Prisma SASE

The Industry's Most Complete Single-Vendor SASE Solution.

Palo Alto Networks Prisma SASE is the industry's most complete single-vendor secure access service edge (SASE) solution, delivering:

- **Zero Trust Security:** Consistently protect the hybrid workforce with the superior security of ZTNA 2.0.
- **Exceptional Network:** Cloud-native architecture with natively integrated SD-WAN and AutonomousDigital Experience Management ensures the best user experiences.
- **AI-Powered Operations:** Cloud-native architecture with integrated Autonomous Digital Experience Management to ensure the best user experiences.

Key Drivers for SASE Adoption

Three fundamental shifts are driving the need for network transformation in the enterprise: hybrid work, cloud and digital transformation, and branch transformation:

- Supporting the hybrid workforce has become the new normal. Organizations are planning to support a model where the majority of employees can work fluidly between corporate offices, branch offices, home offices, and on the road.
- Cloud and digital initiatives are driving organizations to invest more in SaaS and other public cloud services. Cloud adoption enables companies to be more agile, efficient, and flexible, indicative of why 92% of all enterprises are now adopting a multicloud strategy.[1]
- The branch is back, paving the way to accelerated branch transformation initiatives that support a hybrid workforce and the rapid evolution of applications moving toward the cloud. With 62% of employees preferring hybrid work[2] and significant adoption of collaboration tools like UCaaS for productivity, branch transformation is well underway and is fueling the migration to a single-vendor SASE solution.

Mix-and-Match SASE Solution Challenges

Organizations transitioning to a SASE architecture have two options: multivendor or mix-and-match SASE or a unified, single-vendor approach. Taking a multivendor approach to SASE results in the following challenges:

- Compromised security posture with disparate policies and manual processes.
- Loss of SD-WAN functionality with legacy solutions that lack application awareness, direct-to app connectivity, and end-to-end performance visibility, resulting in operational complexity and adverse effects on security.
- Increased cost and complexity resulting from procuring, deploying, and managing multiple solutions.
- Siloed processes and limited visibility and collaboration across security and networking teams.

Why Single-Vendor SASE Is the Right Approach

As SASE adoption continues to accelerate with the adoption of hybrid work and cloud at scale, organizations need to think about the right approach that will allow them to scale their security and networking infrastructure effectively over time.

1. *2021 State of the Cloud Report*, Flexera, March 9, 2021.
2. Bob Laliberte, *Flexible SD-WAN Consumption Model, ESG,* April 2022.

At Palo Alto Networks, we strongly believe an integrated platform approach to SASE is the right choice for customers. Our solution, Prisma SASE, offers:

- Better security outcomes with unified policy and context sharing.
- Reduced operational complexity through unified management.
- The ability to leverage AI and ML with a unified data lake.

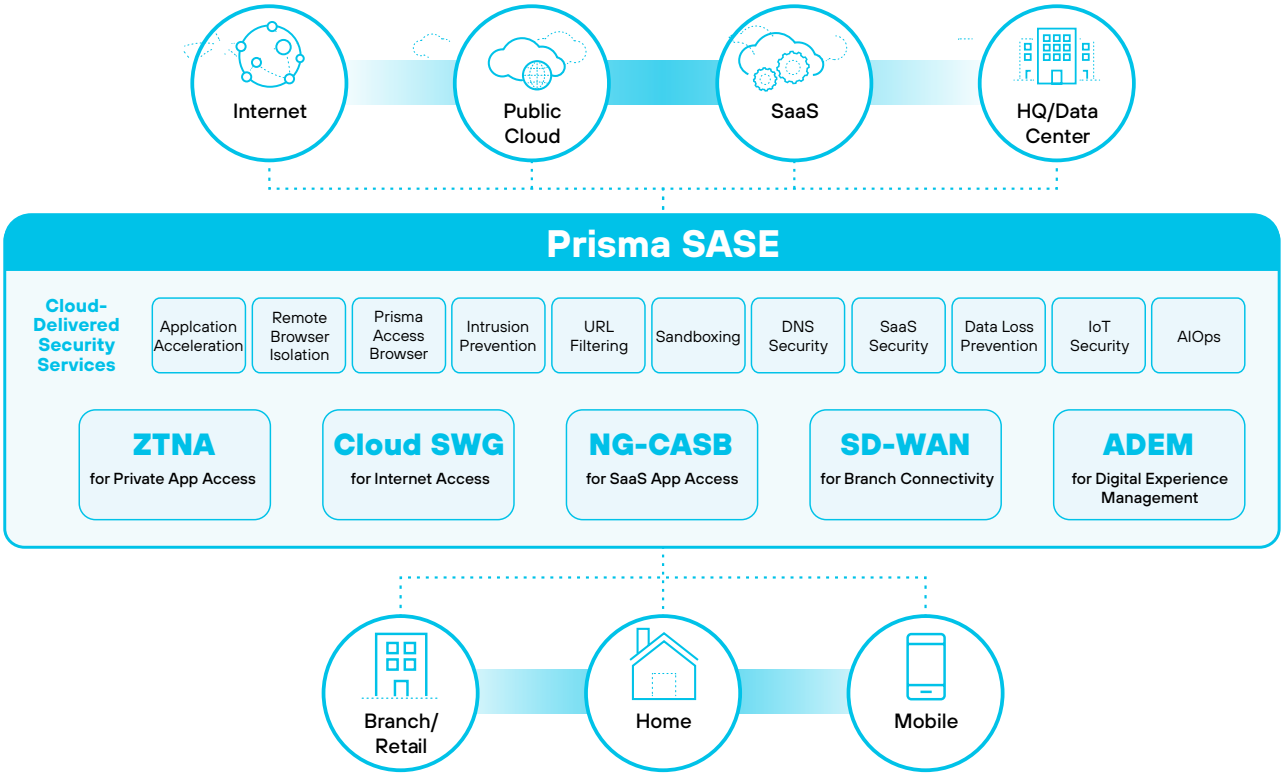

Figure 1: Prisma SASE architecture

Prisma SASE eliminates the limitations of mix-and-match SASE and uniquely delivers ZTNA 2.0, the best user experience, and automation of operations:

- Prisma SASE offers a unified console that allows administrators to manage Prisma Access and Prisma SD-WAN from the same interface. In addition to leveraging the same policy constructs, administrators can now gain visibility into their threat landscape, security alerts, and critical network events within the same management console.
- Leverage a single unified data lake for all data and metrics from Prisma SD-WAN (networking), Prisma Access (security), and ADEM (user experience) that allows it to seamlessly correlate data and cross- reference user and application identification when providing the WAN and security insights. AIOps automation spans all of SASE.
- Prisma SD-WAN provides seamless connectivity and tight integration with Prisma Access, empowering you with the most advanced Layer 7 application-aware SD-WAN fabric. Our solution excels in delivering application SLA-based traffic engineering, ensuring optimal performance and reliability.
- Prisma SASE enables digital experience management for Prisma Access and Prisma SD-WAN to deliver always-on visibility for applications, users, and devices, providing proactive isolation and the troubleshooting and resolution of issues, resulting in reduced operational complexity and costs.
- Consistent security framework using App-ID™, Device-ID™ and User-ID™, resulting in ZTNA 2.0 policy enforcement across the fabric while delivering an exceptional end-user experience. The SASE fabric is a unified network and security fabric with dynamic enforcement of all applications and user policies.

Prisma SASE Features

Prisma SASE delivers a comprehensive list of security, networking, and digital experience services:

Advanced WildFire®: Ensure files are safe by automatically preventing known, unknown, and highly evasive malware 60x faster with the industry's largest threat intelligence and malware prevention engine.

AIOps for SASE: Powerful, natively integrated AIOps capabilities prevent outages and improve security posture with anomaly detection and forecasting, automated troubleshooting, change management modeling, security policy analysis, and more.

App Acceleration: Dynamically adapts to hybrid worker 'first-mile' connectivity conditions to boost connection performance without requiring changes to applications or infrastructure. Leverages an intelligent "App-Aware" edge platform to proactively prepare dynamic content for users, boosting the responsiveness of cloud applications up to 5 times faster than direct-to-Internet.

Autonomous Digital Experience Management (ADEM): Provides segment-wise insights across the entire service delivery path with real and synthetic traffic analysis to drive proactive remediation of digital experience problems.

Cloud access security broker: Complete visibility and control over all SaaS consumption across the enterprise for all users, apps, and locations. Enables access policy, data security, and threat prevention through a combination of both inline and API-based SaaS controls.

CloudBlades: Enables the seamless integration of branch services into the SASE fabric without needing to update branch appliances or controllers, thus eliminating service disruptions, complexity and enabling organizations to simplify network operations and multicloud connectivity and expedite deployments.

Cloud secure web gateway (SWG): Secures against web-based threats using static analysis and machine learning while simplifying the onboarding experience for customers migrating from legacy proxy-based solutions to SASE.

Data loss prevention: Comprehensive data protection that keeps sensitive data safe by classifying and protecting it while at rest and in motion across SaaS apps, networks, and public clouds.

DNS Security: Comprehensive ML-based protection from dozens of attacks and abuse of the DNS protocol that attackers use to covertly control malware and exfiltrate data.

Explicit proxy: Prisma SASE offers flexible connectivity options, including support for explicit proxy connection methods. With Prisma SASE explicit proxy, customers can easily migrate from legacy proxy-based solutions without the need for network architecture changes, facilitating an easy transition to a more secure solution that protects all apps, ports, and protocols.

Firewall as a service (FWaaS): Protects remote locations with Palo Alto Networks Next-Generation Firewall security, delivered as a service from the cloud.

High availability (HA): Prisma SD-WAN ION devices feature the industry's only HA deployment model that can survive a device failure and still preserve 100% of WAN capacity at a branch site.

Integrated 5G: Lightweight appliance portfolio to ensure optimal uptime with 5G leveraged as active and LTE as backup WAN transport for business-critical applications.

IoT Security: Combines machine learning, risk assessment, inline prevention, policy recommendations, and automated policy enforcement to secure IoT devices without the need to deploy costly and difficult-to-manage sensors.

Prisma Access Browser: Secures both managed and unmanaged devices, addressing the evolving security demands of modern organizations and their hybrid workforces. By extending SASE's protective reach to any device in minutes, Prisma Access Browser safeguards business applications and data against a spectrum of threats.

Remote Browser Isolation: Creates a secure isolation channel between users and remote browsers to keep malicious files and zero-day web threats from executing on user machines, leveraging the latest vector and pixel-based technologies to deliver superior isolation with a near-native user experience. Also supports integration with third-party RBI clouds through CloudBlades.

SaaS Security Posture Management (SSPM): Ensures enterprise SaaS apps are securely configured and hardened against attack by continuously evaluating SaaS configurations against security best practices that align thousands of app-specific settings and features to a security framework that an InfoSec operator can easily understand and manage.

SD-branch: Integrated switching with universal Power over Ethernet (uPoE) on SD-WAN appliances powers end devices like IP phones and cameras, point-of-sale systems, and wireless access points without additional switch appliances or power sources.

SD-WAN: Ensure application availability based on real-time application performance SLAs and visibility, simplify tedious network operations, and natively apply best-in-class cloud-delivered security with Prisma Access integration.

SD-WAN Bandwidth On-Demand: Allocate bandwidth seamlessly across branches based on consumption from an aggregate pool to improve application performance and bandwidth availability.

Threat Prevention: Blocks exploits, malware, and command-and-control traffic using industry-first inline deep learning that can stop unknown command-and-control and zero-day exploits.

Managed and Unmanaged Device Access Support: IPsec, SSL, and clientless VPN provide options for connecting users and networks to the secure access service edge.

Zero Trust Network Access (ZTNA) 2.0: Combines fine-grained, least-privileged access with behavior-based continuous trust verification and deep, ongoing security inspection and enterprise DLP to consistently protect all users, devices, apps, and data everywhere.

Table 1: Prisma Access Details, Features, and Specifications			
	Prisma Access for Networks	**Prisma Access for Users**	**Prisma Access for Clean Pipe**
Locatio	140+ locations in 87 countries	• 140+ locations in 87 countries (GlobalProtect)	17 locations
Connection Type	IPsec tunnel	• GlobalProtect app IPsec/SSL • GlobalProtect Clientless VPN • Explicit proxy	Peering via Partner Interconnect (VLAN attachment per tenant)
GlobalProtect® App Platform Support	n/a	• Apple iOS • Apple macOS • Google Android • Android App for Chromebook • CentOS Linux • Red Hat Enterprise Linux • Ubuntu • Windows 10 and UWP IoT Platforms • Raspberry Pi OS • Windows IoT Enterprise • Ubuntu • Google Android	n/a
Service-Level Agreements			
Uptime Availability	99.999% per calendar month		
Connectivity	99.99% for 10 ms over a 1-hour period		

For more details, view the Prisma Access datasheet.

Table 2: Hardware Models									
	ION 1000	**ION 1200**	**ION 1200-S**	**ION 2000**	**ION 3000**	**ION 3200**	**ION 5200**	**ION 9000**	**ION 9200**
Use Case	Small remote office	Enterprise small branch	Enterprise small branch	Enterprise small branch	Enterprise small branch, data center	Enterprise small branch, data center	Enterprise large branch, data center	Multigigabit remote office data center and large campus	Multigigabit remote office data center and large campus
WAN/LAN/Internet Ports	10/100/1000 RJ45 (4)	10/100/1000 RJ45 (4)	1 GE RJ45 (6), 1 GE RJ-45/SFP Combo ports (2), 1 GE RJ-45 bypass ports (2), POE++ ports (4)	10/100/1000 RJ45 (5	10/100/1000 RJ45 (up to 12)	1 GE RJ45 (6), 1 GE RJ-45/SFP Combo ports(2), 1 GE RJ-45 bypass ports (2), POE++ ports(4)	10 GE SFP+ (4) 10/100/1000 RJ45 (11) MGIG RJ45 (4) 1 GE RJ-45 bypass ports (4), POE++ ports (4)	10 GE SFP+ (8) 10/100/1000 RJ45 (8)	10 GE SFP+ (10) 10/100/1000 RJ45 (11) MGIG RJ45 (4) 1 GE RJ-45 bypass ports (8), POE++ ports (4)
Cellular Support	None	4G LTE/5G	4G LTE/5G	None	None	None	None	None	None
Throughput* (Encrypted 1400 byte packets)	250 Mbps	700 Mbps	700 Mbps	700 Mbps	1.5 Gbps (DC) 1 Gbps (Branch)	1.5 Gbps (DC) 1 Gbps (Branch)	4 Gbps (DC) 2 Gbps (Branch)	15 Gbps (DC) 8 Gbps (Branch)	15 Gbps (DC) 8 Gbps (Branch)
Throughput* (Encrypted 600 byte packets)	100 Mbps	250 Mbps	250 Mbps	250 Mbps	600 Mbps (DC) 500 Mbps (Branch)	600 Mbps (DC) 500 Mbps (Branch)	1.5 Gbps (DC) 1 Gbps(Branch)	6 Gbps (DC) 3 Gbps (Branch)	6 Gbps (DC) 3 Gbps (Branch)

* Throughputmeasurements are based on Prisma SD-WAN 6.0.2 release as of August 31, 2022. These numbers aresubject to change

For more details, view the Prisma SD-WAN datasheet.

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_Prisma SASE_04.09.24