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 End-users view physical boundaries as an outdated anachronism, and simply expect to be able to connect and work from any location using a mixture of laptops, smartphones and tablets.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 now have the challenge of protecting all users and locations even when they are beyond the protections of the traditional network perimeter. In these cases, 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.

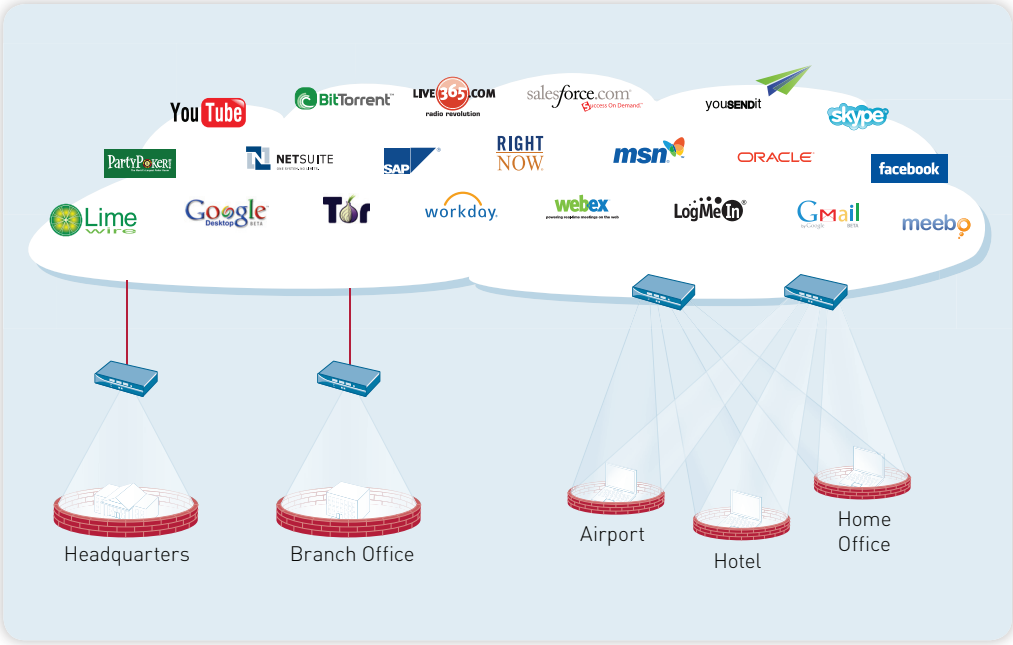
GlobalProtect bridges the divide between remote users and the enterprise security policy. First and foremost, GlobalProtect provides a transparent agent that extends enterprise security policy to all users regardless of their location. This means that all the visibility, control and threat prevention of the next-generation firewall is applied consistently to all enterprise traffic. Additionally, support for Windows, Mac OS X and iOS 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 based quality and consistency in information security. 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.

paloalto NETWORKS
the network security company™

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 be able 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. The GlobalProtect agent is available to all enterprise users free of charge to ensure basic levels of remote connectivity. From this base, GlobalProtect builds more advanced features that transform mobile security. When licensed, the GlobalProtect agent automatically connects the user to the best performing Palo Alto Networks gateway, enabling an enterprise to make use of all its firewalls and deliver the best possible performance for all users and their traffic. Additionally the solution inspects the security of the host machine itself, which can then be tied to next-generation policies based on applications, user role and content. This approach allows security teams to add mobile security policies to their existing next-generation firewall policies instead of creating a separate, independent security policy.

Remote Access for All Users

The GlobalProtect agent is the most basic component of the GlobalProtect solution. Unlike other solutions, the GlobalProtect agent is a free component of the Palo Alto Networks next-generation firewall and can be delivered to all end-users automatically via Active Directory or Microsoft System Configuration Manager or can be downloaded directly from the GlobalProtect portal The agent provides secure connectivity between a remote user and the enterprise Palo Alto Networks firewall to ensure secure connectivity as well as next-generation visibility and control of traffic regardless of location. The agent supports Microsoft Windows XP, Vista, Windows 7, Mac OS X and iOS-based devices such as the iPhone and iPad, enabling IT to extend security and connectivity to a wide variety of today's most popular devices.

The agent establishes a secure tunnel for end-user traffic via IPSec or SSL. This step not only routes traffic back to the next-generation firewall for security enforcement, but also helps prevent users from being lured into "honeypot" connections or falling into Man-in-the-Middle (MITM) exploits.

Advanced Components of GlobalProtect

Building upon basic remote-access capabilities, other more advanced features of GlobalProtect require a license, which is applied to Palo Alto Networks firewalls. Unlike other mobile security solutions, GlobalProtect is not licensed in terms of users. Licenses are tied to the firewalls and can support as many users as needed (limited only by the capacity of the hardware itself).

- **Distributed Multi-Gateway Deployment –** The GlobalProtect gateways are responsible for the majority of the actual security enforcement in the solution. Similar to the portal, any Palo Alto Networks firewall can be a gateway for the GlobalProtect solution. When licensed, multiple GlobalProtect gateways can be deployed. The GlobalProtect agent automatically tests the available gateways to create the fastest connection possible for that user's location. This step enables GlobalProtect to dynamically make use of multiple Palo Alto Networks gateways, and breaks the centralized backhaul approach found in traditional VPN solutions.
- **Host Information Profiles –** In addition to network discovery and VPN connectivity, when licensed, the GlobalProtect agent can gather, compile and provide a Host Information Profile (HIP) to the gateways to augment the security policy as well as provide increased visibility into the state of remote devices. The Host Information Profile includes such information as patch level, disk encryption, personal firewall state, antivirus versions and much more.

Dynamic and Distributed Architecture

The GlobalProtect architecture 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, the GlobalProtect solution actually adapts to the end-user's location to find the best path to a gateway. The GlobalProtect agent 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. This model avoids the congestion and latency common to backhaul solutions and enables the enterprise to get added value from all of their Palo Alto Networks firewalls as they work together as a virtual security service.

Enforce Network Controls Based on User and Device Profile

GlobalProtect also enables new enterprise policies and controls that are tied to the configuration of the end user's device. 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 the GlobalProtect gateway can prevent that user from downloading files if his laptop is not using disk encryption. Alternatively, if the host antivirus is out of date, staff can automatically restrict access to social networking sites where malware tends to propagate. 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 the following host characteristics:

- 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)

Flexible and Seamless Authentication

GlobalProtect provides several options for user authentication. Using single sign-on, the solution seamlessly integrates with the Windows login infrastructure 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 XP
- Microsoft Windows Vista
- Microsoft Windows 7
- Mac OS X (Snow Leopard, Lion)
- Apple iOS (uses built-in IPSec client)

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com