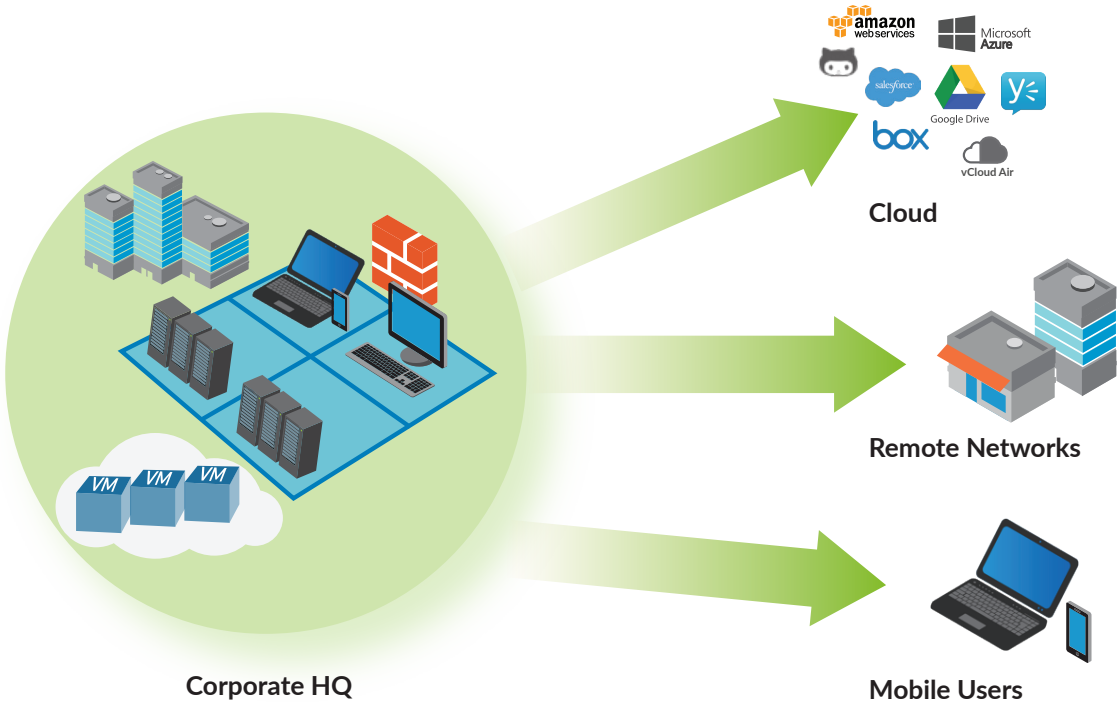
PROTECTING THE EXTENDED PERIMETER WITH GLOBALPROTECT CLOUD SERVICE

Delivering security with operational efficiency from the cloud

Your Perimeter Is Everywhere

The world you need to secure is undergoing tremendous transformation. Global expansion, mobile workforces and cloud computing are shifting the location of your applications, data and users. These changes introduce new opportunities for business, but they also create a set of cybersecurity risks.



These tectonic shifts in location strain an organization's ability to protect data and stop threats consistently. The mandate for security has not changed, but the ability to deliver protection at each location is at a crossroads. Many organizations, faced with the rising costs of extending the perimeter using conventional methods, are left with few other choices. These consequences place organizations at risk. It is important to understand where the risks lie to evaluate what must be done to bring security back into balance.

Underlying Security Issues

In light of the growing number and severity of cyberattacks, IT teams are undertaking enormous effort to strengthen perimeter security measures at headquarters, where the company's people and resources are typically concentrated. These efforts typically involve improving traffic visibility, as well as deploying measures to stop known and unknown exploits and malware. Security teams look for ways to improve their optics into network traffic to understand and mitigate the threat footprint.

With the effort spent to improve security at headquarters, why would any organization do anything less for remote networks or mobile users? High standards for security should be applicable everywhere. These users are no different from the employees at HQ, and they are exposed to the same types of risks. Yet there are many examples of cost, performance and security requirements being in conflict.

Backhauling Traffic to Headquarters

	Security	Management	Performance	Notes
Bring traffic back to HQ (Backhauling)	Same as the traffic at HQ. For mobile users, only protects when tunnel is up.	Same as HQ.	Depends on distance, but most locations experience poor performance.	Very expensive to extend the WAN using leased lines and MPLS.

One approach to enforcing consistent security in remote locations is to build out a WAN in order to bring the traffic back to the security at internet gateways. If all branch traffic is brought back to locations where an organization already has a firewall, then such traffic benefits from the same protections as if it had originated on the local network. This approach provides the consistency that security teams prefer, but it is expensive and, in many cases, poor in performance.

Traditional WANs, built out on leased lines or MPLS connections, are a big-ticket operating expense. The cost was necessary in the past, because users had to reach applications hosted in the internal data center. With a greater number of public cloud- or SaaS-based applications, the traffic mix has shifted, with a growing amount of traffic destined for the web.

These conditions introduce performance implications. To reach a cloud application across a conventional WAN architecture, the traffic has to be backhauled to headquarters, inspected at the egress point by the corporate gateway, sent to the application, and then hairpinned back to the branch office. The traffic path is impractical and slow.

This issue leads to a critical difference between the goals of the networking team and the security team. Networking teams see the opportunity for traffic optimization by setting up another internet connection at the branch office, such as conventional business internet service. If the branch has internet breakout, the traffic path to cloud applications is much shorter, improving the performance of the application while reducing cost.

However, this traffic is not being inspected at all. The security team could implement the full stack of network security normally found at corporate gateways, but it may be difficult to deploy and operate at the branch, especially when there is no IT staffing at the office.

Mobile users face similar challenges. In the past, users needed to reach applications in the internal data center, driving the need for VPN gateways to tunnel traffic back to HQ. This traffic benefited from the security provided at HQ, but in most cases, the organization allows the user to choose when to connect, as well as use a split tunnel that routes only the traffic destined to the data center through the IPsec connection. Both conditions allow traffic to pass to the internet uninspected, as well as invisible to the security team.

Cloud-Based Web Gateways to Partially Inspect Traffic

	Security	Management	Performance	Notes
Cloud web gateways	Web traffic goes through gateway; non-web traffic not inspected or secured.	Separate policy and administration; no consolidated view of traffic.	Performance comes from limited inspection. Performance drops when based in hosted, collocated points of presence.	Does not replace a firewall. Only inspects a limited amount of traffic.

In recent years, the emergence of proxy servers hosted as secure web gateways has provided one approach to the problem of what to do about uninspected traffic passing out the split tunnel at the branch or mobile user's endpoint. Instead of performing full inspection of all network traffic, a web gateway examines traffic from a web browser and blocks websites and known malware. Organizations looking for a better option than no inspection may use this approach without having to deploy a hardware appliance at the branch.

Web gateways are not a substitute for a firewall. Partially inspecting traffic means the remaining traffic passes through uninspected, or else the application breaks. The organization remains blind to applications that legitimately use alternative ports as well as those intentionally evading inspection. Security is compromised because there is no inspection of non-browser traffic, nor protection against other portions of the attack lifecycle, such as secondary malware payloads or ongoing command-and-control traffic with a compromised endpoint.

The lack of full inspection means the organization may remain blind to critical issues. Separate security measures applied to headquarters traffic versus branch traffic introduce incongruity in enforcement of policy and a separate set of logs, making it difficult to track the path of a security incident that spans the organization.

DNS Filtering to Block Based on Domain Name

	Security	Management	Performance	Notes
DNS filtering	Only domain blocking known bad sites; no content inspection.	Separate policy and administration; no consolidated view of traffic.	Performance comes from the lack of inspection.	Ineffective at stopping malicious content or traffic.

DNS filtering is another approach organizations may try to improve security for remote locations and mobile users. By changing the DNS setting at the router or on the endpoint configuration, and rerouting DNS requests through a filtering service, the organization can set policies on what domain names resolve. DNS filtering stops a user's connection to a given site by not resolving certain categories of sites, such as those known to host malware, assuming that the vendor already knows ahead of time that the domain hosts malicious content.

However, these measures do not inspect traffic, leaving the organization in the dark about user activity. The organization only sees the sites users visit, and not the applications they use. Application traffic does not get inspected, leaving a significant hole in the ability to connect the dots as threats traverse the network.

DNS filtering cannot stop targeted attacks because it cannot tell if a previously unknown site is hosting malicious content. Without in-line inspection, it also cannot tell when a valid resource, such as a corporate file share or an internal site, is hosting malicious content or an exploit kit. From a security perspective, it remains trivial to bypass DNS filtering by simply using new, uncategorized domain names or avoiding DNS altogether by using IP addresses. The lack of traffic visibility creates issues with incident response and tracking down indicators of compromise because, when there is absolutely no information at many locations, it is impossible to correlate related events occurring in separate parts of the environment. Without being able to piece intelligence together, the organization remains blind to the big picture.

Requirements for Proper Security

Making the right decisions on security necessitates thinking about what requirements must be universally applied, regardless of location. Any compromise of these principles exposes the organization to risk.

- **Coverage:** Protection must be consistently enforced across all applications, across your network, through the cloud, and wherever your users and offices are.
- **Visibility:** Organizations must be able to see all traffic to make informed security decisions.
- **Enforcement:** Must be able to stop threats within network traffic as well as adapt to new threats.

These principles are key to the Palo Alto Networks® Next-Generation Security Platform. Customers can deploy next-generation firewalls to protect their office networks and data centers. This protection can be extended to other locations using GlobalProtect Large Scale VPN to set up branch office connections, and to users using GlobalProtect subscriptions on next-generation firewalls. IT teams can deploy the necessary firewalls in locations around the world, using either physical appliances or virtualized firewalls to build out the coverage to keep users and offices safe.

Getting appliances in remote areas can be difficult, especially when these offices do not have IT staff on hand. The technology for protection is available in the platform, but the organization may need help to stay on top of dynamic changes, such as office expansion and user growth in remote locations.

For these reasons, Palo Alto Networks now provides a new option to protect networks and users around the world: GlobalProtect cloud service.

Introducing GlobalProtect Cloud Service

The core issue is the growing distance between the firewall that can provide security, and the remote offices and users who need it. Traditional thinking assumed the only way to do this was to bring the traffic to the only location where the organization had security, namely the perimeter firewall. Instead of bringing the traffic back to headquarters, would it not make sense to move firewalls closer to remote offices and mobile workforces? This is the perfect use of the cloud: it provides a delivery model that brings the service to where it is needed.

GlobalProtect™ cloud service delivers upon this vision by helping security teams build out the right security architecture that prevents known and unknown threats at every corner of the extended network. Deploy the protection of the platform to remote locations and mobile users everywhere using a cloud-based security infrastructure.

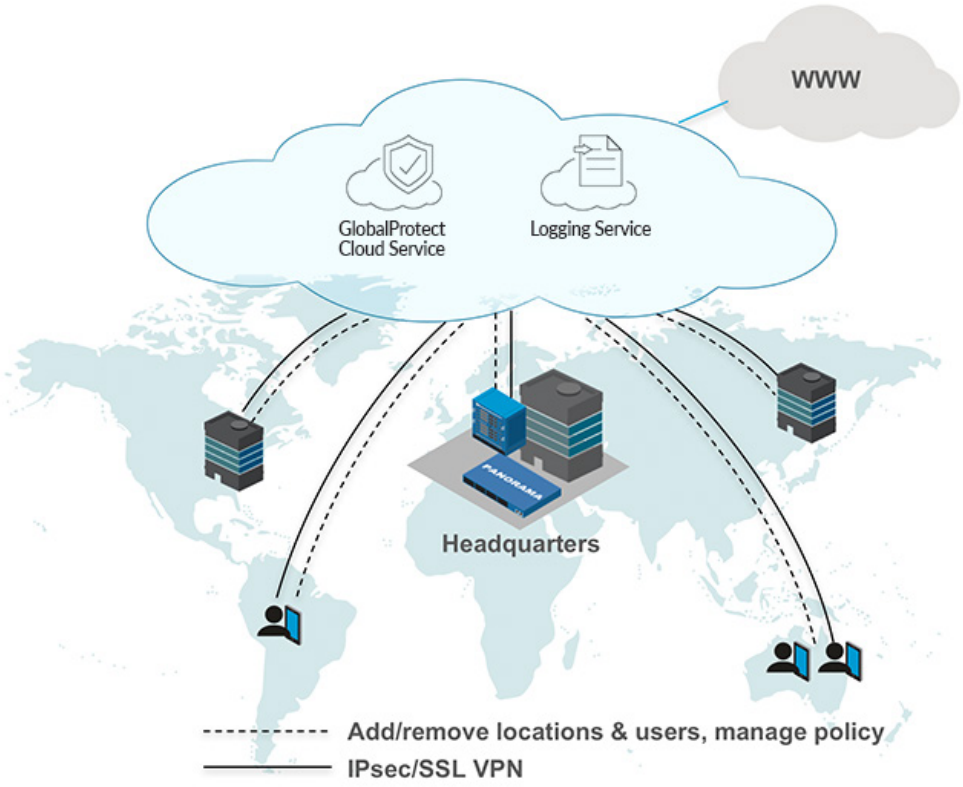
GlobalProtect cloud service delivers the coverage of the Next-Generation Security Platform to maintain visibility in traffic and the enforcement of security policy.

GlobalProtect provides service-based protection for both networks and users:

- **GlobalProtect cloud service for remote networks:** A cloud-based firewall secures traffic for remote branch offices. These firewalls provide the remote office with safe access to cloud and data center applications, along with a clean pipe to the internet.
- **GlobalProtect cloud service for mobile users:** GlobalProtect provides a network of firewalls to which users can connect. The GlobalProtect app automatically selects the best firewall available to access applications. User traffic and applications are protected by the entire suite of next-generation firewall features and capabilities.

GlobalProtect cloud service policies can be used to control access to and inspect all traffic from SaaS applications, the data center or the hybrid cloud. Organizations looking to apply more granular enforcement of cloud security policies can deploy GlobalProtect cloud service with Aperture™ SaaS security to safely enable SaaS-hosted content.

Panorama™ network security management seamlessly manages GlobalProtect cloud service policies in conjunction with all your existing physical and virtual firewalls. Your security paradigm remains consistent, thus eliminating the gap in security and operational challenges normally seen beyond the traditional perimeter.



Key GlobalProtect cloud service benefits:

- Secures the expanded perimeter without compromising security.
- Consolidates administration and management across the entire organization, driving operational efficiency.
- Reduces Capex by switching to a predictable Opex model.
- Maintains consistent security and full inspection of traffic for all locations and users.
- Works seamlessly alongside your existing physical and virtual firewalls.
- Easily add and remove coverage by provisioning firewalls in the cloud.

Protecting Branch Offices With GlobalProtect Cloud Service for Remote Networks

GlobalProtect cloud service allows you to protect your remote locations using our cloud-based next-generation security infrastructure. GlobalProtect cloud service minimizes the operational burden of protecting remote locations by allowing customers to focus on managing policies while we manage the infrastructure. Supported by the entire suite of PAN-OS® security features, including safe enablement of applications, user-based policies, Threat Prevention, URL Filtering and WildFire™ cloud-based threat analysis, GlobalProtect cloud service protects your distributed network more efficiently and cost-effectively than alternative "do-it-yourself" approaches.

The traffic at the branch office routes through GlobalProtect cloud service over an industry-standard IPsec VPN connection or via SD-WAN integration. Security teams provision coverage by adding and removing locations using Panorama, and establishing the IPsec tunnel to a termination device such as a router, firewall or SD-WAN at the remote location. Once connected, teams can use Panorama to manage policies and query Palo Alto Networks Logging Service, which stores the logs on activities occurring within GlobalProtect cloud service.

Within GlobalProtect cloud service, all sites are connected in a full mesh VPN configuration, without requiring any complex configuration at the site itself. Only an IPsec connection is required from the remote site to the cloud.

Panorama manages the firewalls within GlobalProtect cloud service in the same manner as it does existing devices. The firewalls in GlobalProtect cloud service for remote networks include subscriptions for Threat Prevention, PAN-DB, URL Filtering and WildFire, with AutoFocus™ contextual threat intelligence service and Aperture available as optional add-ons.

Use Cases for GlobalProtect Cloud Service for Remote Networks

- **Onboard each remote site with all traffic to cloud:** With a full IPsec tunnel set up between the remote office and the cloud, the organization benefits from full inspection of all network traffic. GlobalProtect cloud service provides secure internet access and routes traffic over a site-to-site connection for accessing applications in the data center.
- **Onboard remote sites by integrating with a head-end SD-WAN device:** SD-WAN solutions route traffic across multiple low-cost internet connections to reduce cost compared to traditional WAN links. Secure traffic by terminating the tunnels at GlobalProtect cloud service.

Protecting Mobile Workforces With GlobalProtect Cloud Service for Mobile Users

Mobile users pose a unique security challenge: they are not located near a corporate network, yet they still need to access a variety of cloud-, internet- and data center-based applications. The organization must find ways to maintain visibility into traffic and enforce security policy for users connecting from public networks and private homes.

GlobalProtect cloud service provides a network of cloud-based next-generation security gateways that secures traffic. Mobile workforces are distributed around the world, and GlobalProtect cloud service for mobile users establishes points of presence for them to use.

GlobalProtect cloud service works together with the GlobalProtect agent/app on laptops and mobile devices. When a remote user has internet connectivity, the GlobalProtect app locates the best gateway available for the user's location and sets up an IPsec/SSL VPN tunnel. All traffic passes through GlobalProtect cloud service, providing the user with the same network security protections to maintain visibility into traffic, enforce security policies, and stop known and unknown threats.

The flexibility of the cloud makes it simple to scale across a global footprint and adjust coverage as necessary. GlobalProtect automatically scales service up and down to handle the shifts in demand when conditions and traffic patterns change. Changes to configurations are transparent to end users, requiring no action on their part to automatically take advantage of new configurations.

Use Cases for GlobalProtect Cloud Service for Mobile Users

- **Augmenting Coverage:** Customers already using next-generation firewalls with GlobalProtect subscriptions can use GlobalProtect cloud service to augment coverage for mobile users. GlobalProtect cloud service provides the additional gateways organizations need, which work alongside those already in place. All gateways, whether on customer-managed firewalls or on GlobalProtect cloud service, can be used by end users interchangeably.
- **Transitioning from remote access to mobile workforce security:** Remote access is primarily based on the premise that users need access to internal resources. As such, all traffic must go back to a centralized location. To secure all traffic, the organization needs more firewalls in these users' locations. To get global coverage instantly, the organization can use GlobalProtect cloud service to provision the necessary gateways, greatly reducing the time to secure the user population.

- **New rollouts:** GlobalProtect cloud service greatly speeds up the deployment of the firewalls used to support always-on security configuration for protecting users. IT does not have to procure rack space, configure and ship physical appliances, or make capital expenditures to set up the infrastructure. With GlobalProtect cloud service, gateways are instantly provisioned, set up with auto-scaling, managed through Panorama, and ready for use with your security policies.

Using GlobalProtect Cloud Service for Securing SaaS Applications

Users at the branch office and off-premise need access to cloud-hosted applications. GlobalProtect cloud service delivers important prevention capabilities and policy controls to make SaaS safe.

GlobalProtect cloud service takes a holistic, prevention-first approach toward securing the cloud and SaaS applications. Armed with the ability to identify more than 2,300 applications in use, and by whom, your security teams have the power to make more informed security decisions and, more importantly, begin reducing your organization's attack surface area by enabling business applications based on user identity. GlobalProtect cloud service can stop malware in the cloud from infecting endpoints and stop command-and-control communication to attackers. The service can prevent the exfiltration of sensitive data across all apps, SaaS-based or not.

Complementing these application control and threat prevention capabilities is the ability to use Aperture with GlobalProtect cloud service to gain deep context into SaaS applications, such as user activity (upload/download/share), accounts (managed/consumer), sharing activity (internal/external), domains (trusted/non-trusted) and devices (managed/personal), along with surgical control across these granular contexts. Native integration with WildFire Threat Intelligence Cloud prevents known and unknown threats from spreading through SaaS applications.

Conclusion

Don't make the mistake of inadequately protecting your remote networks and mobile users. If security is your priority, it must cover every corner of your organization in the same manner. GlobalProtect cloud service makes it simple to deliver the necessary security to prevent attacks on your remote networks and mobile users. It is the only offering that provides the convenience of cloud-deployed firewalls that work hand in hand with management for perimeter and data center firewalls, making it possible to secure your entire network using a common management framework across all PAN-OS firewalls. It makes administration easy, allowing your team to zero in on critical issues more quickly. It reduces capital expenditure through predictable operational expenses. These capabilities streamline the work of your security team, allowing them to stay focused on the big picture for protecting your organization.

paloalto NETWORKS®

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

protecting-the-extended-perimeter-with-globalprotect-cloud-service-wp-060917