GlobalProtect Deployment Guide

March 2015

Every organization wants its employees to be productive. In a growing number of cases, this includes an employee population that is highly mobile — traveling and using a wide array of tools, including laptops, smartphones and tablets.

Under these conditions, it can be difficult to consistently and effectively secure the devices used and the data accessed by the employee. In addition, the devices may be personal, in some cases, raising additional questions about what are the appropriate policies. Many organizations are encountering issues with the strategies they have taken to date to secure mobile devices, due to incomplete security measures or shortcomings with the user experience.

Enterprises should enable employees to work effectively while applying appropriate security controls. This document outlines how organizations can use GlobalProtect™ to provide a secure environment for the increasingly mobile workforce.

Application and Data Access Considerations

Applications and data that can be accessed should be evaluated and categorized as being either highly sensitive, medium sensitive, or non-sensitive. Access should be based on:

- The user's role and function in the organization
- The type and state of the device being used
- The network on which the device is being used

Highly sensitive applications may include source code systems, financial databases, and IT management tools. Access to highly sensitive applications should only be allowed when there is high certainty of the security of the device accessing them and the user of the device. Only un-compromised, managed corporate devices should be allowed to access these applications. When accessed from external networks, two-factor authentication like OTP should be considered to ensure only authorized users are accessing these applications.

For medium-sensitivity applications, access from personal devices could be allowed. Transparent authentication like certificates and/or AD credentials will increase security without affecting usability. However, only un-compromised, managed devices should be allowed to access these applications.

For non-sensitive applications, allowing access from unmanaged devices may be acceptable.

Personal Devices

For personal devices, full device management is not necessary. However, corporate applications on the mobile device should be managed and only allowed to share data with other managed apps. This will ensure the corporate data is kept isolated from the unmanaged personal applications. Allowing users to use the native user interface and built-in applications, such as the email client of their preferred device, can increase productivity. Restricting users to webmail interfaces, containers or other non-native interfaces will frustrate users and reduce their productivity.

Email is one of the most frequently used applications on a mobile device and requires additional considerations. ActiveSync should only be allowed on managed devices. Email account settings should be managed to prevent attachments from being stored on an unmanaged device, so that sensitive information cannot be shared with unmanaged applications. If unmanaged devices are allowed to access email services, enforce restrictions on access to attachments when reading messages.

Preventing and Detecting Compromised Devices

No data is safe if the device is infected with malware or if it has been rooted or jailbroken. Because network traffic inspection is critical to keeping the device and data safe, devices must be consistently connected to the security infrastructure. This is done through a VPN tunnel for all traffic from the corporate device. In order to respect user privacy on personal devices, tunnel only traffic from managed applications and balance the risk by continuously monitoring the device state to detect the installation of malware or to detect a rooted or jailbroken device.

Network Infrastructure

It is critical that sufficient infrastructure is in place to handle the traffic from all of the devices used by the mobile workforce. The first step is understanding where the users are predominantly located and the number of users in each location. It is also important to consider where users travel regularly so that they have a positive experience when on the road. The goal is to create an infrastructure that has enough regional capacity to accommodate the expected number of active users.

In addition to users accessing corporate applications and data from external networks, it is important to consider the policy for your internal wired and wireless networks. In many environments, a guest wireless network needs to be factored in as well. Understanding the state of the devices when connecting to these networks internally is just as important as when users are connecting from the outside.

GlobalProtect

GlobalProtect is an integrated security solution from Palo Alto Networks® to protect the mobile workforce. It provides the ability to configure, manage, deploy and enforce the above mentioned security requirements.

There are several components in a complete GlobalProtect deployment:

- GlobalProtect Gateways for VPN termination, security inspection and policy enforcement
- GlobalProtect Portal to manage the client GlobalProtect App
- GlobalProtect App which runs on laptops and mobile devices
- GlobalProtect Mobile Security Manager for managing mobile devices and detecting compromised devices

GlobalProtect App

GlobalProtect App is installed on each endpoint. For Mac OS X and Windows laptops, the app can be distributed via AD group policy or other software distribution mechanisms. For iOS and Android devices, the GlobalProtect App is available in the Apple App Store or Google Play.

For other types of devices, standard IPsec clients may be used, although not all functionality will be available.

GlobalProtect Portal

GlobalProtect Portal is typically deployed on a pair of PAN-OS® firewalls in high availability. In most cases, the Portal will reside on a firewall that is also acting as a GlobalProtect Gateway. To ensure only authorized users register their devices on GlobalProtect Portal, use AD authentication for GlobalProtect Portal.

GlobalProtect Gateways

For security inspection and policy enforcement, deploy multiple PAN-OS firewalls as external GlobalProtect Gateways to provide coverage for users in various regions.

Configure internal PAN-OS firewalls as Internal GlobalProtect Gateways for network policy enforcement when the endpoints are on the internal network.

External Gateways

In order to provide reasonable security while providing a seamless user experience, use client certificates and AD authentication for external GlobalProtect Gateways that are protecting the less sensitive corporate applications. External GlobalProtect Gateways protecting highly sensitive applications should be configured as manual gateways, and should require a client certificate along with two-factor authentication. When users access these applications, they select the specific gateway and are prompted for two-factor authentication.

To ensure enough regional capacity to accommodate the expected quantity of active users, deploy external gateways within a 150 ms or better latency for common Internet services. For most environments, 25 Mbps per 100 concurrent users should provide sufficient bandwidth. For example, if 300 concurrent users are expected at a specific gateway, then 75 Mbps of bandwidth to the gateway and VPN throughput within the gateway would be required. The platform of choice for a given gateway can be deduced from the supported concurrent tunnels and VPN throughput numbers listed on the spec sheets for the next-generation firewall.

Using Amazon AWS for External GlobalProtect Gateways

To provide global coverage, GlobalProtect gateways can be deployed in a virtual form factor on public cloud infrastructure such as Amazon AWS. The following are locations where Amazon AWS service is available: Oregon, Northern California, Virginia, Ireland, Singapore, Sydney, Tokyo, Beijing and Brazil. The VM-Series firewall in AWS significantly simplifies the logistics and reduces the costs that are typically required to set up this infrastructure to have coverage in the regions where you do not have a presence.

Internal Gateways

Configure PAN-OS firewalls protecting high- and medium-sensitive applications as internal GlobalProtect Gateways. The perimeter firewall facing your enterprise can act as an internal gateway as well. To identify users while providing a seamless user experience, use client certificates and AD authentication.

GlobalProtect Mobile Security Manager

Deploy a GlobalProtect Mobile Security Manager on the GP-100 platform for on-device policy enforcement. All internal gateways and external gateways should retrieve device state information from Mobile Security Manager. Use AD authentication for enrollment. Mobile Security Manager can onboard mobile devices with auto-configured accounts and configurations.

Host Information Profiles

To ensure that only managed and uncompromised devices are accessing the authorized applications, a security policy with the following device state requirements (HIP Profiles) should be enforced on all external and internal gateways:

- Device is managed.
- Mobile device is not rooted or jailbroken.
- Android device is not infected with malware.
- Laptops are running antivirus software with up-to-date signature definitions.
- To ensure that only corporate devices are accessing highly sensitive applications, a security policy to detect device ownership should to be enforced:
    - For Windows and Mac OS X, match the domain the device is connected to and the presence of systems management software like Altiris.
    - For iOS and Android devices, select corporate-owned devices in Mobile Security Manager and tag them accordingly. Then, use the tag to identify the devices as corporate devices in the security policy on the GlobalProtect Gateways.

Mobile Device Configurations

The following mobile configurations are recommended:

- Corporate Data – To ensure that corporate data is secure, require that device storage is encrypted and a strong passcode is set.
- Corporate Network Settings – Configure network, Wi-Fi and VPN settings on the user's behalf so they can use the device on corporate networks and with corporate applications.
- Corporate ActiveSync account – Require client certificate for authentication to ensure that ActiveSync is managed and allowed only from this managed account. The required client certificate should be included in the ActiveSync configuration itself.
- Corporate trusted CA certificate.
- Managed apps that are allowed to access corporate data.
    - o For personal devices, use per-app VPNs for all managed apps and corporate domains
    - o For corporate devices, use a always-on device-level VPN

Security Policies

Best practices for security policy should be followed for all traffic to the data center and to the Internet. This includes using the next-generation firewall features for WildFire™, IPS, App-ID™, antivirus, spyware, etc. For highly sensitive applications, rules should be created to only allow access from the gateway that is using two-factor authentication.

Security Zones

The organization should define the following network security zones:

- Internet (all traffic and services on the public Internet)
- GlobalProtect Users (all traffic coming over the VPN connections from external endpoints and for all traffic coming from internal endpoints)
- Corporate Data Center (all corporate data center apps)

SSL Decryption

Traffic encrypted with SSL is growing. By decrypting the SSL traffic, administrators can achieve the following:

- Identify the application being used in order to apply granular application control.
- Identify if there is any malware present within applications such as social media or webmail.
- Identify botnet command and control communications obfuscated using SSL.
- Identify leakage of confidential data.

Palo Alto Networks firewalls offers the following decryption methods: SSL inbound inspection and SSL Forward Proxy. We recommend SSL Inbound inspection to be performed on data center firewalls which are facing the Web or application server. Decrypt the appropriate URL of your business that the server is hosting.

In addition, consider implementing SSL outbound inspection on the GlobalProtect Gateway. When implementing SSL outbound inspection, the firewall intercepts the client's SSL requests to the server. To achieve this, the clients should trust the forward-trust certificate of the firewall. Administrators need to distribute the CA of forward-trust certificate of the firewall to the clients. The following are URL categories to consider for SSL outbound decryption:

- peer-to-peer
- social networking

- unknown
- Web-based email
- online storage and backup
- computer and internet-info (optional)

To protect end-user privacy and to stay compliant with corporate and regulatory policies, do not decrypt the following categories when implementing SSL outbound decryption:

- Financial services
- Health and medicine
- Government
- Legal
- Military

Management

Because all of the gateways will have nearly identical configuration, Panorama is recommend to manage the configurations. This will consist of the following:

- A device group for the security policy, security and HIP profiles. There should be no need for unique security rules on each gateway.
- A template to share networking settings, including LSVPN configuration, so that the devices can access corporate applications. It is recommended to configure each gateway as a GlobalProtect Satellite, connecting back to the LSVPN gateway that is also running the GlobalProtect Portal. That gateway would either have direct access to, or a site-to-site VPN connection to the corporate data center.
- Consolidate logging and reporting for the whole infrastructure.

Monitor the health of the GlobalProtect Infrastructure

To ensure enough capacity and proactively minimize downtime, monitor the health of the GlobalProtect infrastructure using a network performance monitoring utility. Continuously monitor the firewall CPU usage, Network Latency and Tunnel usage.

CPU and Tunnel usage – If the CPU usage is 80 percent or above, or if the average tunnel usage is 80 percent or above the platform capacity, these are signs of a performance bottleneck. Consider adding extra capacity by adding a new gateway or upgrading the gateway to a bigger platform. Poll the Gateway at one minute intervals.

Latency – Baseline the latency to access the GlobalProtect gateway interface by pinging at a regular interval. Ping the GlobalProtect gateway interface from a location where your network-monitoring tools are deployed, preferably from the corporate network. An increase in the latency could be a delay in the network or an indication of a performance bottleneck.

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