GLOBALPROTECT CLOUD SERVICE

All your users, whether at branch offices or on the go, connect to GlobalProtect cloud service to safely access cloud and data center applications as well as the internet.

Global expansion, mobile workforces, and cloud computing are changing the ways organizations implement and deploy applications. You can get the protection you need, where you need it, with Palo Alto Networks GlobalProtect™ cloud service. A generational step forward in cloud-delivered security, it uses a global distributed architecture to connect all your users and applications while delivering the full protection of the Palo Alto Networks Security Operating Platform.

Key Use Cases

- Address global expansion and mobile workforce security.
- Provides security for direct-to-internet and SD-WAN projects.
- Secure Multiprotocol Label Switching (MPLS) transition strategies.
- Rapidly deploy consistent security following a recent merger or acquisition.
- Deploy as a managed security offering for MSSPs.

Key Capabilities

- Bring network security to branch offices without on-premises security hardware.
- Protect your entire mobile workforces in any location.

What Makes GlobalProtect Cloud Service Different?

GlobalProtect cloud service is designed to prevent successful cyber-attacks, so it does more than just secure the web. The web is not the only source of risk, and it's essential to inspect all traffic. Anything short of full inspection of all traffic is missing the big picture.

GlobalProtect cloud service protects all traffic, on all ports and from all applications, in a consistent manner. This means you can:

- Prevent successful cyberattacks with the same proven security philosophies and shared threat intelligence as an on-premises Palo Alto Networks Security Operating Platform deployment for deep visibility and precise control that extends across your organization.
- Fully inspect all application traffic bidirectionally—including SSL/TLS-encrypted traffic—on all ports, whether communicating with the internet, the cloud, or between branches.
- Take advantage of flexible deployment models to choose the best option for your requirements and network design. You use GlobalProtect cloud service in conjunction with physical or virtualized Palo Alto Networks next-generation firewalls.
- Benefit from comprehensive threat intelligence powered by automated threat data from Palo Alto Networks and hundreds of third-party feeds.

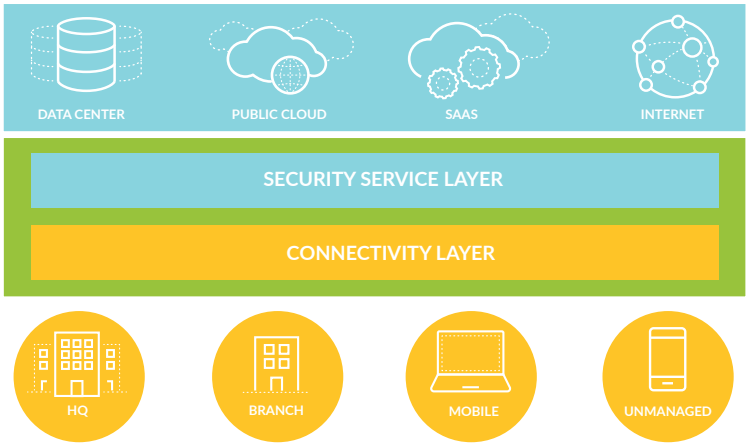

Figure 1: GlobalProtect cloud service architecture

Connectivity Layer

GlobalProtect cloud service goes beyond traditional remote-access virtual private network (VPN) connectivity to provide secure access to all applications—in the cloud, in your data center, or on the internet—in a consistent manner.

		Location of the Application							
		Branch Office	HQ / Regional HQ	Public Cloud	Hybrid Cloud	Private Cloud / Data Center	SaaS	Web	Internet
Location	Branch / Remote Network	✓	✓	✓	✓	✓	✓	✓	✓
	Mobile User	✓	✓	✓	✓	✓	✓	✓	✓

Networking for Remote Networks

- Connect branch offices to GlobalProtect cloud service over a standard IPsec VPN tunnel, using common, IPsec-compatible devices, such as your existing branch router, SD-WAN edge device, or a third-party firewall.
- Use Border Gateway Protocol (BGP) for simplified routing from the branch.

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.
- Use an always-on full tunnel for optimal security. GlobalProtect cloud service supports split tunnel based on access route, route; per-app VPN split tunneling; and split tunnel based on low-risk/high-bandwidth applications, such as streaming video.

Management Layer

Management with Panorama

- Enforce intuitive policy control with Panorama™ network security management, with applications, users, threats, malware, URLs, file types, and data patterns all in the same policy.
- Gain actionable insight into traffic and threats with Application Command Center (ACC), and enjoy fully customizable reporting.
- Get aggregated logging and event correlation.

Bandwidth Management

- Enable application whitelisting and blocking policies with App-ID™ technology to free up the network from unnecessary, bandwidth-hogging applications.
- Prioritize and shape the traffic handled by GlobalProtect cloud service using quality of service (QoS) policies.

Logging with Cortex Data Lake

- Take advantage of automated, centralized, cloud-scalable log storage with Cortex™ Data Lake.
- Centralize your management and reporting.
- Forward logs to your syslog server and/or security information and event management (SIEM) system.

Security Service Layer

Visibility and Access Control

- Identify application traffic and enforce security policies across all ports and protocols. Custom App-IDs enforce policies over internal and custom applications.
- Identify users and enforce access policies with User-ID™ technology.
- Use multi-factor authentication (MFA) for additional identity assurance.
- Enforce granular policy based on the state of users' devices with Host Information Profiles (HIPs).

Data Protection

- Use GlobalProtect cloud service for in-line enforcement of policies to control access to sanctioned applications, provide security to safely use tolerated applications, and block access to unsanctioned applications.
- Maintain bidirectional control over the unauthorized transfer of files, Social Security and credit card numbers, and custom data patterns.
- Control and block applications that pose risks to data.
- Control file movement over the network with policies to enable or restrict file transfer capabilities based on application, user, and file type.
- Deploy Aperture™ SaaS security service (subscription required) to address cloud access security broker (CASB) requirements for risk discovery, deep visibility, and data protection with software-as-a-service applications.

Inline SaaS Security

- Control access and protect data in sanctioned applications
- Permit tolerated applications with visibility and inspection
- Block access to unsanctioned applications

Threat Prevention

- Use in-line malware prevention to apply payload-based signatures based on Palo Alto Networks cloud-delivered threat intelligence.
- Use intrusion prevention system (IPS) capabilities to protect hosts and workloads, in both directions, by blocking exploits and evasive techniques—including port scans, buffer overflows, packet fragmentation, and obfuscation.
- Block command-and-control (C2) activity, data exfiltration, and delivery of secondary malware payloads.
- Block suspicious or malformed Domain Name System (DNS) queries, and sinkhole DNS queries from infected hosts to sever communications back to the attacker.

URL Filtering/Web Security

- Block access to inappropriate or unauthorized URL categories.
- Automatically block web-based attacks, including phishing links in emails, phishing sites, HTTP-based C2, and pages that carry exploit kits.
- Stop in-process credential phishing by blocking users from sending corporate credentials to unknown sites.
- Build custom URL categories, alerts, and notification pages.

WildFire Malware Analysis

- Detect zero-day malware and exploits with layered analysis through WildFire® malware prevention service.
- Automate prevention in as few as five minutes.
- Take advantage of community-based data for protection.

AutoFocus Threat Intelligence (Subscription Required)

- Gain context and classification for attacks—including malware family, adversary, and campaign—through AutoFocus™ contextual threat intelligence service to speed prioritization and response efforts.
- Make security teams more effective with rich, globally correlated threat analysis sourced from WildFire.

Magnifier Behavioral Analytics (Subscription Required)

- Use automated profiling of user and device behavior to identify anomalies with Magnifier™ behavioral analytics.
- Spot stealthy network threats by identifying behavioral anomalies indicative of C2, lateral movement, and data exfiltration.

Packaging and Licensing

	GlobalProtect Cloud Service for Remote Networks	GlobalProtect Cloud Service for Mobile Users
Use Case	• Branch offices • Remote sites • Virtual private clouds • SD-WAN gateways • SD-WAN edge devices	Mobile users with: • Laptops • Smartphones • Tablets
LICENSING		
Basis	Mbps	Users
	Based on bandwidth pool, which can be divided in increments of 2, 5, 10, 20, 25, 50, 100, 150, 300, 500 or 1000 Mbps.	Based on total number of unique users
Service Tunnels		
Baseline Service Tunnels	Up to three service tunnels included	
Additional Service Tunnels	Deploy additional service tunnels (up to a total of 100) by allocating 300 Mbps of remote network bandwidth pool per additional service tunnel	
CONNECTIVITY		
Connection Type	Site-to-site IPsec	GlobalProtect app IPsec/SSL
GlobalProtect App Platform Support	N/A	• Apple iOS • Apple macOS • Google Android • Google Chrome OS • Linux CentOS • Red Hat Enterprise Linux • Ubuntu • Windows
SECURITY		
URL Filtering	Included	
Threat Prevention	Included	
WildFire	Included	
Host Information Profile	Included	
Magnifier	Subscription required	
Aperture	Subscription required	
AutoFocus	Subscription required	
Logging	Subscription Required	
SSL Decryption	Included	
SaaS Application Usage Report	Included	
Inline SaaS Security	Included	

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-cloud-service-ds-031519