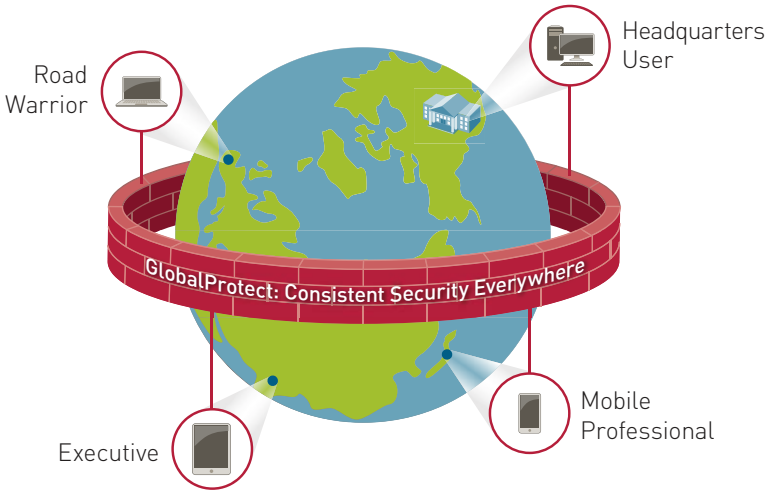
# GlobalProtect™: Safely Enabling Mobile Devices

GlobalProtect provides a unique mobile security solution that integrates traditionally distinct technologies to manage the device, protect the device and control the data.

### GlobalProtect components:

- **GlobalProtect Gateway:** Delivers mobile threat prevention and policy enforcement based on apps, users, content, device and device state
- **GlobalProtect App:** Enables device management, provides device state information, and establishes secure connectivity
- **GlobalProtect Mobile Security Manager:** Provides device and app management, malware detection and shares device state information with GlobalProtect Gateway




Mobile computing is one of the most disruptive forces in information technology. It is revolutionizing how and where employees work, and the tools that they use to perform their jobs. Mobile devices are not just ways to access existing applications such as corporate email, but the platform for opening up entirely new ways of doing business.

Organizations must take steps to manage the risks that mobile devices face. In order to fully realize all of mobility's benefits and safely enable mobile devices, enterprises must:

### Manage the Device

- Ensure devices are safely enabled by configuring the device with proper security settings. Simplify deployment and setup by provisioning common configurations like account settings for email and credentials such as certificates.

### Protect the Device

- Protect the mobile device from exploits and malware. Protecting the device also plays an important role for protecting the data as well, because data is not safe on a compromised device.

### Control the Data

- Control access to data and control the movement of data between applications. Establish policies that define who can access sensitive applications, and the particular devices that can be used.

### Introducing GlobalProtect from Palo Alto Networks®

GlobalProtect from Palo Alto Networks safely enables mobile devices for business use by providing a unique solution to manage the device, protect the device and control the data. It blends together the necessary technology and intelligence to provide a comprehensive solution for mobile security, enabling the organization to stop mobile threats, enforce security policies, and protect networks from compromised and non-compliant mobile devices.

paloalto NETWORKS®

GlobalProtect has three primary components:

- **GlobalProtect Gateway:** Delivers mobile threat prevention and policy enforcement based on apps, users, content, device and device state. Extends a VPN tunnel to mobile devices with GlobalProtect App. Integrates with WildFire for preventing new malware.
- **GlobalProtect App:** Enables device management, provides device state information, and establishes secure connectivity. Connects to the GlobalProtect Gateway to access applications and data in accordance to policy. Exchanges device configuration and device state with the GlobalProtect Mobile Security Manager.
- **GlobalProtect Mobile Security Manager:** Provides device management to configure the device. Uses WildFire malware signatures to identify devices with infected apps. Shares information about the device and device state with GlobalProtect Gateway for enforcing security policies. Hosts an enterprise app store for managing business apps. Isolates business data by controlling lateral data movement between business and personal apps.

## GlobalProtect Gateway

GlobalProtect Gateway establishes VPN connections to protect the traffic, enforces policy to manage access to applications and data, and provides protection against mobile threats. GlobalProtect Gateway runs on the Palo Alto Networks next-generation firewall, which is available in hardware (such as the PA-3000 Series or the PA-200) and virtualized (such as the VM-Series) form factors.

### *IPSec/SSL VPN Connections for Network Privacy and Consistent Security Everywhere*

In order to protect network traffic, GlobalProtect Gateway delivers IPsec and SSL VPN connections to mobile devices using GlobalProtect App. The VPN connection maintains network privacy even when the mobile device is being used in public locations such as hotels, conference halls and coffee shops. Multiple GlobalProtect Gateways can be deployed to service users in different geographies, and GlobalProtect App will automatically select the optimal gateway for the best performance in a given location.

The VPN connection terminates at the GlobalProtect Gateway running on the next-generation firewall and thus provides consistent enforcement of network security policies, regardless of the user's location. GlobalProtect can automatically establish a VPN connection whenever connectivity is available and extend a "logical" perimeter that consistently protects local and remote users with the same policies, wherever they may go.

## Mobile Threat Prevention

GlobalProtect Gateway delivers mobile threat prevention using technologies from the next-generation firewall, powered by a system to gather and distribute intelligence about the latest mobile apps and threats. The threat prevention technologies identify and block exploits, malware, malicious URLs and command & control traffic to disrupt the lifecycle of modern malware.

In order to identify newly emerging threats, WildFire from Palo Alto Networks dynamically analyzes the behaviors of samples gathered from app stores and GlobalProtect Gateways from around the world. When WildFire discovers a new piece of malware, it will automatically provide new signatures to GlobalProtect Gateway (for threat prevention) and GlobalProtect Mobile Security Manager (to detect devices infected with malware). GlobalProtect can automatically take action against infected devices by notifying the user and restricting access to the sensitive parts of the network.

### *Control Access to Applications and Data*

Security teams can establish policies based on application, user, content, device, and device state in order to maintain granular control over the users and the devices accessing a given application.

GlobalProtect uses a Host Information Profile (HIP) to share information about the device and the device state. Host Information Profile contains information about the device characteristics, configuration and state, which can be used for making policy decisions about the resources the device can access. For example, an organization may permit approved employees to access customer data from a corporate device, while blocking access from a personally owned device.

An organization may want to apply policies that restrict access based on other characteristics of the device. For example, security teams may want to provide full access to devices with current operating systems, but restrict access to devices on older, unsupported platforms.

### *Controlling Data Movement through File Blocking and Data Filtering*

GlobalProtect Gateway includes file and data filtering technology to control data movement. Data filtering features enable administrators to implement policies that reduce the risks associated with the transfer of unauthorized files and data.

Some of the file blocking and data filtering methods include:

- **File blocking by type:** Control file transfers based on policy for specific file types.
- **Data filtering:** Control the transfer of sensitive data patterns such as credit card and social security numbers.
- **File transfer function control:** Allow users access applications, but limit or restrict the use of file transfer functions.

### *Internal Gateway*

GlobalProtect Gateway can also be used to strengthen the security of the internal network as well. Instead of implicitly trusting everyone connected to the local network, many organizations are adopting policies to trust no one before they are identified. Internal GlobalProtect Gateways help organizations establish stronger internal controls by establishing the identity of the user and device state before providing access to sensitive applications.

## GlobalProtect App

GlobalProtect App on mobile devices establishes a device-level VPN connection to the GlobalProtect Gateway in order to protect traffic and enforce security policies. The same app connects to GlobalProtect Mobile Security Manager to enable device management and share information about the state of the device. GlobalProtect App can automatically select the optimal gateway for a given location to provide a transparent user experience for security. On iOS devices, GlobalProtect App can be configured for app-level VPN.

## GlobalProtect Mobile Security Manager

GlobalProtect Mobile Security Manager ensures that devices are appropriately configured for use in a business environment, manages the distribution of business apps, and provides protection for business data resident on mobile devices. GlobalProtect Mobile

Security Manager runs on the GP-100 appliance, and works together with GlobalProtect Gateway and GlobalProtect App.

## Device Management

GlobalProtect Mobile Security Manager configures and manages device settings, such as requirements for a passcode and passcode complexity. Some security teams may want to create policies that disable particular device functions (the camera for example). In addition, GlobalProtect Mobile Security Manager can configure account settings for email, VPN and Wi-Fi networks.

GlobalProtect Mobile Security Manager can assist users who are having issues with their mobile device by performing key operations such as locking or unlocking the device remotely, or wiping a lost device.

- **App Management and Distribution** GlobalProtect Mobile Security Manager can be set up as an enterprise app store. It can push business apps to mobile devices from the Apple App Store, Apple Volume Purchase Program (VPP), and Google Play, thus helping the users get the apps they need for work.

### *Business Data Segmentation*

**For iOS7 and later:**

- **Isolate Business Data and Control Data Movement:** GlobalProtect Mobile Security Manager can isolate business data from personal data by providing organizations with control over the lateral movement of business data from a managed business app to a personal app.
- **Selective Wipe:** Selective wipe allows organizations to wipe managed apps, accounts and data without affecting the rest of the user's personal content.

## Device State

GlobalProtect Mobile Security Manager performs ongoing checks to monitor the configuration and state of a managed mobile device. The information about device state plays an important role for ongoing compliance with security policy, allowing the security team to stay on top of device and app usage within the organization. Device state helps administrators identify a number of risky conditions, such as whether the device has been jailbroken or rooted, for example.

GlobalProtect Mobile Security Manager shares information about device state with the GlobalProtect Gatewaywhich in turn uses this information to make security policy decisions. For instance, a policy might use device state as part of the criteria for determining the level of access, while excluding access from non-compliant and compromised devices.

GlobalProtect Mobile Security Manager takes inventory of the applications that are on the device, and looks for malware using signatures from WildFire. When GlobalProtect Mobile Security Manager finds malware, GlobalProtect Gateway can take action to limit the resources that the device can access until the issue has been remediated.

## GlobalProtect Gateway Specifications

### VPN CONNECTION

- IPsec
- SSL
- Automatic discovery of optimal gateway
- Manual gateway selection
- Automatic or manual connection

### INTELLIGENT POLICY ENGINE

- Extensive visibility and traffic classification
- Policy based on application, user, content, device and device state

### DEVICE STATE

Host Information Profile (HIP) provides device state details about the condition of the endpoint/mobile device.

**For Windows and Mac platforms, the Host Information Profile includes additional information such as:**

- Patch management
- Host antivirus
- Disk encryption
- Data loss prevention
- Host antispyware
- Host firewall
- Disk backup
- Customized host conditions (e.g. registry entries, running software)

**For iOS and Android platforms, the Host Information Profile includes device state information, such as:**

- Managed/unmanaged device status
- Jailbroken / rooted
- Malware infection
- Device ownership (Corporate/BYOD)
- Device security settings (device passcode status, encryption)
- IMEI
- Serial number
- Whitelisted apps
- Blacklisted apps

### MOBILE THREAT PREVENTION

- Vulnerability (IPS) and malware (AV) protection
- URL filtering for protection against malicious websites
- WildFire static and dynamic analysis

### AUTHENTICATION

All PAN-OS™ Authentication methods supported, including:

- Kerberos
- LDAP
- Local user database
- RADIUS
- Client certificates

**Two-Factor Authentication:** Certificate plus password, one-time password, smart card

**On Windows:** Supports single sign-on through Windows loginlatform, including hardware (such as the PA-5000 series, the PA-3000 series and the PA-200) and virtual (VM-Series) form factors.

### PLATFORM

- Palo Alto Networks next-generation security platform, including hardware (such as the PA-5000 series, the PA-3000 series and the PA-200) and virtual (VM-Series) form factors.

## GlobalProtect Mobile Security Manager Specifications

### MANAGE DEVICE SETTINGS

Configure and manage mobile device settings, such as:

- Passcode
- Certificates
- Device restrictions
- Email account settings
- Wi-Fi networks
- VPN settings

### DEVICE STATE DETECTION

Obtain the device state for visibility, compliance, and automatic policy enforcement. Device state detection includes:

- Device operating system
- Device identifiers: Serial number, IMEI
- Jailbroken / Rooted
- Whitelisted apps
- Malware infection
- Blacklisted apps

### OPERATIONS

- Wipe device
- Selective wipe
- Lock device
- Unlock device
- Locate the device
- Push policies to the device
- Send message to the device

### DETECT MALWARE

- Detect malware on Android devices using signatures from WildFire

### REPORTING

- Dashboard and reporting on device usage, device states, and policy compliance

### PLATFORMS

- Palo Alto Networks GP-100
- Maximum number of supported devices: 100,000

## GP-100 Specifications

### I/O

- (4) 10/100/1000 (1), DB9 console serial port

### STORAGE

- GP-100 1TB RAID: 2 x 1TB RAID certified HDD for 1TB of RAID storage

### POWER SUPPLY (AVG/MAX POWER CONSUMPTION)

- 500W/500W
- MAX BTU/HR
- 1,705

### INPUT VOLTAGE (INPUT FREQUENCY)

- 100-240VAC (50-60Hz)

### MAX CURRENT CONSUMPTION

- 10A@100VAC

### MEAN TIME BETWEEN FAILURE (MTBF)

- 14.5 years

### RACK MOUNTABLE (DIMENSIONS)

- 1U, 19" standard rack (1.75"H x 23"D x 17.2"W)

### WEIGHT (STAND ALONE DEVICE/AS SHIPPED)

- 26.7lbs/35 lbs

### SAFETY

- UL, CUL, CB
- EMI
- FCC Class A, CE Class A, VCCI Class A

### ENVIRONMENT

- Operating temperature: 40 to 104 F, 5 to 40 C
- Non-operating temperature: -40 to 149 F, -40 to 65 C

## GlobalProtect App Specifications

### SUPPORTED PLATFORMS

- Windows 8.1, 8, 7, Vista, XP
- Mac OS X 10.6 and later
- Android 4.0.3 and later
- Apple iOS 6.0 and later
- Linux supported using third party vpnc client

### LOCALIZATION

- English
- Spanish
- German
- French
- Japanese
- Chinese

paloalto NETWORKS®
the enterprise security company™

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com