Prisma Access

Digital transformation, cloud adoption, and remote work have eroded physical perimeters. With applications and data stored everywhere, organizations need a scalable way of securing remote access for every user and branch location. Modernize your infrastructure with Palo Alto Networks Prisma® Access to seamlessly extend consistent, centralized, best-in-class security controls to every user and location.

Prisma Access consolidates all of the networking and security capabilities organizations need into a single cloud-delivered platform, transforming network security and allowing organizations to enable flexible remote workforces. It provides complete security for all application traffic while ensuring an exceptional user experience.

The Prisma Access Difference

Prisma Access is designed from the ground up 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. Prisma Access provides the foundation for consistent cloud-delivered security for all users and locations, including:

- **Superior protection for all applications and data** by securing remote access to all privileged data across web- and non-web-based traffic, reducing the risk of data breaches.
- **Complete best-in-class security** with industry-leading capabilities converged into a single cloud-delivered platform, providing more security coverage than any other solution.
- **Optimized user experience** built on a massively scalable network with ultra-low latency and backed by industry-leading SLAs, ensuring the best digital experience for end users.

When combined with CloudGenix® SD-WAN, Prisma Access transforms networking and security with the most complete secure access service edge (SASE) solution in the industry.

Security-as-a-Service Layer

Prisma Access includes comprehensive security capabilities consolidated into a single service edge.

Firewall as a Service

Prisma Access provides firewall-as-a-service (FWaaS) capabilities with the full functionality of 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 cloud secure web gateway (SWG) functionality for remote users across all web traffic protocols and applications in hybrid environments. It also provides URL and content filtering for users based on dynamic group monitoring, allowing you to implement granular behavior-based policies. Integrated proxying gives users maximum flexibility for how they connect to the Prisma Access service. 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 (RBAC) and provides a single pane of glass to create and enforce policies. Prisma Access supports both agent-based and agentless connection methods 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

Prisma Access natively provides inline visibility and control of software-as-a-service (SaaS) applications. With the addition of Prisma SaaS, API-based security and contextual controls can be introduced for sanctioned SaaS applications. 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 and the type of application, including its associated risk and bandwidth utilization.

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.

Digital Experience Monitoring

The Autonomous Digital Experience Management (ADEM) add-on for Prisma Access provides native end-to-end visibility for SASE. With ADEM, you gain segment-wise insights across the entire service delivery path, with real and synthetic traffic analysis that enables autonomous remediation of digital experience problems when they arise. The complementary Prisma Access Insights lets you monitor and get on-demand visibility into the health of your Prisma Access deployment.

Centralized Management

Prisma Access supports two management options:

- **Panorama™ network security management** for centralized policy management across all Palo Alto Networks Next Generation Firewalls and Prisma Access. Panorama saves time and reduces complexity by managing network security through a single pane of glass.
- **Prisma Access Cloud Management** to streamline Prisma Access configuration management with seamless onboarding, continuous assessment of security posture, digital experience monitoring, and reporting through a unified experience delivered from the cloud.

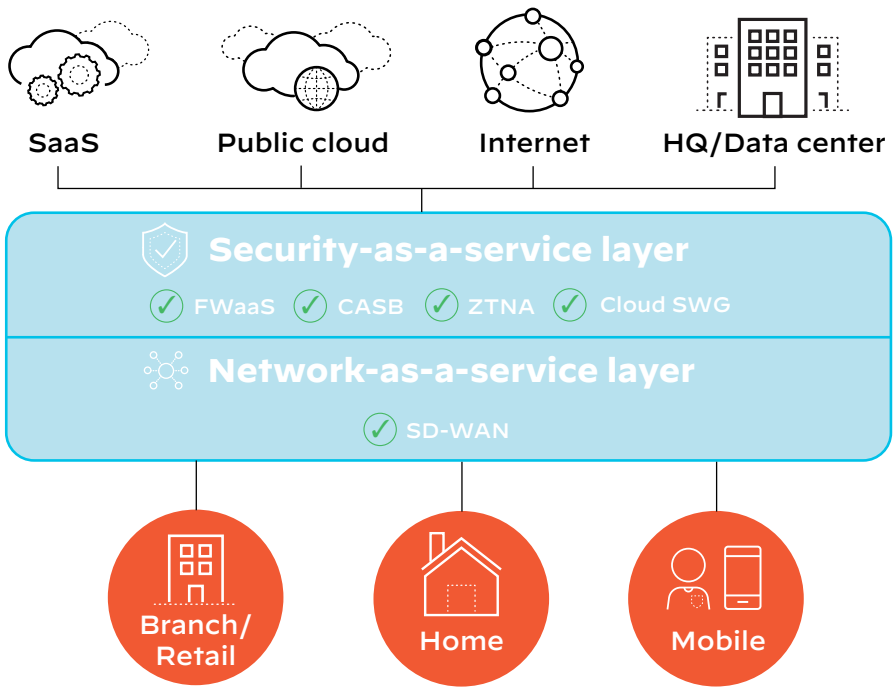

Figure 1: Prisma Access architecture

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	100+ in 76 countries (GlobalProtect) 25 locations (explicit proxy)	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		

Table 2: Prisma Access Features	
Feature	**Description**
App-ID	Continuously classifies all applications regardless of port, TLS/SSL 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.
Device-ID*	Allows policies to be created that follow a device no matter where in the network it is connected. Enforcement based on device attributes such as operating system version enables security teams to control the attack surface more strictly. Device-ID logging provides additional visibility as well as context and, combined with App-ID and User-ID, allows for deep insights into behavior on the network.
SSL Decryption	Inspects and applies policy to TLS/SSL-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.
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.
AI/ML-Based Detection	Delivers inline, signatureless attack detection and zero-day exploit prevention. Prisma Access adapts and provides instantaneous real-time protection vs. scheduled updates. It prevents up to 95% of unknown threats instantly, with less than 10-second signature delivery, resulting in a 99.5% reduction in infected systems.
IoT Security*	Combines machine learning with our leading App-ID technology and crowdsourced telemetry to profile all devices for discovery, risk assessment, vulnerability analysis, anomaly detection, and trust-based policy recommendations. It prevents known and unknown IoT, IoMT, and OT threats and delivers native enforcement with a Palo Alto Networks ML-Powered NGFW or via orchestration with third parties.
Explicit Proxy	Allows customers to choose proxy mode where the client (browser) is configured to use a proxy server. This explicit proxy option is an alternate way for mobile users to connect to Prisma Access and secure their internet and SaaS application traffic (HTTP/HTTPS). PAC files are supported for browser configuration.
PAN-OS Policy Optimizer	Provides a simple workflow to migrate your legacy port-based rule base to an App-ID rule base. This reduces your attack surface and increases the efficacy of your security policies.
Remote Browser Isolation Support	Integrates, through CloudBlades, with third-party RBI clouds by leveraging existing NGFW URL categorization and URL rewrite features to forward select/all internet bound traffic to the RBI cloud. This capability provides a seamless user experience while forwarding certain traffic (unknown or high-risk categories) to RBI for additional inspection; the remaining traffic can be inspected by Prisma Access and egress directly to the internet.
Reporting	Includes, as a standard, a detailed, customizable 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.
Digital Experience Monitoring*	Offers visibility into user experience as well as application and network performance with the Autonomous Digital Experience Management (ADEM) add-on. ADEM provides segment-wise insights across the entire service delivery path, with real and synthetic traffic analysis that enables the ability to drive autonomous remediation of digital experience problems when they arise.
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.

Table 2: Prisma Access Features (continued)	
Feature	**Description**
Device Quarantine	Blocks compromised devices from accessing privileged data. You can either manually or automatically add compromised devices to a quarantine list and block users from logging into the network from those devices using GlobalProtect. You can also restrict access to applications from these compromised devices.
Quality of Service (QoS)	Enables you to dependably run high-priority applications and traffic under limited network capacity. QoS prioritizes business-critical traffic or traffic that requires low latency, such as VoIP or videoconferencing. You can also reserve a minimum amount of bandwidth for business-critical applications.
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, such as 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.

* Requires an add-on license.

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

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