STRATA™
BY PALO ALTO NETWORKS

SD-WAN Subscription on the Next-Generation Firewall

Easily adopt an end-to-end SD-WAN architecture with natively integrated, world-class security and connectivity

Benefits

- Implement SD-WAN safely with natively integrated, industry-leading security.
- Adopt SD-WAN easily by enabling it on your existing firewalls and consuming Prisma Access SD-WAN hub as a service.
- Deliver an exceptional end-user experience by leveraging Prisma Access SD-WAN hub to optimize performance.

The effects of the cloud on network and security transformation are undeniable. As the number of devices at branch locations grows and applications become more bandwidth-intensive, businesses are forced to spend more to accommodate demand. As a result, traditional wide area network (WAN) architectures with multiprotocol label switching (MPLS), which tend to eat up bandwidth as they backhaul traffic from branches to the cloud, render legacy approaches ineffective.

Software-defined wide area networking (SD-WAN), an approach that uses commodity links and allows you to intelligently manage as well as control connectivity between branches and cloud instances, is now a necessity for distributed enterprises. According to Gartner, by 2023, more than 90% of WAN edge infrastructure refreshes will be based on vCPE platforms or SD-WAN vs. traditional routers.[1] However, with its benefits, SD-WAN also brings many challenges, such as lack of security, unreliable performance, and complexity. When security is an afterthought, it tends to be either subpar or bolted on, introducing management complexity. Moreover, network performance becomes less reliable because enterprises use the congested internet as the WAN middle mile—and when they try to address this by building their own SD-WAN hub infrastructures, they run into complexity. Ultimately, enterprises turn to multiple vendors or service providers to solve performance issues, which increases costs while decreasing control and visibility.

Secure SD-WAN by Palo Alto Networks

Palo Alto Networks SD-WAN offering lets you easily adopt an end-to-end SD-WAN architecture with natively integrated, world-class security and connectivity. Using Prisma™ Access as the SD-WAN hub, you can optimize the performance of your entire network. This minimizes latency and ensures reliability, resulting in an exceptional user experience at the branches. You can consume our secure Prisma Access SD-WAN hub as a service, eliminating the complexity of building your SD-WAN hub infrastructure, or you can build the hub and interconnect infrastructure yourself using Palo Alto Networks Next-Generation Firewalls. Regardless of your deployment model, our tight integration will allow you to manage security and SD-WAN on a single, intuitive interface.

Optimized Connectivity for Improved User Experience

Palo Alto Networks SD-WAN lets you measure and monitor specific paths as well as dynamically move sessions to the optimal path, guaranteeing the best branch user experience. You can simply enable the SD-WAN subscription on your Next-Generation Firewalls and begin intelligently, securely routing branch traffic to your cloud applications.

Greater Performance with SD-WAN Hub

SD-WAN leverages commodity links, such as broadband internet, LTE, and more. However, while these links are cost-effective, they lack the reliable performance of dedicated, private links.

With Prisma Access acting as the SD-WAN hub, users can essentially go through a private network, bypassing the congested, unpredictable internet. By using a reliable, cloud native global backbone as your WAN middle mile, you ensure the best performance and user experience.

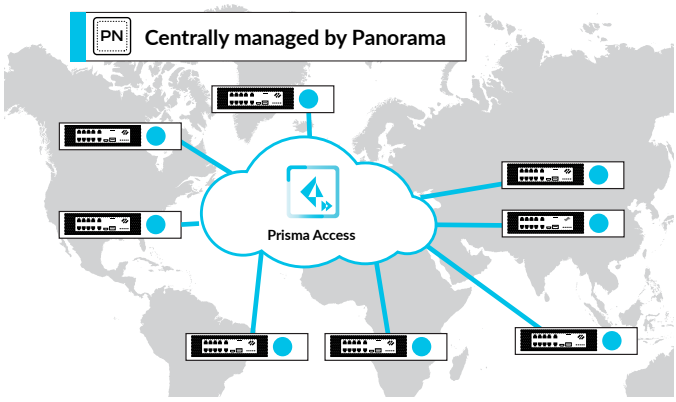

Figure 1: Palo Alto Networks SD-WAN cloud-based approach

Central Management for Security and Connectivity

Eliminate the need to manage multiple, disparate consoles from different vendors by using Panorama™ network security management for both security and connectivity. Integrated SD-WAN configuration and monitoring allows you to leverage the familiar Panorama user and application workflow, cutting the time you need to spend reconfiguring policies and visualizations. Additionally, you get granular SD-WAN monitoring data and a dedicated configuration tree, giving you greater visibility into your network.

Simplified Branch Onboarding

Provisioning a new branch requires IT staff to configure and deploy appliances. Doing this on a large scale, and at distributed locations, makes branch onboarding costly and slow.

With zero touch provisioning (ZTP), you can automate tedious onboarding processes. Appliances can be drop-shipped to your branch locations, where they are powered up and connected to the internet. To complete onboarding, administrators simply need to register on a web portal. Then, administrators can immediately start managing deployment and configuration from a single location through Panorama.

Flexible Deployment Options

Palo Alto Networks supports multiple SD-WAN deployment options, including mesh, hub-and-spoke, and cloud-based deployments. Furthermore, you can consume Prisma Access SD-WAN hub as a service or simply enable the SD-WAN subscription on your Next-Generation Firewalls.

1. Christian Canales, Andrew Lerner, Mike Toussaint, and Joe Skorupa, "Magic Quadrant for WAN Edge Infrastructure," Gartner, October 18, 2018, https://www.gartner.com/en/documents/3891709/magic-quadrant-for-wan-edge-infrastructure.

SD-WAN Software Licenses

- (Required) SD-WAN subscription on all physical appliances that will participate in the SD-WAN deployment. This license requires PAN-OS® 9.1.
- (Required to use Prisma Access for SD-WAN hub) Prisma Access SD-WAN Branch Interconnect license.

Table 1: Palo Alto Networks SD-WAN Supported Features and Capabilities

Category	Features
AAA/Authentication	RADIUS, local authentication and authorization, multitenant 3-tier RBAC architecture, auditing, roles and privileges
Availability	Hardware high availability in active/passive mode
SD-WAN features	• Link metric collection, jitter, drop, delay • Intelligent path selection based on metric; dynamic application steering • Application and network condition aware sub-second steering • Session-based link aggregation • Scalable bidirectional path health measurements, QoS, traffic shaping • Predefined application thresholds for common application categories • Forward error correction (FEC) • Packet duplication • SaaS application path monitoring: end-to-end application monitoring from the branch to the SaaS app server
Network services	IPv4, DNS, DHCP client, DHCP server, DHCP relay, NAT
Dynamic QoS/traffic shaping	QoS shaping, policing, and rate limiting with per-flow queueing and separate cleartext and tunnel treatment. Support for 8 queues, type of service (ToS), and DSCP code points with patented bidirectional session-based DSCP tagging.

Routing	• Static routes
	• OSPF
	• BGP
	  • Local route ID and local AS, path selection, BGP confederations, route flap dampening, graceful restart, IGP-BGP route injection
	  • Route import, export, and advertisement; prefix-based filtering; address aggregation
	• Multiple virtual routers
	• Authentication by MD5

SD-WAN high availability	Active/passive HA; dual power supply
Connectivity architecture	Hub-and-spoke IPsec tunnels with automatic configuration
Management	Single pane of glass for security and SD-WAN management • Panorama-managed, API, syslog, SNMP • RBAC • Scale up to 5,000 devices per Panorama • Zero touch provisioning (ZTP)* • Monitoring and visualization • Dashboard views of SD-WAN impacted applications and links with drill down • SD-WAN link down alerts to detect blackout situations • SD-WAN reporting • Link jitter, delay, and drop trend charts
Deployment flexibility	• Physical and virtualized Next-Generation Firewalls for both branch and hub • Hub-and-spoke • Mesh† • Cloud-delivered with CloudGenix and Prisma Access

* Coming soon with new SKUs.
† Coming soon.

Table 2: SD-WAN Device Specifications*				
	PA-220	PA-220R	PA-820	PA-850
Branch office bandwidth (recommended range)	1–150 Mbps	1–150 Mbps	50–500 Mbps	50–700 Mbps
Max. overlay IPsec tunnels	1K	1K	1K	1K
IPsec overlay performance with App-ID	290 Mbps	290 Mbps	870 Mbps	1 Gbps
Max. concurrent sessions	64K	64K	128K	196K
Max. number of routes	2.5K	2.5K	5K	5K
Appliance datasheet	Learn more	Learn more	Learn more	Learn more
Connectivity Options				
LAN/WAN 1G RJ-45	8	6	4	4
LAN/WAN 1G SFP	—	2	8	4
LAN/WAN 1G/10G SFP	—	—	—	4
LAN/WAN 40G QSFP	—	—	—	—
Serial console port USB console port Management port	1	1	1	1
HA—dual power input	Optional	Optional	No	Yes

*Any appliance can be used as a hub or branch.

Table 3: SD-WAN Device Specification*										
	PA-3220	PA-3250	PA-3260	PA-5220	PA-5250	PA-5260	PA-5280	VM-300	VM-500	VM-700
IPsec overlay performance with App-ID	2.0 Gbps	2.3 Gbps	3.5 Gbps	7.4 Gbps	15.2 Gbps	21.8 Gbps	21.8 Gbps	1.8 Gbps	4 Gbps	6.1 Gbps
Max. overlay IPsec tunnels	2K	3K	3K	3K	4K	5K	5K	1K	1K	8K
Max. concurrent sessions	1M	2M	3M	4M	8M	32M	32M	819,200	2M	10M
Max. number of routes	16K	16K	44K	100K	100K	100K	100K	10K	32K	100K
Appliance datasheet	Learn more	Learn more	Learn more	Learn more	Learn more	Learn more	Learn more	Learn more	Learn more	Learn more
Connectivity Options										
LAN/WAN 1G/10G SFP	8	8	8	16	16	16	16	—	—	—
LAN/WAN 40/100G QSFP28	—	—	4	4 (40G only)	4	4	4	—	—	—
Serial console port Management port	1	1	1	1	1	1	1	—	—	—
HA—dual power input	Optional	Optional	Optional	Yes	Yes	Yes	Yes	—	—	—

*Any appliance can be used as a hub or branch.

To compare performance and specifications for all our firewall offerings, visit paloaltonetworks.com/products/product-selection.

paloalto 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