-4°F–158°F (-20°C–70°C)	-4°F–158°F (-20°C–70°C)	-40°F–158°F (-40°C–70°C)	-4°F–158°F (-20°C–70°C)	-4°F–158°F (-20°C–70°C)	-4°F–15°F (-20°C–70°C)
Operating humidity (noncondensing)	10%–90%	10%–90%	5%–90%	5%–90%	5%–90%	5%–90%	10%–90%
Storage humidity (noncondensing)	10%–90%	10%–90%	5%–95%	5%–90%	5%–95%	5%–95%	10%–90%
MTBF (years)	133 (1200 base) 57 (1200-C) 50 (1200-C5G)	60 (1200-S base) 39 (1200-S-C) 36 (1200-S-C5G)	48	69 (3200H base) 32 (3200H 5G)	12	10	22

Table 1. Hardware Models (continued)							
	ION 1200	ION 1200-S	ION 3200	ION 3200H	ION 5200	ION 9200	PA 5440
Dimensions (LxWxH in inches)	6.42" x 9.53" x 1.73"	9" x 13" x 1.73"	8.88" x 13" x 1.66"	9.38" x 15.35" x 1.74" (ION 3200H) 9.96" x 15.35" x 1.74" (ION 3200H 5G)	14.15" x 17.12" x 1.70"	14.15" x 17.12" x 1.70"	22.5" x 17.34" x 3.44"
Weight	3.75 lbs. (1.7 kg)	7.85 lbs. (3.5 kg)	8.7 lbs. (4 kg)	11 lbs. (5 kg [ION 3200H]) 11.6 lbs. (5.3 kg [ION 3200H 5G])	15.5 lbs. (7 kg)	15.5 lbs. (7 kg)	35 lbs. (15.88 kg)

Notes: (1) WAN and LAN Ethernet ports are suitable for interconnection to other local device Ethernet ports. These ports aren't designed for direct connection to Public Switched Telephone Network (PSTN) ports or interfaces. Also, copper-based WAN ports, LAN ports, and copper-based modular transceivers aren't rated to connect to telecommunications outside plant (OSP) cabling. (2) All IONs have an AUX port, which you can connect at a baud rate of 115,200 for out-of-band management. (3) For more details, see the Key Specifications for Palo Alto Networks Interfaces and Transceivers datasheet.

* Throughput measurements based on the Prisma SD-WAN 6.5.1 release as of February 1, 2025. These numbers are subject to change.

† Performance is measured with 2 VPN tunnels.

‡ DC VPN scale for ION 3000 (end-of-sale product) is 500 and ION 9000 (end-of-sale product) is 5000.

§ Threat Prevention throughput is measured with a best practices profile using SD-WAN appmix transactions and direct internet.

Table 2. Hardware Models with Cellular Support for Remote Offices				
	ION 1200-C-NA ION 1200-S-C-NA	ION 1200-C-ROW ION 1200-S-C-ROW	ION 1200-C5G-WW ION 1200-S-C5G-WW	ION 3200H-C5G-WW
Supported RF bands	**LTE:** B2, B4, B5, B7, B12, B13, B14, B25, B26, B41, B42, B43, B48, B66, B71 **3G:** B2, B4, B5	**LTE:** B1, B3, B7, B8, B20, B28, B32, B38, B40, B41, B42, B43 **3G:** B1, B5, B8	**ION 1200-C5G-WW and ION 1200-S-C5G-WW support:** **5G NR Sub-6 GHz (FR1):** n1, n2, n3, n5, n28, n41, n66, n71, n77, n78, n79 **LTE:** B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B32, B34, B38, B39, B40, B41, B42, B46, B66, B71 **3G:** B1, B2, B4, B5, B6, B8, B9, B19 **Only ION 1200-S-C5G-WW supports:** **5G NR Sub-6 GHz (FR1):** n7, n8, n12, n20, n38, n40 **LTE:** B43	**5G NR Sub-6 GHz (FR1):** n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n38, n40, n41 **LTE:** B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B32, B34, B38, B39, B40, B41, B42, B43, B46, B66, B71 **3G:** B1, B2, B4, B5, B6, B8, B9, B19
Carrier certifications	AT&T, PTCRB, T-Mobile, Verizon, Bell Canada (ION 1200-C-NA)	GCF	AT&T, GCF, PTCRB, T-Mobile, Verizon, and Telstra	AT&T, PTCRB, Verizon, T-Mobile, and GCF In progress: Telstra

Table 3. Software Models					
	For Remote Offices			For Data Centers	
	ION 3102V	ION 3104V	ION 3108V	ION 7108V	ION 7116V
Platforms	ESXi, Hyper-V, KVM	ESXi, Hyper-V, KVM	ESXi, Hyper-V, KVM	ESXi, Hyper-V, KVM, Azure, AWS, Google Cloud	ESXi, Hyper-V, KVM, Azure, AWS, Google Cloud
Throughput	Up to 100 Mbps	Up to 200 Mbps	Up to 350 Mbps	Up to 3 Gbps	Up to 10 Gbps
vCPU	2	4	8	8	16
RAM (GB)	8	8	8	32	64
Disk (GB)	40	40	40	100	100

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

prisma_ds_sdwan-ion-device-specifications_111725