GlobalProtect

GlobalProtect Extends Consistent and Best-in-Class Protection to All of Your Remote Users, Regardless of Their Location

The world you need to secure continues to expand as users and applications shift to locations outside the traditional network perimeter. Security teams face challenges with maintaining visibility into network traffic and enforcing security policies to stop threats. Traditional technologies used to protect mobile endpoints, such as host endpoint antivirus software and remote access virtual private networks (VPNs), can't stop the advanced techniques employed by today's sophisticated attackers.

GlobalProtect® enables you to protect your mobile workforce by extending the consistent protections of Palo Alto Networks Next-Generation Firewalls and Prisma® Access to all users, regardless of location. It secures traffic by applying the platform's capabilities to understand application use, associate the traffic with users and devices, and enforce security policies with next-generation technologies.

Table 1: Key Usage Scenarios and Benefits

Capability	Description
Secure Remote Access	• Provide secure access to internal and cloud-based business applications.
Advanced Threat Prevention	• Prevent known and unknown command-and-control (C2) traffic. • Block known and unknown command injection and SQL injection exploits. • Inspect and classify network traffic while blocking malware and vulnerability exploits in a single pass. • Prevent lateral movement and quarantine compromised devices.
Advanced URL Filtering	• Take control of your web traffic and automate security actions based on users, risk ratings, and content categories. • Block access to known and unknown malicious sites. • Industry-leading phishing protections that combat the latest evasion techniques used by attackers. • Secure access to web-based SaaS applications.
Bring-Your-Own-Device Policies	• Support app-level VPN for user privacy. • Enable secure, clientless access for partners, business associates, and contractors. • Support automated identification of unmanaged devices. • Support customized authentication mechanisms for managed and unmanaged devices.
Zero Trust Implementation	• Deliver continuous trust verification and security inspection. • Consistent policy enforcement for all users, regardless of their location. • Enforce step-up multifactor authentication to access sensitive resources.

Implementing Zero Trust

Zero Trust for Your Remote Users

GlobalProtect, along with the rest of Palo Alto Networks security services, safeguards your mobile workforce by inspecting all network traffic in real time, with Cloud-Delivered Security Services powered by Precision AI™. Whether your users are remote, hybrid, or in HQ, these services work together to protect all users, apps, devices, and data, stopping known and unknown threats, including phishing, ransomware, command and control, malware, DNS-layer attacks, and much more. Laptops, smartphones, and tablets with the GlobalProtect app automatically establish a secure IPsec/TLS/Tunnel connection, including proxy mode, to Prisma Access or a Next-Generation Firewall using the best gateway, thus providing full visibility of all network traffic, applications, ports, and protocols. By eliminating the blind spots in mobile workforce traffic, your organization can maintain a comprehensive view into all network traffic.

Zero Trust for Your Network

Not all users need access to all assets inside your corporate network. Security teams are adopting Zero Trust principles to segment their networks and enforce precise controls for access to internal resources. GlobalProtect provides the fastest, most authoritative user identification for the platform, enabling you to write precise policies that allow or restrict access based on business need. Furthermore, GlobalProtect provides host information that establishes device compliance criteria associated with security policies. These measures allow you to take preventive steps to secure your internal networks, adopt Zero Trust network controls, and reduce the risk of attack. When GlobalProtect is deployed in this manner, the internal network gateways may be configured with or without a VPN tunnel.

Additionally, GlobalProtect enables you to quarantine compromised devices by utilizing an endpoint's immutable characteristics. This will allow administrators to restrict network access as well as prevent the compromised endpoint from infecting other users and devices. Quarantine restrictions can apply whether the compromised device is external or on the internal network.

Inspection of Traffic and Enforcement of Security Policies

GlobalProtect enables security teams to build policies that are consistently enforced, whether the user is internal or remote. Security teams can prevent successful cyberattacks by bringing all the platform's capabilities to bear:

- **App-ID™** technology identifies application traffic, regardless of port number, and enables organizations to establish policies to manage application usage based on users and devices.
- **User-ID™** technology identifies users and group memberships for visibility as well as the enforcement of role-based network security policies.
- **SSL Decryption** inspects and controls applications that are encrypted with SSL/TLS/SSH traffic and stops threats within the encrypted traffic.
- **Advanced Threat Prevention** stops known and unknown exploits, malware, spyware, and command-and-control (C2) threats with the industry's first prevention of zero-day attacks, stopping 60% more zero-day injection attacks and 48% more highly evasive command-and-control traffic than traditional IPS solutions.
- **Advanced WildFire®** ensures safe access to files with the industry's largest malware prevention engine, stopping up to 22% more unknown malware and turning detection into prevention 180X faster than competitors.
- **Advanced URL Filtering** ensures safe access to the web and prevents 40% more threats in real time than traditional filtering databases with the industry's first prevention of known and unknown phishing attacks, stopping up to 88% of malicious URLs at least 48 hours before competitors.
- **Advanced DNS Security** protects your DNS traffic and stops advanced DNS-layer threats, including DNS hijacking, all in real time with 2X more DNS-layer threat coverage than competitors.
- **Next-Generation CASB** discovers and controls all SaaS consumption in your network, with visibility into 60K+ SaaS apps and protects your data with 28+ API integrations.
- **IoT/OT Security** secures your blind spots and protects every connected device unique to your vertical with the industry's most comprehensive Zero Trust solution for IoT devices, discovering 90% of devices within 48 hours.
- **AI Access Security™** enables the safe use of GenAI apps with real-time visibility of over 800 GenAI apps, access control, and data protection.

Secure Access Control

User Authentication

GlobalProtect supports all existing PAN-OS® authentication methods, including Kerberos, RADIUS, LDAP, SAML 2.0, client certificates, biometric sign-in, and a local user database. Once GlobalProtect authenticates the user, it immediately provides Prisma Access or a Next-Generation Firewall with a user-to-IP-address mapping for User-ID.

Strong Authentication Options

GlobalProtect supports a range of third-party multifactor authentication (MFA) methods, including one-time password tokens, certificates, and smart cards, through RADIUS and SAML integration.

These options help organizations strengthen the proof of identity for access to internal data center or software-as-a-service (SaaS) applications.

GlobalProtect has options to make strong authentication even easier to use and deploy:

- **Cookie-based authentication**: After authentication, you may choose to use an encrypted cookie for subsequent access to a portal or gateway for the lifetime of that cookie.
- **Simplified certificate enrollment protocol support**: GlobalProtect can automate the interaction with an enterprise public key infrastructure (PKI) for managing, issuing, and distributing certificates to GlobalProtect clients.
- **MFA**: Before a user can access an application, they can be required to present an additional form of authentication.

Host Information Profile

GlobalProtect checks the endpoint to get an inventory of how it's configured and builds a host information profile (HIP) that's shared with Prisma Access and Next-Generation Firewalls. They use the HIP to enforce application policies that only permit access when the endpoint is properly configured and secured. These principles help enforce compliance with policies that govern the amount of access a given user should have with a particular device.

HIP policies can be based on a number of attributes, including:

- Managed/Unmanaged device identification
- Machine certificates present on device
- Device information received from mobile device manager
- Operating system and application patch level
- Host antimalware version and state
- Host firewall version and state
- Disk encryption configuration
- Data backup product configuration
- Customized host conditions (e.g., registry entries, running software)

Control Access to Applications and Data

Security teams can establish policies based on application, user, content, and host information to maintain granular control over access to a given application. These policies may be associated with specific users or groups defined in a directory to ensure that organizations provide the correct levels of access based on business need. The security team can further establish policies for step-up MFA to provide additional proof of identity before accessing particularly sensitive resources and applications.

Enhanced Monitoring and Visibility with Strata Cloud Manager

Integration within Palo Alto Networks Zero Trust management and operations solution, Strata™ Cloud Manager, provides continuous, real-time monitoring and insights into those using GlobalProtect, allowing you to optimize the health and experience of your remote users. Additionally, Strata Cloud Manager offers one-click, centralized troubleshooting so you can quickly remediate your user connection issues.

Secure Browser and Devices

The effects of hybrid work, bring-your-own-device (BYOD) policies, and our heavy reliance on doing work within the browser are changing the number of use case permutations that security teams need to support. It's necessary to provide application access to all users, whether they're employees or contractors, who can use a wide range of devices (e.g., mobile, managed, unmanaged). Integration with mobile device management (MDM) offerings, such as Workspace ONE and Ivanti, can help you deploy GlobalProtect as well as provide additional security measures through the exchange of intelligence and host configuration. Using these with GlobalProtect, your organization can maintain visibility and the enforcement of security policy on a per-app basis while maintaining data separation from personal activities to honor the user's expectations of privacy in BYOD scenarios.

GlobalProtect supports clientless SSL VPN for secure access to applications in the data center and the cloud from unmanaged devices. This approach allows customers to enable secure access for third-party users and employees connecting from BYOD devices. It does this by providing access to specific applications through a web interface, both without requiring users to install a client and without setting up a VPN tunnel.

Additionally, customers can benefit from enterprise-grade browser security. With the native integration of Prisma Access Browser, you can effortlessly onboard contractors and third parties in minutes and securely enable BYOD policies, empowering your workforce with device choice without compromising security. Prisma Access Browser allows you to implement security directly in the browser, where users and data interact, giving you advanced data loss prevention capabilities, enhanced privacy, and improved cost efficiency.

Architecture Matters

As part of Palo Alto Networks unified network security platform, GlobalProtect is natively integrated within the various form factors, including NGFW and Prisma SASE, to best support you wherever you are in your cloud transformation journey. When securing your remote users with our unified network, Palo Alto Networks network security platform offers:

- **Unified agent**:
  - Deliver secure, seamless, and optimized access to all apps (e.g., internet, SaaS, and private) and data for users, while enforcing robust security policies.
  - Secure all apps, both web and nonweb, and take dynamic actions such as quarantining the endpoints, restricting overprivileged access to apps, and much more.
  - Use the same agent to provide ADEM, with the benefit of improved UX.
- **Unified management**:
  - Get a single pane of glass into your entire network through Strata Cloud Manager.
  - Experience real-time visibility and monitoring (plus configurations and configuration management) across NGFW and SASE deployments.
  - Gain contextual insights for all applications, users, and devices.
- **Multiple form factors**:
  - Choose from NGFW for on-premises, Prisma Access for SASE, or a combination of the two for hybrid environments, depending on your deployment.
  - Receive best-in-class protection with Cloud-Delivered Security Services powered by Precision AI.

Cloud-Based Gateways

Workforces shift from one location to another, creating changes in traffic load. This is especially true when considering how companies evolve, whether on a temporary basis (e.g., following a natural disaster) or a permanent one (e.g., when entering new markets).

Prisma Access by Palo Alto Networks provides a comanaged option for deploying coverage in the locations organizations need, using your security policies. It can be used with your existing firewalls, making your architecture adaptable to changing conditions.

Prisma Access supports autoscaling, which dynamically allocates new firewalls based on load and demand in a given region.

Table 2: GlobalProtect Features

Category	Specification
Tunnel Mode	IPsec
	SSL
	Proxy
	Clientless VPN
	Per App VPN on Android, iOS
Gateway Selection	Automatic selection
	Preferred gateway selection
	External gateway selection by source location
	Internal gateway selection by source IP
Connection Methods	User login (always on)
	On demand
	Pre-logon (always on)
	Pre-logon, then on demand
	User-initiated pre-logon
Connection Mode	Internal mode
	External mode
Layer 3 Protocols	IPv4
	IPv6
Single Sign-On	SSO (Windows credential provider)
	Kerberos SSO
	SSO for macOS
Split Tunneling	Include routes, domains, applications
	Exclude routes, domains, applications
Authentication Methods	SAML 2.0
	LDAP
	Client certificates
	Kerberos
	RADIUS
	Two-factor authentication
	Authentication method selection based on operating system or device ownership

Table 2: GlobalProtect Features (continued)	
Category	**Specification**
HIP Reporting, Policy Enforcement, and Notifications	Patch management
	Host antispyware
	Host antimalware
	Host firewall
	Disk encryption
	Disk backup
	Data loss prevention
	Customized HIP conditions (e.g., registry entries, running software)
Managed Device Identification	By machine certificates
	By hardware serial number
Multifactor Authentication	At connect time and resource access time
MDM/EMM Integration	Workspace ONE
	Ivanti
	Microsoft Intune
Strata Cloud Manager	Palo Alto Networks Next-Generation Firewalls, including physical and virtual appliances
	Prisma Access
	Panorama® network security management
GlobalProtect App Supported Platforms	Microsoft Windows and Windows UWP
	Apple macOS
	Apple iOS and iPadOS
	Google Chrome OS
	Android OS
	Linux OS (Red Hat, CentOS, Ubuntu)
	IoT devices
IPsec X-Auth	Apple iOS IPsec client
	Android OS IPsec client
	Third-party VPN and strongSwan client
GlobalProtect App Localization	Chinese, English, French, German, Japanese, Spanish
Other Features	User-ID
	IPsec to SSL VPN fallback
	Enforce GlobalProtect connection for network access
	Tunnel configuration based on user location
	HIP report redistribution
	Certificate checks in HIP
	SCEP-based automatic user certificate management
	Script actions that run before and after sessions
	Dynamic GlobalProtect app customization
	App configuration based on users, groups, and/or operating systems
	Automatic internal/external detection

Table 2: GlobalProtect Features (continued)	
Category	**Specification**
Other Features	Manual/automatic upgrade of GlobalProtect app
	Certificate selection by OID
	Blocking of access by lost, stolen, or unknown devices
	Smart card support for connection/disconnection
	Transparent distribution of trusted root CAs for SSL decryption
	Disabling of direct access to local networks
	Customizable welcome and help pages
	RDP connection to a remote client
	Operating system-native notifications
	User sign out restriction
	Proxy support
	Enforcement of GlobalProtect exclusions
	Connection with SSL only
	RSA software token integration
	Device quarantine

Conclusion

Palo Alto Networks next-generation cybersecurity plays a critical role in preventing breaches. Use GlobalProtect to extend the protection of the platform to users wherever they go. By using GlobalProtect, you can get consistent enforcement of security policy so that even when users leave the building, their protection from cyberattacks remains in place.

Resources

- Prisma Access webpage
- Prisma Access Browser webpage

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_globalprotect_121024