SECURING SD-WAN WITH THE SECURITY OPERATING PLATFORM

Palo Alto Networks delivers security to protect SD-WAN environments. GlobalProtect™ cloud service provides a unique, cloud-based environment that adapts to the dynamics of SD-WAN to stop threats and enable access to internal and cloud-based applications.

Balancing Network Optimization and Security

As organizations grow, they need to build out infrastructure to connect and secure branch offices in different geographic regions. This process is a delicate balancing act of aligning an organization's requirements for reliability, performance, and security while being mindful of capital expenses and ongoing operational costs. Deciding how to connect distant offices is not easy, because distance drives costs up and performance down. In addition, the shift toward deploying applications in the cloud increases the number of possible permutations to link users to applications and correspondingly creates new issues regarding whether security, performance, or cost takes precedence.

SD-WAN greatly benefits organizations looking for more flexibility to connect remote networks. Rather than routing all branch traffic through the internal core network, SD-WAN makes it possible to manage and deploy connections to branch offices and support business applications using commodity internet. However, even with the optimization of the network path over low-cost connections, the question of where to put the security remains.

Security Challenges for SD-WAN

Options for security in SD-WAN need to be as flexible as the networking, but traditional measures are not always easy to adapt. In a traditional campus network design, there is a full stack of network security appliances at the internet perimeter that can protect the branch, should all traffic be brought through the core network. The other option is to deploy network security appliances at the branch office, which complicates the design.

A better approach should bring the security closer to the branch office. Providing security from the cloud opens up new possibilities.

GlobalProtect Cloud Service

GlobalProtect cloud service delivers cloud-based security infrastructure for protecting remote networks and mobile users. It provides security by allowing organizations to set up regional protection for the SD-WAN fabric.

GlobalProtect cloud service provides the networking and security to enable business applications and internet access. SD-WAN devices at the branch establish IPsec tunnels to GlobalProtect cloud service for policy enforcement. These firewalls, managed by Palo Alto Networks and running your security policies, provide the same traffic inspection and threat prevention capabilities to all locations. In addition, GlobalProtect cloud service provides networking to headquarters and other branches as well as breakout to the internet.

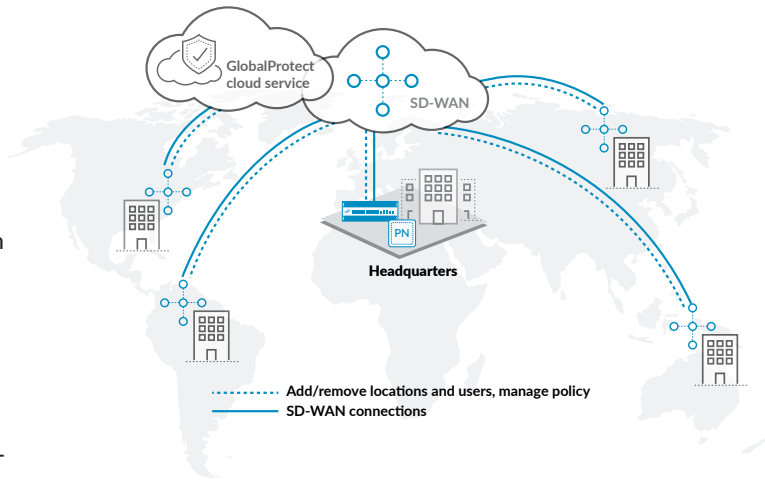

Figure 1: Protecting the SD-WAN fabric with GlobalProtect cloud service

Full Protection of the Security Operating Platform

Take advantage of the full capabilities of the platform, including:

- Safe enablement of applications
- App-ID™ technology

- User-ID™ technology
- Threat Prevention
- URL Filtering with PAN-DB
- WildFire® malware prevention service
- SSL/TLS decryption
- Credential theft prevention

WildFire is the world's largest distributed sensor system focused on identifying and preventing unknown threats, with more than 26,000 enterprise, government, and service provider customers contributing to the collective immunity of all other users. When it identifies novel malware or exploits, WildFire automatically creates and shares new prevention controls in as few as five minutes, without human intervention.

WildFire also forms the central prevention orchestration point for the Palo Alto Networks Security Operating Platform, allowing the enforcement of new controls across:

- Threat Prevention to block malware, exploits, and command-and-control (anti-C2 and DNS-based callback) activity.
- URL Filtering with PAN-DB to prevent newly discovered malicious URLs.
- AutoFocus™ contextual threat intelligence service to extract, correlate, and analyze threat intelligence with high relevance and context.
- Traps™ advanced endpoint protection and Aperture™ SaaS security service to determine verdicts and block threats in real time.
- Integration with our technology partners to determine verdicts on third-party services with the WildFire API.

Secure Access to Cloud and SaaS Applications

SD-WAN allows organizations to accelerate the adoption of SaaS applications. Key security issues organizations face include making sure sanctioned apps are used appropriately, allowing tolerated apps as long as there are protections in place to stop threat vectors, and enforcing policy to control access to unsanctioned applications.

GlobalProtect cloud service acts as the central point to maintain visibility into cloud applications, stop malicious content, and enforce security policy to control access to cloud applications.

Aperture, available as an addition to GlobalProtect cloud service, provides granular enforcement across all user, folder, and file activity within sanctioned SaaS applications, producing detailed usage analysis and analytics.

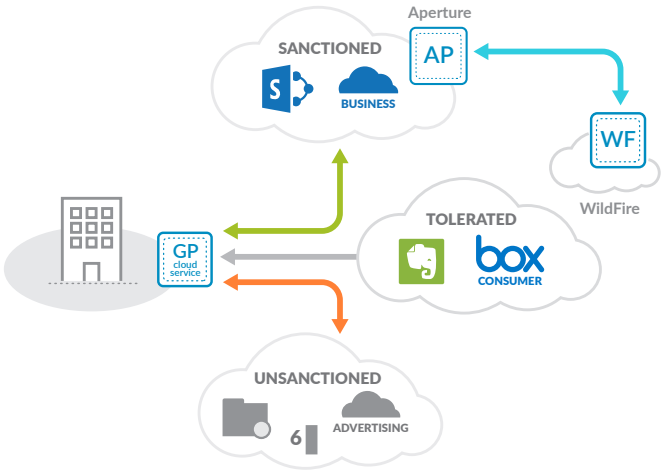

Figure 2: Accelerating adoption of SaaS applications via SD-WAN

Simplified Management

Centrally manage your SD-WAN security with Panorama™ network security management. Panorama enables you to control security on your distributed network from one central location.

Designed to Grow

As your wide area network grows, use GlobalProtect cloud service with hardware and virtualized firewalls to meet different deployment requirements at your perimeter, data center, branch office, and cloud. Mix and match your deployments to meet your changing requirements by sharing common management, reporting tools, and logging for seamless enforcement of security policy at every corner of your network.

Integration with SD-WAN

You can connect your remote and edge networks to GlobalProtect cloud service via an on-premises IPsec VPN-capable device, or you can utilize a technology integration partner that supports SD-WAN or IPsec VPN connectivity options. GlobalProtect cloud service integration partners include Aruba Networks, a Hewlett Packard Enterprise company; CloudGenix; Nuage Networks from Nokia; Viptela; VMware NSX SD-WAN by VeloCloud. These GlobalProtect cloud service technology partners join existing SD-WAN technology partners who have integrated with our next-generation firewall, including Ecessa Edge, Riverbed Technology, Silver Peak Systems, and Talari Networks.

3000 Tannery Way
Santa Clara, CA 95054

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

www.paloaltonetworks.com

securing-sd-wan-with-palo-alto-networks-next-generation-securing-platform-sb-012519