

- **GlobalProtect Gateway:** 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. However, unlike the portal, you can leverage as many gateways simultaneously as you need, ensuring multiple potential routes between an agent and gateway. The Gateway has three core functions: First and foremost, it performs the full breadth of next-generation firewalling functionality including application control, threat prevention, URL filtering, user visibility, etc on all traffic from associated GlobalProtect Agents. It also provides the end of the secure connection established by the Agent. Lastly, it receives the Host Information Profile (HIP) and enforces policies accordingly.

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 hosted security service.

Enforce Network Controls Based on User 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. Or alternatively, if the host antivirus is out of date, staff can automatically restrict access to social networking sites where malware tends to propagate.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
- Host Firewall Version
- Disk Encryption
- Data Backup Products
- Customized host conditions

Transparent VPN and Single Sign-On

GlobalProtect also acts as a transparent SSL VPN that establishes a secure tunnel for end-user traffic regardless of their method of connectivity. This step helps prevent users from being lured into "honeypot" connections or falling into Man-in-the-Middle (MITM) exploits by ensuring that all traffic remains encrypted between the end-user laptop and the Palo Alto Networks gateway. This provides an additional set of protections for users who may need to use unfamiliar networks for connectivity when they are outside the corporate network.

Additionally GlobalProtect provides a single sign-on solution for end-users. The solution seamlessly integrates with the Windows Login utility to securely store logon information for subsequent logons such as VPN authentication.

Supported operating systems

- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 7



Palo Alto Networks
 232 E. Java Drive
 Sunnyvale, CA. 94089
 Sales 866.207.0077
www.paloaltonetworks.com

Copyright © 2011, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, the Palo Alto Networks Logo, PAN-OS, App-ID and Panorama are trademarks of Palo Alto Networks, Inc. All specifications are subject to change without notice. Palo Alto Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. PAN-OS 4.0, March 2011.