GlobalProtect

GlobalProtect extends the protection of the Palo Alto Networks Next-Generation Firewall to the members of your mobile workforce, no matter where they go.

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), cannot stop the advanced techniques employed by today's sophisticated attackers.

GlobalProtect™ network security for endpoints enables you to protect your mobile workforce by extending the Palo Alto Networks Next-Generation Firewall 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.

Key Usage Scenarios and Benefits

Remote Access VPN

- Provides secure access to internal and cloud-based business applications.

Advanced Threat Prevention

- Secures internet traffic.
- Stops threats from reaching the endpoint.
- Protects against phishing and credential theft.
- Quarantines compromised devices by leveraging immutable characteristics.

URL Filtering

- Enforces acceptable use policies.
- Filters access to malicious domains and adult content.
- Prevents the use of avoidance and evasion tools.
- Secures access to SaaS applications.
- Controls access and enforces policies for SaaS applications while blocking unsanctioned applications.

Bring-Your-Own-Device Policies

- Supports app-level VPN for user privacy.
- Enables secure, clientless access for partners, business associates, and contractors.
- Supports automated identification of unmanaged devices.
- Supports customized authentication mechanisms for managed and unmanaged devices.

Zero Trust Implementation

- Delivers reliable user identification.
- Delivers immediate and accurate host information for visibility and policy enforcement.
- Enforces step-up multi-factor authentication to access sensitive resources.

Extending the Platform Protection Externally

GlobalProtect safeguards your mobile workforce by inspecting all traffic using your Next-Generation Firewalls deployed as internet gateways, whether at the perimeter, in the Demilitarized Zone (DMZ), or in the cloud. Laptops, smartphones, and tablets with the GlobalProtect app automatically establish a secure IPsec/SSL VPN connection to the 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 consistent view into applications.

Implementing Zero Trust in 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.

In addition, 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 of 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.
- **WildFire® malware prevention service** automates the analysis of content to identify new, previously unknown, and highly targeted malware by its behavior and generates the threat intelligence to stop it in near-real time.

- **Threat Prevention** for IPS and antivirus blocks network-based exploits targeting vulnerable applications and operating systems, denial-of-service (DoS) attacks, and port scans. Antivirus profiles stop malware and spyware from reaching the endpoint using a stream-based engine.
- **URL Filtering with PAN-DB** categorizes URLs based on their content at the domain, file, and page level, and receives updates from WildFire so that when web content changes, so do categorizations.
- **File blocking** stops the transfer of unwanted and dangerous files while further scrutinizing allowed files with WildFire.
- **Data filtering** enables administrators to implement policies that can be used to stop the unauthorized movement of data, such as the transfer of customer information or other confidential content.

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 the Next-Generation Firewall with a user-to-IP-address mapping for User-ID.

Strong Authentication Options

GlobalProtect supports a range of third-party multi-factor 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, he or she 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 the Next-Generation Firewall. The Next-Generation Firewall uses 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 anti-malware 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 Troubleshooting and Visibility

GlobalProtect Application Command Center (ACC) widgets, reports, and the new GlobalProtect log provide full visibility into GlobalProtect usage in your deployment. Detailed logging of the connection workflow in stages greatly simplifies troubleshooting of user connection issues. This logging allows administrators to easily identify the stage/event in the connection process where a given user has an issue.

Secure and Enabled BYOD

The effects of bring-your-own-device (BYOD) policies are changing the number of use case permutations that security teams need to support. It is necessary to provide application access to a broader spectrum of employees and contractors using a wide range of mobile devices.

Integration with mobile device management offerings, such as AirWatch® and MobileIron®, can help you deploy GlobalProtect as well as provide additional security measures through the exchange of intelligence and host configuration. Using these in conjunction 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 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.

Architecture Matters

The flexible architecture for GlobalProtect provides many capabilities that can help you solve an array of security challenges. At the most basic level, you can use GlobalProtect as a replacement for the traditional VPN gateway, eliminating the complexity and headaches of administering a standalone, third-party VPN gateway.

Options for manual connections and gateway selection enable you to tailor the configuration to support business requirements as needed.

In a more comprehensive deployment for securing traffic, GlobalProtect can be deployed with an always-on VPN connection with a full tunnel, ensuring that protection is always present and transparent to the user experience. Exceptions can be defined for latency-sensitive traffic by application, domain names and routes, or video traffic.

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 co-managed option for deploying coverage in the locations organizations need, using your security policies. It can be used in conjunction with your existing firewalls, making your architecture adaptable to changing conditions.

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

Conclusion

The Palo Alto Networks Next-Generation Firewall 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.

Table 1: GlobalProtect Features

Category	Specification
VPN Connection	IPsec
	SSL
	Clientless VPN
	Per-app VPN on Android, iOS
Gateway Selection	Automatic selection
	Manual selection
	Preferred gateway selection
	External gateway selection by source location
	Internal gateway selection by source IP
Connection Methods	User logon (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

Table 1: GlobalProtect Features (continued)	
Authentication Methods	SAML 2.0
	LDAP
	Client certificates
	Kerberos
	RADIUS
	Two-factor authentication
	Authentication method selection based on operating system or device ownership
HIP Reporting, Policy Enforcement, and Notifications	Patch management
	Host anti-spyware
	Host anti-malware
	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
MFA	At connect time and resource access time
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
	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

Table 1: GlobalProtect Features (continued)	
MDM/EMM Integration	AirWatch
	MobileIron
	Microsoft Intune
Management Tools and APIs	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 XAuth	Apple iOS IPsec client
	Android OS IPsec client
	Third-party VPNC and strongSwan client
GlobalProtect App Localization	Chinese, English, French, German, Japanese, Spanish

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