Prisma Access

The way we work has changed. Remote workforces and work from anywhere are now the norms, requiring infrastructure and services that are essential for employee productivity to be available and secure 24/7. Modernize your infrastructure with Prisma® Access to seamlessly extend consistent, centralized, and best-in-class security controls to every user and location.

Prisma Access transforms networking and security to deliver the industry's most comprehensive cloud native secure access service edge (SASE) so organizations can easily support the dynamic needs of their digital workforces.

The Prisma Access Difference

Prisma Access is designed from the ground up to enable organizations to lower the costs and complexities of securely connecting users and devices to any service required, anywhere. The cloud native architecture of Prisma Access ensures on-demand and elastic scale of comprehensive networking and security services across a global, high-performance network. With Prisma Access, organizations can easily modernize their infrastructure with a true SASE approach that delivers:

- **The most complete cloud-edge architecture**, consolidating more networking and security capabilities into a single cloud-delivered service.
- **Best-in-class protection** that reduces risk by delivering a consistent posture across all users and locations, with industry-leading cybersecurity.
- **Full bidirectional inspection of all traffic**, including TLS-/SSL-encrypted traffic, on all ports.
- **Comprehensive threat intelligence** powered by automated threat data from Palo Alto Networks and hundreds of third-party feeds.

Security-as-a-Service Layer

Firewall as a Service

Prisma Access provides firewall-as-a-service (FWaaS) capabilities with the full functionality of a Palo Alto Networks Next-Generation Firewalls (NGFWs). This includes inbound and outbound protection, native user authentication and access control, and Layer 3–7 single-pass inspection to secure branch offices against threats.

Cloud Secure Web Gateway

Prisma Access provides secure web gateway (SWG) functionality for remote users across all web traffic protocols and applications in hybrid environments. Prisma Access also provides URL and content filtering for users based on dynamic group monitoring, allowing you to implement granular behavior-based policies. Advanced DNS security prevents command-and-control (C2) callback and DNS tunneling attacks.

Zero Trust Network Access

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 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.

Cloud Access Security Broker

With the optional addition of Prisma SaaS, Prisma Access implements security controls that combine inline API security and contextual controls to determine access to sensitive information. These controls are implemented together in an integrated manner and applied throughout all cloud application policies.

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.

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. 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 services.

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 or software-defined wide area network (SD-WAN) appliance. You can use Border Gateway Protocol (BGP) or static routing from the branch, and you can use equal-cost multipath (ECMP) routing for faster performance and better redundancy across multiple links.

Deployment Visibility—Prisma Access Insights

Prisma Access Insights is a comprehensive network monitoring app in Prisma Access. It provides on-demand insight into service and deployment health, plus proactive assistance capabilities, such as real-time alerts.

Management

Prisma Access supports two management options:

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

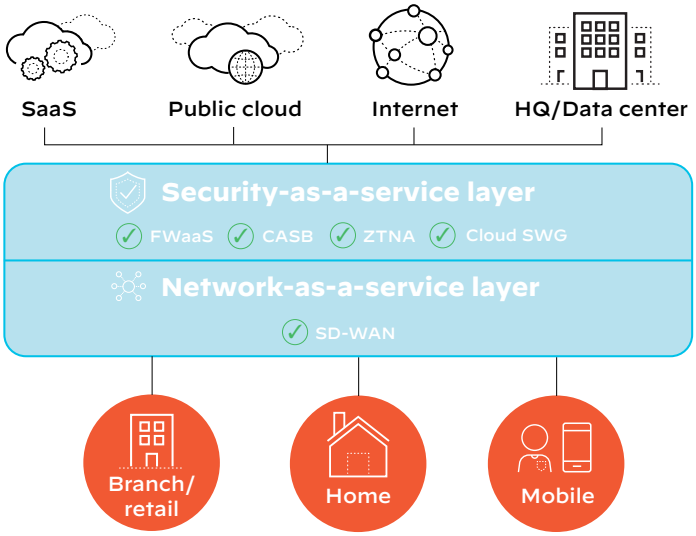

Figure 1: Prisma Access architecture

Table 1: Prisma Access Details, Features, and Specifications			
	Prisma Access for Networks	**Prisma Access for Users**	**Prisma Access for Clean Pipe**
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		Raspberry Pi OS Windows IoT Enterprise Ubuntu Google Android	
Service-Level Agreements			
Uptime Availability	99.999% per calendar month		
Connectivity*	99.99% for 10 ms over a 1-hour period		
Feature	**Description**		
App-ID	Continuously classifies all applications regardless of port, SSL/SSH encryption, or technique used by an attacker to evade detection. Unlike legacy solutions that depend on Layers 3 and 4 as the first layers of control before application classification is applied, Prisma Access applies App-ID along with other Layer 7 controls, such as User-ID.		
User-ID	Integrates with a wide range of user identity repositories so that your policies follow your users and groups regardless of their location. User repositories include wireless LAN controllers, VPNs, directory servers, browser-based captive portals, proxies, and more.		
SSL Decryption	Inspects and applies policy to SSL/SSH-encrypted traffic, both inbound and outbound, including for traffic that uses HTTP/2. For privacy and regulatory compliance, you can enable or disable decryption flexibly based on URL, source, destination, user, user group, and port.		
Reporting	Includes, as a standard, a detailed, customizable software-as-a-service (SaaS) application usage report that provides insight into all SaaS traffic—sanctioned and unsanctioned—on your network. You can also create custom reports based on your needs as well as easily schedule, download, and share them with others in your organization.		
User Authentication	Supports all existing PAN-OS authentication methods, including Kerberos, RADIUS, SAML, LDAP, client certificates, and a local user database. Once GlobalProtect authenticates the user, it immediately provides Prisma Access with a user-to-IP address mapping for use by User-ID technology.		
DNS Security	Automatically prevents C2 callback and tunneling to tens of millions of malicious domains identified with real-time analysis and continuously growing global threat intelligence. You can predict and stop malicious domains from domain generation algorithm-based malware with instant enforcement.		
URL Filtering	Protects users by automatically preventing web-based attacks, including those that use phishing, C2, and exploit kits. Phishing and JavaScript-based attacks are detected inline and blocked in milliseconds without requiring analyst intervention. You can address any compliance or regulatory issues by controlling web access based on organizational policy.		
Data Loss Prevention (DLP)	Includes a set of tools and processes that allow you to protect sensitive information against unauthorized access, misuse, extraction, or sharing. DLP on Prisma Access enables you to enforce data security policies and prevent the loss of sensitive data across mobile users and remote networks.		
Dynamic User Group (DUG) Monitoring	Provides dynamic security actions based on user behavior to restrict suspicious or malicious users. Allows you to define DUGs in Prisma Access to take time-bound security actions without waiting for changes to be applied to user directories.		
Host Information Profile (HIP)	Checks the endpoint to get an inventory of how it's configured and builds a HIP. Prisma Access uses the HIP to enforce application policies that only permit access when the endpoint is properly configured and secured.		

* Regional differences may apply. For more details, refer to the Prisma Access Service-Level Agreement.

Table 1: Prisma Access Details, Features, and Specifications (continued)	
Feature	**Description**
Site-to-Site IPsec VPN	Supports site-to-site tunnels over IPv4 and IKEv1/IKEv2 to ensure compatibility. For multiple connection sites, ECMP routing can provide additional redundancy and cost efficiency by balancing sessions over available internet connections.
Logging	Shows overall traffic, application, user, threat, URL, and data filter logging to facilitate organization of data via the cloud-based Cortex Data Lake.
Policy Automation	Enables you to use information from third-party sources to drive security policy updates dynamically through a combination of Dynamic Address Groups (DAGs) and the XML API.
Intrusion Prevention System (IPS)	Blocks vulnerability exploits, buffer overflows, and port scans. Additional capabilities, like blocking invalid or malformed packets, IP defragmentation, and TCP reassembly, protect you from attackers' evasion and obfuscation methods. Vulnerability-based signatures are continuously updated from the WildFire malware prevention service. Custom signatures can also be manually imported, including from popular formats like Snort and Suricata.
Anti-Malware	Uses a stream-based engine that blocks inline at very high speeds, detecting known malware as well as unknown variations of known malware families. IPS and anti-malware address multiple threat vectors with one license, eliminating the need to buy and maintain separate IPS and proxy-based products from legacy security vendors.
C2 Protection	Stops malicious outbound communications stemming from malware infections, passively analyzes DNS queries, and identifies the unique patterns of botnets. This reveals infected users and prevents secondary downloads and data from leaving your organization.
Unknown Threat Detection with Advanced Analysis	Identifies unknown threats with shared data from the industry's largest enterprise malware analysis community, including threats submitted from networks, endpoints, clouds, and third-party partners. Leveraging our custom-built hypervisor with bare metal analysis, WildFire uses various complementary analysis engines that can detect sandbox-evading attacks.
Protection from Unknown Threats	Automatically generates protections across the attack lifecycle when a new threat is first discovered—blocking malicious files, access to malicious URLs, and C2 traffic—and then delivers those protections to all WildFire subscribers in seconds for most new threats.
File Behavior Analysis	Uses detailed behavior analysis to help you to understand how newly discovered malware operates. Integrated logs enable you to quickly identify infected users and investigate potential breaches with detailed analysis of, and visibility into, unknown threat events.
Cloud-Based Prevention	Employs a unique cloud-based, modular architecture, providing automatic prevention based on global threat intelligence without the headache of having to implement and manage separate devices for web and email at every ingress/egress point in your network.
Multi-Vector Analysis and Visibility	Combines the cloud scale of WildFire with advanced file analysis and URL crawling to deliver Multi-Vector Recursive Analysis, a unique and comprehensive solution that prevents multi-stage, multi-hop attacks. Unlike other solutions, WildFire can follow multiple stages of attack even if execution fails in a given stage. When WildFire visits embedded links or links in emails as part of its email link analysis, it updates URL Filtering if any corresponding webpages host exploits or display phishing activity.
Comprehensive File Execution	Executes unknown files in multiple OS and application versions simultaneously to fully understand the scope of a threat. Multi-version analysis ensures WildFire analysis is thorough, unlike sandboxes that require golden images, which could deem a malicious file benign simply because the target OS or application version wasn't specified in the golden image.

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