GLOBALPROTECT

Prevent Breaches and Secure the Mobile Workforce

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

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

URL Filtering

- Enforces acceptable use policies
- Filters access to malicious domains and adult content
- Prevents the use of avoidance and evasion tools

Secure Access to SaaS Applications

- Controls access and enforces policies for SaaS applications while blocking unsanctioned applications

BYOD

- Supports app-level VPN for user privacy
- Enables secure clientless access for partners, business associates and contractors

Strengthens Internal Network Segmentation

- 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

The world you need to secure continues to expand as both 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 VPN, are not capable of stopping the advanced techniques employed by today's more sophisticated attackers.

Palo Alto Networks® GlobalProtect™ network security client for endpoints enables organizations to protect the mobile workforce by extending the Next-Generation Security Platform 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.

Extending the Platform Protection Externally

GlobalProtect safeguards the mobile workforce by inspecting all traffic using the organization's next-generation firewalls that are deployed as internet gateways, whether at the perimeter, in the DMZ or in the cloud. Laptops, smartphones and tablets with the GlobalProtect app automatically establish a secure SSL/IPsec VPN connection to the next-generation firewall with the best performance for a given location, thus providing the organization with full visibility of all network traffic, applications, ports and protocols. By eliminating the blind spots in mobile workforce traffic, the organization maintains a consistent view into applications.

Securing the Network Internally

Not all users need access to every corner of the corporate network. Security teams are adopting network segmentation to partition their network and enforce precise controls for access to internal resources. GlobalProtect provides the fastest, most authoritative user identification for the platform, enabling organizations to write precise policies that allow or restrict access based on business need. Furthermore, GlobalProtect provides host information that establishes device criteria associated with security policies. These measures allow organizations to take preventive steps to secure their internal networks, adopt Zero Trust network controls and reduce the attack surface area.

When GlobalProtect is deployed in this manner, the internal network gateways may be configured for use with or without a VPN tunnel.

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 apply all of the platform's capabilities for cyberattack prevention, including:

- **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.
- **Decryption –** Inspects and controls applications that are encrypted with SSL/TLS/SSH traffic. Stops threats within the encrypted traffic.
- **WildFire™ cloud-based threat analysis 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 –** Intrusion prevention blocks network-based exploits targeting vulnerable applications and operating systems, 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 –** 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.

Customized Host Conditions (e.g., Identifying Users and Devices)

User Authentication

GlobalProtect supports all of the existing PAN-OS® authentication methods, including Kerberos, RADIUS, LDAP, SAML 2.0, client certificates 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 methods, including one-time password tokens, certificates and smart cards, through RADIUS integration.

These options help organizations strengthen the proof of identity for access to internal data center or SaaS applications.

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

- **Cookie-based authentication:** After authentication, an organization 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 PKI for managing, issuing and distributing certificates to GlobalProtect clients.

Host Information Profile

GlobalProtect checks the endpoint to get an inventory of how it's configured and builds a host information profile that's shared with the next-generation firewall. The next-generation firewall uses the host information profile 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.

Host information profile policies can be based on a number of attributes, including:

- 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, multi-factor authentication in order to provide additional proof of identity before accessing particularly sensitive resources and applications.

Secure and Enabled BYOD

The effects of BYOD are changing the number of use case permutations that security teams need to support. It is necessary to provide access to applications to a broader spectrum of employees and contractors using a wide range of mobile devices.

Integration with mobile device management solutions, such as AirWatch® and MobileIron®, help organizations deploy GlobalProtect as well as provide additional security measures through the exchange of intelligence and host configuration. When used in conjunction with GlobalProtect, the

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 offers convenience and security by providing access to specific applications through a web interface without requiring the user to install a client beforehand or set up a full tunnel.

Architecture Matters

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

Options for manual connections and gateway selection enable organizations 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.

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 (such as a natural disaster in a region) or a permanent one (such as entering new markets).

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

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

Conclusion

The protections provided by Palo Alto Networks Next-Generation Security Platform play a critical role in preventing breaches. Use GlobalProtect to extend the protection of the platform to users wherever they go. By using GlobalProtect, organizations can get consistent enforcement of security policy so that even when users leave the building, their protection from cyberattacks remains in place.

GlobalProtect Features

Category	Specification
VPN Connection	IPsec
	SSL
	Clientless VPN
	Per-app VPN on Android™, iOS, Windows® 10
Gateway Selection	Automatic selection
	Manual selection
	External gateway selection by source location
	Internal gateway selection by source IP
Connection Methods	User login (always-on)
	On-demand
	Pre-login (always-on)
	Pre-login, then on-demand
Connection Mode	Internal mode
	External mode
Layer 3 Protocols	IPv4
	IPv6
Single Sign-On	SSO (Windows credential provider)
	Kerberos SSO

Category	Specification
Split-Tunneling	Include routes
	Exclude routes
Authentication Methods	SAML 2.0
	LDAP
	Client certificates
	Kerberos
	RADIUS
	Two-factor authentication
Host Information Profile Reporting, Policy Enforcement and Notifications	Patch management
	Host anti-spyware
	Host antivirus
	Host firewall
	Disk encryption
	Disk backup
	Data loss prevention
	Customized host information profile conditions (e.g., registry entries, running software)
Multi-Factor Authentication	Advanced authentication for sensitive resource access
Other Features	User-ID
	IPsec to SSL VPN fallback
	Enforce GlobalProtect connection for network access
	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
	Block access from lost or stolen and unknown devices
	Smart card support for connection/disconnection
	Transparent distribution of trusted root CAs for SSL decryption
	Disable direct access to local networks
	Customizable welcome and help pages
	RDP connection to a remote client

Category	Specification
MDM/EMM Integration	AirWatch
	MobileIron
Management Tools and APIs	Palo Alto Networks Next-Generation Security Platform, including physical (such as the PA-7000 Series, the PA-3000 Series and the PA-200) and virtual (VM-Series) form factors
	Microsoft InTune®
	GlobalProtect cloud service
GlobalProtect App Supported Platforms	Microsoft® Windows and Windows UWP
	Apple® Mac® OS X®
	Apple iOS
	Google® Chrome® OS
	Android® OS
	Linux® supported using third-party VPNC and StrongSwan client
IPsec Xauth	Apple iOS IPsec client
	Android OS IPsec client
GlobalProtect App Localization	English
	Spanish
	German
	French
	Japanese
	Chinese

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

globalprotect-ds-082817