

# GlobalProtect

Delivering full next-generation firewall controls and integrated threat prevention to any user in any location.

- Consistent visibility and enforcement of enterprise security policy both inside and outside of the physical enterprise.
- Deep policy controls based on applications, user, content and host profile.
- Leverages any and all Palo Alto Networks™ firewalls to deliver protection and performance to any end-user location.



Modern enterprises are no longer bound by the physical constraints of the office, as network users and applications have become more flexible and distributed. End-users view physical boundaries as an outdated anachronism, and simply expect to be able to connect and work from any location using a mixture of laptops, smartphones and tablets. This has created a challenge for IT security teams who must protect all users even when they are not at their office desk. In these situations, IT teams are often forced to settle for security compromises that fall well short of the standard of security set by the next-generation firewall.

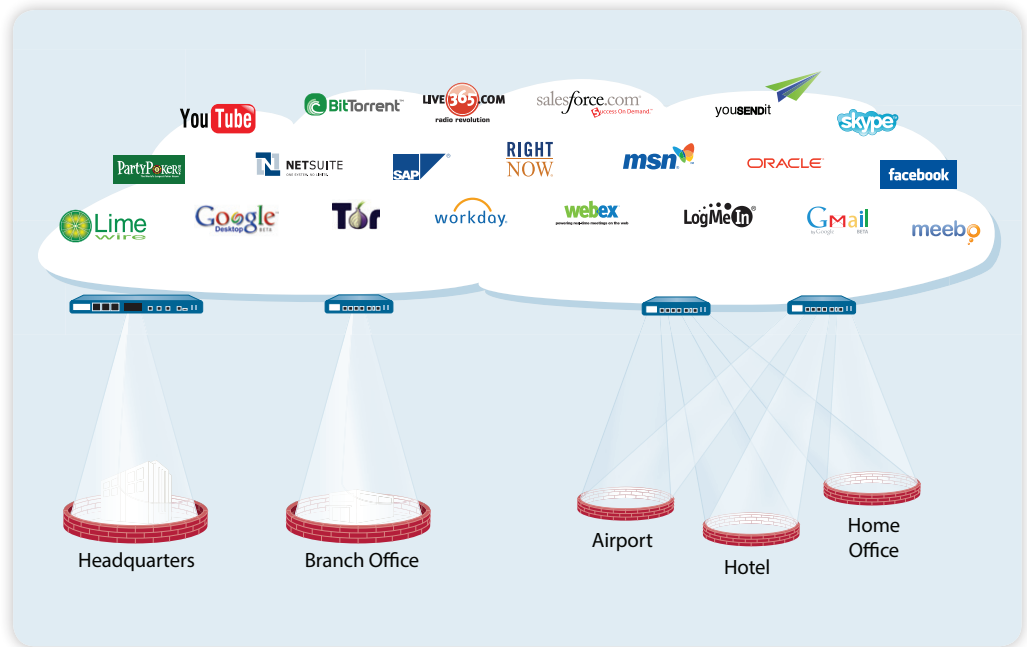
GlobalProtect bridges the divide between remote users and the enterprise security policy. First and foremost, GlobalProtect not only provides VPN access to corporate network but also extends enterprise security policy to all users regardless of their location. GlobalProtect frees enterprises from having to deploy different stacks of non-deterministic and inconsistent security solutions like proxy and VPN for their remote users. GlobalProtect connects users to the next-generation firewall to deliver full visibility, control and threat prevention to all enterprise traffic. Additionally, support for Windows, Mac OS X, Linux, iOS and Android devices ensures broad coverage of today's most popular computing platforms. This approach allows IT teams to reverse the steady erosion of enterprise security policy, and easily extend policy everywhere it needs to go.

Second, GlobalProtect enables new policy controls based on the configuration of the end-point itself, such as the operating system patch level, validating that the antivirus solution is up to date or that disk encryption is enabled. These controls are fully integrated into the next-generation firewall, enabling new policies such as restricting access to sensitive or risky applications if the user's system is not properly configured or up to date. When added to the next-generation controls based on application, user and content, this provides security teams with even more flexibility to design the ideal security policy for the enterprise.

As a complete solution, GlobalProtect provides consistent visibility, enforcement and protection regardless of an end-user's location or mode of connectivity. This approach breaks the reliance on the outdated notion of a physical perimeter, and enables the enterprise to migrate to a logical perimeter. This approach re-establishes the corporate security policy as the rule of law for all network connections and brings a unified and consistent approach to policy enforcement, threat prevention and security reporting.

### The GlobalProtect Solution

GlobalProtect extends security policy to all users, no matter where they are located.



### Applications and Users On the Move

Modern enterprises and their networks are no longer centralized fortresses of data, with users and applications tucked safely behind a well-managed perimeter. Instead, work increasingly takes place outside the traditional office, and businesses need to enable users to remain productive regardless of their location, and a myriad of mobile devices and connectivity options deliver on this need. Similarly, enterprise applications and data are being increasingly abstracted from their traditional in-house infrastructure and are migrating off-site either to the cloud or remote hosting centers.

As these assets have moved beyond the traditional perimeter, they have also moved beyond the protection of the corporate firewalls, application control, IPS and filtering solutions that make up the bedrock of corporate security policy. This leads to wide variability in terms of security quality and consistently undermines the enterprise security policy.

For users in the field, the risks posed by evasive applications, social networking, and modern threats remain high, but the protections drop off precipitously when the user is outside the network perimeter. In terms of policy, security teams must maintain parallel policies for the corporate network and mobile users, each with very different capabilities, rules and reporting. Correlating information between these products just adds to the already large operational burden. The end-result is that the security policy, the quality of protection and the overall risk are essentially left to chance based on how and where the user chooses to connect.

### The GlobalProtect Solution

GlobalProtect introduces a modern approach to enterprise security that incorporates mobile computing into the overall enterprise security strategy. GlobalProtect begins with a familiar mobile security technology – the remote access VPN. GlobalProtect agent automatically connects the user to the

optimal gateway. An enterprise can use all of its Internet firewalls as GlobalProtect gateways in order to deliver the best performance for all users and their traffic. itself, which can then be tied to next-generation policies based on applications, user role and content. This approach allows security teams to manage policy for all users from a single location instead of creating separate, independent policies.

### Dynamic and Distributed Architecture

GlobalProtect leverages the distributed nature of modern enterprises to break the bottlenecks that have traditionally plagued centralized solutions such as SSL VPNs. Instead of sending all traffic back to a single centralized location, GlobalProtect actually adapts to the end-user's location to find the best path to a gateway, without requiring any effort on the user's behalf. GlobalProtect automatically tests all available gateways to determine the route with the fastest response times. This approach ensures that a user always leverages the fastest option based both on location and relative load on the various gateways. It provides protection against failure if a gateway becomes unavailable, as GlobalProtect will automatically switch to the next best available gateway. This model avoids the congestion and latency common to backhaul solutions and enables the enterprise to maximize value from all of their Palo Alto Networks firewalls.

### Consistent Security Everywhere

GlobalProtect leverages the full complement of network security measures in the Palo Alto Networks next-generation firewall to keep users safe and under the jurisdiction of corporate policy at all times. By maintaining a persistent connection to the optimal gateway, both internal and external users enjoy the same protection against dangerous content such as modern malware. Policies for acceptable use and security can be enforced in all locations, ensuring that there are no gaps in coverage whether in the office or on the road.

### Enforce Network Controls Based on User and Device Profile

GlobalProtect also enables new enterprise policies and controls that tie to the configuration of the end user's device using a Host Information Profile (HIP). If the user's end-point is not properly secured, security teams can automatically enforce network controls to compensate. For example, a user may have rights to access certain information on the enterprise network, but GlobalProtect can prevent that user from downloading files if his laptop is not using disk encryption. Alternatively, if the endpoint antivirus is out of date, GlobalProtect can automatically restrict access to risky or sensitive applications. When added to the application, user and content controls available from the Palo Alto Networks next-generation firewall, security teams now have a level of control and flexibility that they have never had from traditional solutions. Just as the next-generation firewall allows for more granular controls of firewall policy, GlobalProtect offers granular control of user rights based on their host configuration. Policies can be based on:

- Operating System and Application Patch Level
- Device type, such as iOS, Android, Windows, or Mac
- 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)

### Flexible and Seamless Authentication

GlobalProtect provides several options for user authentication. Using single sign-on, the solution seamlessly integrates with Windows login to securely and transparently sign the user into the GlobalProtect infrastructure after logging in to Windows.

Several different authentication infrastructures can be used to authenticate users. GlobalProtect supports all of the existing PAN-OS authentication methods including Kerberos, RADIUS, LDAP, client certificates, and a local user database.

### Supported Operating Systems

- Microsoft Windows 8
- Microsoft Windows 7
- Microsoft Windows Vista
- Microsoft Windows XP
- Mac OS X
- Apple iOS 5.1 and later
- Android 4.03 and later
- Linux (using vpnc)