Palo Alto Networks and Citrix SD-WAN

Palo Alto Networks and Citrix SD-WAN

The increasing adoption of cloud-hosted applications, including the move to SaaS, is causing enterprise IT to evaluate alternatives to inefficient backhauling of Internet traffic over costly legacy WAN architecture. The ability to breakout Internet traffic out from the branch is critical to delivering a more reliable, low-latency user experience. To avoid introducing a costly security stack at each branch, a more cost-effective and simpler model is needed. The partnership between Palo Alto Networks and Citrix now offers distributed enterprises a more reliable and secure way to connect users in branches to applications in the cloud.

Citrix SD-WAN provides a comprehensive solution for enterprise application delivery to branches, whether it is from the datacenter, from public clouds or SaaS. Citrix SD-WAN identifies applications through a combination of an integrated database of over 4,000 applications, including individual SaaS applications, and uses deep packet inspection technology for real-time discovery and classification of applications. It uses this application knowledge to intelligently steers traffic from the branch to the Internet, cloud or SaaS.

Palo Alto Networks' 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, cloud-based firewalls that protect the SD-WAN fabric. GlobalProtect cloud service provides the networking and security to enable business applications and Internet access. Citrix SD-WAN devices at the branch establish IPsec tunnels to regional firewall in GlobalProtect cloud service for policy enforcement. These firewalls, managed by Palo Alto Networks and running the customer's security policies, provide the same traffic inspection and threat prevention capabilities as any other Palo Alto Networks next-generation firewall (NGFW). In addition, GlobalProtect cloud service provides networking to headquarters, other branches and breakout to the Internet.

By partnering with Palo Alto Networks, GlobalProtect cloud service in combination with Citrix SD-WAN offers enterprises a cloud-based secure web gateway for centralizing and simplifying policy management of next-gen security for branch users worldwide. GlobalProtect cloud service provides NGFW for Internet traffic from the branch to reduce the overhead of having to manage firewalls at the branches. Because Citrix SD-WAN provides the ability to route traffic from the branch to the Internet via GlobalProtect cloud service, there is no longer the need to deploy firewalls at the branches.

How the Joint Solution Works

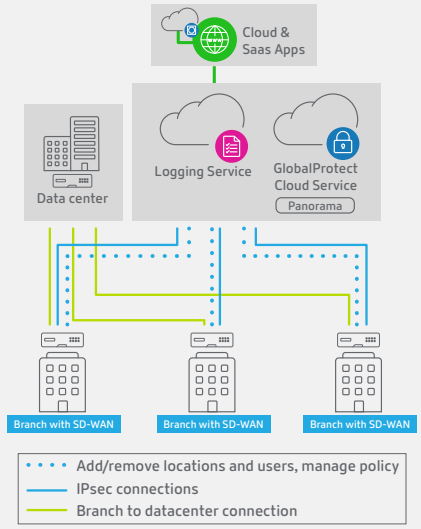
Citrix SD-WAN customers establish IPsec tunnels from their branches and redirect their Internet traffic to GlobalProtect cloud service, which has their integrated next-gen firewalls. The Citrix SD-WAN public IP address is provided to Palo Alto Networks GlobalProtect cloud service where their public IP address and all crypto suits such as IPsec encryption and authentication algorithms are added. This allows GlobalProtect cloud service to inspect real-time application content for data theft and malware protection while URL filtering identifies and controls access to web traffic, intrusion detection service looks for malicious activity in the network, and intrusion protection

determines what actions should be taken on the malicious traffic using defined policies. It uses deep packet inspection to identify all the applications, not just based on the ports, and can identify users to ensure proper authentication.

Supported by the entire suite of security features and subscriptions based on PAN-OS®, GlobalProtect cloud service allows you to implement a prevention philosophy that protects remote networks and mobile users with the same security functionality that protects your network. The Palo Alto Networks Panorama configuration management portal offers IT a centralized way to efficiently add and remove users and locations and configure and manage the firewall. In addition, Palo Alto Networks has the ability to configure any firewall policies requested from an enterprise reducing OPEX by eliminating this management task.

IPsec crypto suites are configured on GlobalProtect cloud service using Panorama, and IPsec Peer (GlobalProtect cloud service IP) and related IPsec Crypto Suite are configured on Citrix SD-WAN.

General Deployment



Key Benefits of the GlobalProtect cloud service Solution:

- **Scalability and Resilience:** GlobalProtect cloud service leverages a cloud-based infrastructure, allowing you to avoid the challenges of sizing firewalls and compute resource allocation, minimizing coverage gaps or inconsistencies associated with your distributed organization. The elasticity of the cloud scales as demand shifts and traffic patterns change. All GlobalProtect cloud service locations are connected through a full mesh VPN without the complexity of configuration, since the only IPsec connection required is from the remote site to the cloud. GlobalProtect cloud service does the rest.
- **Logging and Reporting:** Supporting GlobalProtect cloud service is a cloud-based logging service that can be used to collect all logs generated by remote networks and mobile users. Using Panorama, you can query Palo Alto Networks Logging Service for analysis, report generation or incident forensics.
- **Identify applications, not ports:** Using deep packet inspection, GlobalProtect cloud service identifies all applications, across all ports, irrespective of protocol, SSL encryption, or evasive tactic. The application identification is the basis for applying all of the security policies.
- **Identify users, not just IP addresses:** GlobalProtect cloud service provides user identification to check for proper authentication leveraging information stored in enterprise directories for visibility, policy creation, reporting, and forensic investigation.
- **Inspects content in real-time:** Intrusion prevention technology provides identification of attacks and malware embedded in application traffic in the network (at low-latency, high throughput speeds) and then determines what action to be taken for protection of the network.
- **Policy consistency with centralized management:** GlobalProtect cloud service is managed using the same Panorama deployment that manages Palo Alto Networks' physical or virtualized next-generation firewalls. The ability to create and deploy consistent policies for your remote networks using objects in place for your existing firewall deployment further enhances visibility and operational efficiencies.
- **Deliver multi-gigabit throughput:** Combine high performance hardware and software in a purpose-built platform to enable low latency, multi-gigabit performance with all services enabled.

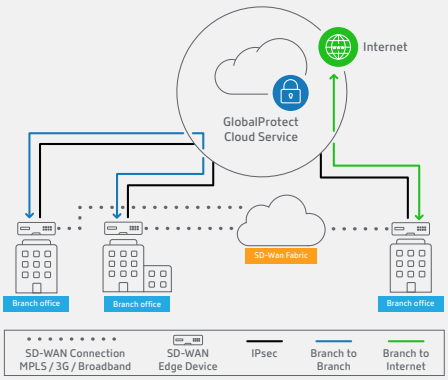
Deployment Scenarios

Branch-to-Internet and Branch-to-Branch

For direct Internet breakout from the branch to the Internet, branch traffic will go through GlobalProtect cloud service before heading out to the Internet.

For branch-to-branch communication, we'll specify the IPsec policies go through GlobalProtect cloud service first through an IPsec tunnel. GlobalProtect cloud service determines if it's getting traffic from branch 1, and then sends it to branch 2 via an IPsec tunnel by creating policies.

Branch-to-Internet and Branch-to-Branch

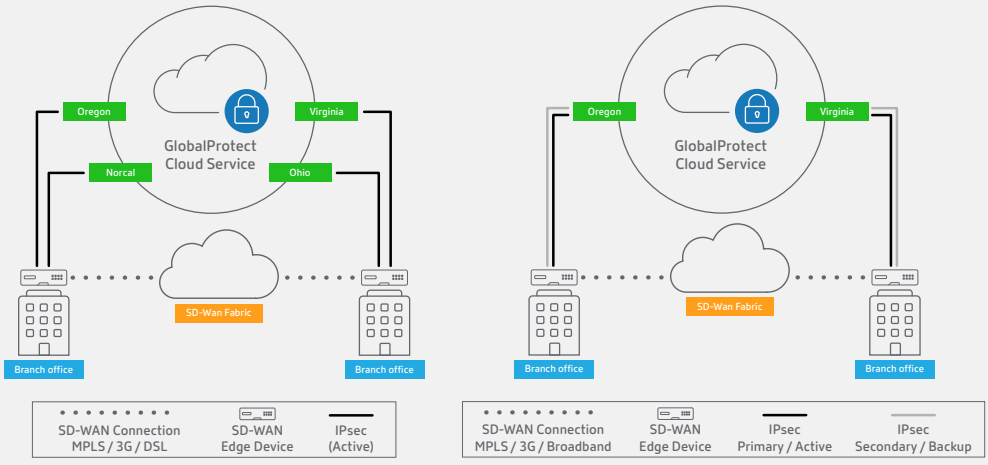


Active-Active and Active-Passive Tunnels

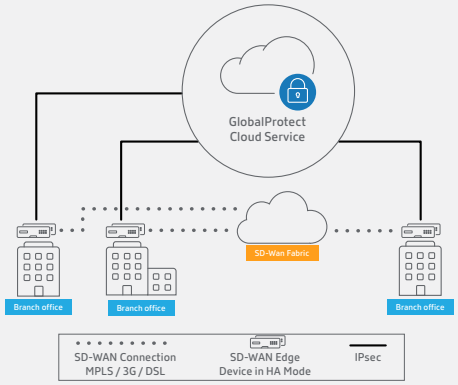
For active/active tunnels from a branch, two IPsec tunnels to GlobalProtect cloud service are established using Citrix SD-WAN for sending different types of traffic through different tunnels based on policies. For multiple destination protected networks, SD-WAN can load balance traffic towards GlobalProtect cloud service using active-active IPsec tunnels.

For active/passive, two IPsec tunnels are established with same parameters and the same protected networks to GlobalProtect cloud service and only one tunnel will be active all the time. This allows tunnels to be available all the time for redirecting Internet traffic by configuring IPsec protected networks.

Active-Active and Active-Passive Tunnels



SD-WAN Edge Device in HA Mode



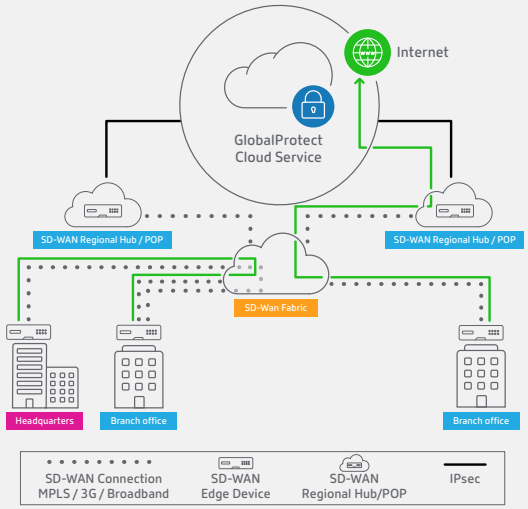
SD-WAN Edge Device in HA Mode

IT can configure SD-WAN in high-availability (HA) mode by establishing an IPsec tunnel from each branch to GlobalProtect cloud service. Traffic redirection from SD-WAN to GlobalProtect cloud service will always happen through the active appliance. If there is an HA event, the secondary SD-WAN appliance will take over and start sending traffic to GlobalProtect cloud service.

SD-WAN Branch to GlobalProtect cloud service via Regional Hub / Data center

Establish an IPsec tunnel to GlobalProtect cloud service from a regional SD-WAN hub/datacenter by configuring the branch SD-WAN devices to redirect Internet traffic towards the regional hub/datacenter. From the regional hub/datacenter, all the Internet traffic will then be sent through an IPsec tunnel to GlobalProtect cloud service.

SD-WAN Branch to GlobalProtect cloud service via Regional Hub / Data center



Citrix SD-WAN ensures branch users have reliable, secure, and simplified access to all their applications, delivered from the cloud or SaaS, in order to be productive.

Learn more at citrix.com/sdwan

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States