Prisma Access

Global expansion, mobile workforces, and cloud computing are changing the ways organizations implement and deploy applications. Get the protection you need, where you need it, with Prisma™ Access. Prisma Access delivers a secure access service edge (SASE) that provides globally distributed networking and security to all your users and applications.

Whether at branch offices or on the go, your users connect to Prisma Access to safely access cloud and data center applications as well as the internet.

What Makes Prisma Access Different?

Prisma Access is designed to prevent successful cyberattacks, and that's why it does more than just secure the web. To stop cyberattacks, it's necessary to inspect all traffic. Anything short of full inspection of all traffic introduces a significant gap in security.

Prisma Access consistently protects all traffic, on all ports and from all applications, enabling your organization to:

- **Prevent successful cyberattacks** with proven security philosophies and threat intelligence for deep visibility and precise control that extends across your organization.
- **Fully inspect all application traffic** bidirectionally—including SSL/TLS-encrypted traffic—on all ports, whether communicating with the internet, with the cloud, or between branches.
- **Benefit from comprehensive threat intelligence** powered by automated threat data from Palo Alto Networks and hundreds of third-party feeds.

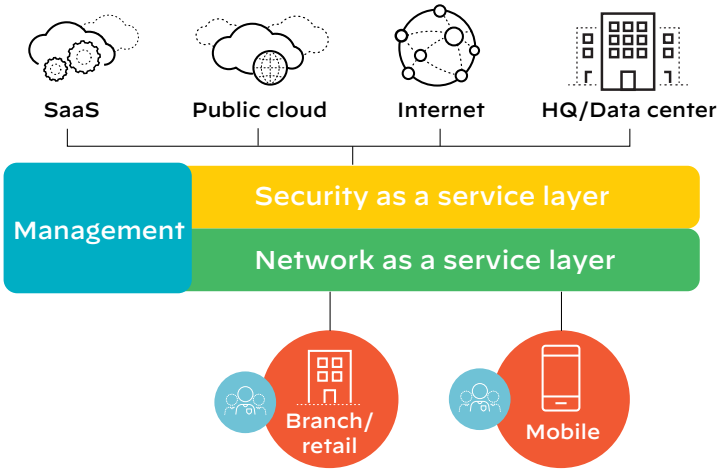

Figure 1: Prisma Access architecture

Network as a Service Layer

Prisma Access provides consistent, secure access to all applications—in the cloud, in your data center, or on the internet.

Table 1: Secure Application Access Everywhere

	Branch office	HQ/ Regional HQ	Public cloud	Private cloud/data center	SaaS	Web	Internet
Remote network	✓	✓	✓	✓	✓	✓	✓
Mobile user	✓	✓	✓	✓	✓	✓	✓

Networking for Remote Networks

Connect branch offices to Prisma Access over a standard IPsec VPN tunnel using common IPsec-compatible devices, such as your existing branch router, SD-WAN edge device, or a third-party firewall. You can use Border Gateway Protocol (BGP) or static routes for routing from the branch, and you can use equal cost multi-path (ECMP) routing for faster performance and better redundancy across multiple links.

Networking for Mobile Users

Connect mobile users with the GlobalProtect™ app, which supports user-based always-on, pre-logon always-on, and on-demand connections. Use an always-on full tunnel for optimal security. Prisma Access supports split tunneling based on access route, applications, per-app VPN split tunneling, and split tunneling based on low-risk/high-bandwidth applications, such as streaming video.

Bandwidth Management

Enable application allow listing and blocking policies with App-ID™ technology to free up the network from unnecessary, bandwidth-hogging applications. Prioritize and shape the traffic handled by Prisma Access using quality of service (QoS) policies.

Logging

Prisma Access lets you take advantage of automated, centralized, cloud-scalable log storage, allowing you to centralize your management and reporting as well as forward logs to your syslog server and/or security information and event management (SIEM) system.

Security as a Service Layer

Firewall as a Service

Prisma Access provides firewall as a service (FWaaS) that protects branch offices from threats while also providing the security services expected from a next-generation firewall. The full spectrum of FWaaS includes threat prevention, URL filtering, sandboxing, and more.

DNS Security

Prisma Access delivers our DNS Security service, which provides a combination of predictive analytics, machine learning, and automation to combat threats in DNS traffic. Organizations can block known malicious domains, predict new malicious domains, and stop DNS tunneling.

Threat Prevention

Using Prisma Access for threat prevention combines the proven technologies in the Palo Alto Networks platform, together with global sources of threat intelligence and automation, to stop previously known or unknown attacks.

Cloud Secure Web Gateway

Prisma Access for secure web gateway (SWG) functionality is designed to maintain visibility into all types of traffic while stopping evasions that can mask threats. Our web filtering capabilities also drive our credential theft prevention technology, which can stop corporate credentials from being sent to previously unknown sites.

Data Loss Prevention

Prisma Access combines integration with inline data loss prevention (DLP) controls and with API-driven DLP in corporate cloud applications (the latter through Prisma SaaS). Through this enterprise DLP service, Prisma Access provides consistent discovery and protection of sensitive data everywhere, across networks, clouds, and users. It helps prevent data breaches and enhance data privacy and compliance.

Zero Trust Network Access

ZTNA authenticates and connects users to applications based on granular, role-based access control and provides a single pane of glass to create and enforce policies. Prisma Access also supports both agent-based and agentless connection methods to provide secure remote access regardless of a user's location. Unlike standalone VPN or proxy solutions, Prisma Access performs single-pass traffic inspection for malware, data loss, and malicious behavior after users connect.

Management

Prisma Access supports two management options:

- **Panorama™ network security management** for centralized administration across Palo Alto Networks Next-Generation Firewalls and Prisma Access.
- **Cloud management** through a web-based interface with preconfigured profiles and streamlined workflows, using the Prisma Access app in the hub.

Table 2: Prisma Access Details, Features, and Specifications

	Prisma Access for Networks	Prisma Access for Users	Prisma Access for Clean Pipe
Use cases	• Branch offices/retail • Virtual private clouds • Palo Alto Networks SD-WAN hub • Third-party SD-WAN security	• Mobile users with: » Laptops » Smartphones » Tablets • Zero Trust network access	• Service provider/telco multitenant environments • Security of traffic outbound to the internet
Licensing			
Basis	Mbps	Users	Mbps
	Based on bandwidth pool; each connection can be assigned up to 300 Mbps (500 Mbps and 1 Gbps currently available in preview)	Based on total number of unique users	Based on bandwidth pool; can be divided up to 10 Gbps per tenant
Minimum deployment size	Bandwidth pool of 200 Mbps	200 users	100 Mbps per tenant
Service Tunnels			
Baseline service tunnels	Up to three service tunnels included		N/A
Additional service tunnels	Additional service tunnels (up to a total of 100) can be created by allocating 300 Mbps of the bandwidth pool per additional tunnel		N/A

Table 2: Prisma Access Details, Features, and Specifications (continued)			
Connectivity			
Locations	100+ in 76 countries		17 locations
Connection type	IPsec tunnel SD-WAN (PAN-OS 9.1 or later)	GlobalProtect app IPsec/SSL	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	N/A
IoT Platforms		Rasbian Windows IoT Enterprise Ubuntu Google Android	
Management			
Panorama	• License for Panorama required • No license for Prisma Access Panorama plugin • Prisma Access does not count against the Panorama device license		
Cloud management	No license required for Prisma Access app on the hub		
Security			
URL Filtering	Included		
Threat Prevention	Included		
WildFire	Included		
Host information profile	Included		
DNS Security	Included		
Data Loss Prevention	Subscription required		
Cortex XDR	Subscription required		
Prisma SaaS	Subscription required		
AutoFocus	Subscription required		
Logging			
Cortex Data Lake	Prisma Access requires Cortex Data Lake for logging (subscription required)		

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