STRATA™
BY PALO ALTO NETWORKS

SD-WAN-Abonnement in der Next-Generation Firewall

Einfache Implementierung einer lückenlosen SD-WAN-Architektur mit nativ integrierten, erstklassigen Sicherheits- und Verbindungsfunktionen

Vorteile

- Sichere SD-WAN-Implementierung mit nativer Integration in branchenführendes Sicherheitssystem
- Einfache SD-WAN-Integration durch Aktivierung in Ihren bestehenden Firewalls und Nutzung des SD-WAN-Hubs Prisma Access als Service.
- Ausgezeichnete Endbenutzer-erfahrung durch Einsatz des SD-WAN-Hubs Prisma Access zur Optimierung der Leistung

Die Cloud trägt eindeutig zur Optimierung von Netzwerk und Sicherheit bei. Durch die steigende Anzahl von Geräten in den Zweigstellen und immer bandbreitenintensivere Anwendungen entstehen für Unternehmen immer größeren Ausgaben, um der Nachfrage gerecht zu werden. Traditionelle WAN-Architekturen (WAN = Wide Area Network) mit Multiprotocol Label Switching (MPLS), die hohe Bandbreiten für den Rücktransport des Datenverkehrs von den Zweigstellen zur Cloud verbrauchen, machen ältere Ansätze obsolet.

Der SD-WAN-Ansatz (SD-WAN = Software-defined Wide Area Networking) verwendet Standardlinks und ermöglicht das intelligente Verwalten und die Steuerung der Konnektivität zwischen Zweigstellen und Cloud-Instanzen. Für verteilte Unternehmen ist er mittlerweile unverzichtbar. Laut einer Studie von Gartner werden bis 2023 über 90 % der WAN-Infrastrukturaktualisierungen auf vCPE-Plattformen oder SD-WAN basieren statt auf traditionellen Routern.1 Neben vielen VorteilenbringtSD-WANallerdingsaucheinigeHerausforderungen mit sich, wie zum Beispiel mangelnde Sicherheit, unzuverlässige Leistung und eine komplexe Bereitstellung. Wenn Sicherheit nicht prioritär behandelt wird, entstehen suboptimale Situationen oder es müssen nachträgliche Ergänzungen erfolgen, was zu komplexer Verwaltung führt. Darüber hinaus macht das überlastete Internet als WAN-Übertragungsweg die Netzwerkleistung weniger zuverlässig. Der Aufbau einer eigenen SD-WAN-Infrastruktur bedeutet für Unternehmen jedoch ein Mehr an Komplexität. Leistungseinbußen werden dann meist durch mehrere Anbieter oder Serviceprovider gelöst. Das führt jedoch zu höheren Kosten und beeinträchtigt Steuerung und Transparenz.

Sicheres SD-WAN von Palo Alto Networks

Mit der SD-WAN-Lösung von Palo Alto Networks können Sie ganz einfach eine lückenlose SD-WAN-Architektur mit nativ integrierten erstklassigen Sicherheits- und Verbindungsfunktionen implementieren. Mit Prisma™ Access als SD-WAN-Hub lässt sich die Leistung ihres gesamten Netzwerks steigern. Durch Minimierung der Latenz und eine höhere Zuverlässigkeit sorgen Sie so für eine hervorragende Benutzererfahrung in Ihren Zweigstellen. Wenn Sie Prisma Access als Service nutzen, brauchen Sie sich nicht um den Aufbau einer komplexen SD-WAN-Infrastruktur zu kümmern. Sie können den Hub und die entsprechende Infrastruktur auch selbst einrichten und die Next-Generation Firewalls von Palo Alto Networks nutzen. Ganz gleich, welches Bereitstellungsmodell Sie wählen: Dank der nahtlosen Integration können Sie die Sicherheitsfunktionen und das SD-WAN über eine einzige benutzerfreundliche Oberfläche verwalten.

Optimierte Konnektivität für eine verbesserte Benutzererfahrung

Mit dem Palo Alto Networks SD-WAN lassen sich bestimmte Pfade messen und überwachen sowie Sitzungen dynamisch dem optimalen Pfad zuweisen. So gewährleisten Sie eine optimale Benutzererfahrung in den Zweigstellen. Sie können das SD-WAN-Abonnement ganz einfach über die Next-Generation Firewalls aktivieren, um den Datenverkehr aus den Zweigstellen sicher zu ihren Cloud-Anwendungen zu leiten.

Bessere Leistung mit SD-WAN-Hub

SD-WAN nutzt Standardlinks wie Breitbandinternet, LTE und andere. Diese Links sind zwar kosteneffizient, bieten jedoch nicht die Zuverlässigkeit von dezidierten, privaten Links.

Mit Prisma Access als SD-WAN-Hub können Sie private Netzwerke

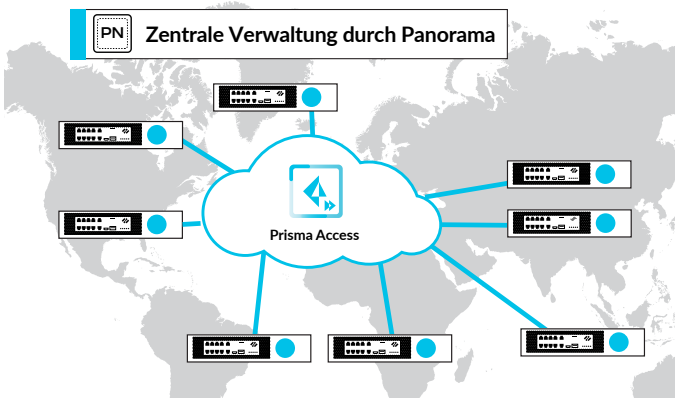

Abbildung 1: Cloudbasierter Ansatz mit dem SD-WAN von Palo Alto Networks

nutzen und das überlastete und unberechenbare Internet umgehen. Durch die Nutzung eines verlässlichen cloudnativen Backbones als „Mitte“ des Übertragungswegs sorgen Sie für höchste Leistung und eine optimale Benutzererfahrung.

Zentrale Verwaltung und sichere Konnektivität

Nutzen Sie das Panorama™-Netzwerksicherheitsmanagement für eine sichere Konnektivität und verzichten Sie auf verstreute Konsolen von verschiedenen Anbietern. Durch die integrierte SD-WAN-Konfiguration und Steuerung profitieren Sie vom vertrauten Benutzer- und Anwendungsworkflow von Panorama. Das verkürzt die Neukonfigurierung von Visualisierungen und Richtlinien.

Darüber hinaus bieten Ihnen die detaillierten SD-WAN-Überwachungsdaten und der dezidierte Konfigurationsbaum mehr Transparenz für Ihr Netzwerk.

Vereinfachtes Onboarding

Für die Einrichtung einer neuen Zweigstelle müssen Appliances konfiguriert und bereitgestellt werden. Bei umfangreichen Architekturen und verstreuten Zweigstellen wird das Onboarding zeit- und kostenaufwendig.

Mit der einfachen, automatisierten Bereitstellung (Zero Touch Provisioning, ZTP) werden langwierige Onboarding-Prozesse automatisch durchgeführt. Appliances können direkt zu Ihren Zweigstellen geliefert werden, wo sie eingeschaltet und mit dem Internet verbunden werden. Um das Onboarding abzuschließen, brauchen die Administratoren sich nur über ein Webportal anzumelden. Installation und Konfiguration lassen sich dann umgehend von einem zentralen Standort aus über Panama verwalten.

Flexible Optionen

Palo Alto Networks unterstützt verschiedene SD-WAN-Umgebungen, darunter Mesh-Netzwerke, Hub-and-Spoke- sowie cloudbasierte Umgebungen. Darüber hinaus können Sie den SD-WAN-Hub Prisma Access als Service nutzen oder einfach das SD-WAN-Abonnement über Ihre Next-Generation Firewalls aktivieren.

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

SD-WAN-Softwarelizenzen

- (Erforderlich) SD-WAN-Abonnement für jede Hardwaregerät, das Teil der SD-WAN-Umgebung ist. Diese Lizenz erfordert PAN-OS® 9.1.
- (Bei der Nutzung von Prisma Access für den SD-WAN-Hub erforderlich) Lizenz für Zweigstellenvernetzung mit Prisma Access SD-WAN.

Tabelle 1: Unterstützte Funktionen und Merkmale des SD-WAN von Palo Alto Networks

Kategorie	Merkmal
AAA/Authentifizierung	RADIUS, lokale Authentifizierung und Autorisierung, mandantenfähige dreistufige RBAC-Architektur, Auditing, Rollen und Privilegien
Verfügbarkeit	Hohe Verfügbarkeit der Hardware im Aktiv-/Passivmodus
SD-WAN-Merkmale	• Erfassung von Linkmetriken, Jitter, Drop, Delay • Metrikbasierte intelligente Pfadauswahl; dynamische Anwendungssteuerung • Sub-Second Steering für Anwendungs- und Netzwerkbedingungen • Sessionbasierte Link Aggregation • Skalierbare, bidirektionale Messungen der Pfadzustände, QoS, Traffic Shaping • Vordefinierte Schwellenwerte für gängige Anwendungskategorien • Korrektur von Weiterleitungsfehlern (Forward Error Correction, FEC) • Paketduplizierung • Pfadüberwachung für SaaS-Anwendungen: lückenlose Überwachung der Anwendungen von der Zweigstelle bis zum SaaS-App-Server
Netzwerkdienste	IPv4, DNS, DHCP-Client, DHCP-Server, DHCP-Relay, NAT
Dynamisches QoS/Traffic Shaping	QoS Shaping, Richtlinienanwendung und Ratenlimitierung mit Per-Flow Queueing, separatem Klartext und Tunnelbehandlung; Unterstützung für acht Queues, Leistungsart (Type of Service, ToS) und Differentiated Services Code Point (DiffServ-Codepunkt, DSCP) mit patentierter, bidirektionaler, sitzungsbasierter DSCP-Markierung

Routing	• Statische Routen
	• OSPF
	• BGP
	  • Lokale Route-ID und lokales AS, Pfadauswahl, BGP-Konföderationen, Route Flap Dampening, unterbrechungsfreier Neustart, IGP-BGP-Route-Injection
	  • Routeimport, Routeexport und Werbung; präfixbasierte Filterung, Adressaggregation
	• Mehrere virtuelle Router
	• Authentifizierung durch MD5

Hohe SD-WAN-Verfügbarkeit	Aktiv-/Passiv-HA; duale Stromzufuhr
Konnektivitätsarchitektur	Hub-and-Spoke-IPsec-Tunnel mit automatischer Konfiguration
Management	Ganzheitliche Übersicht des SD-WAN-Sicherheitsmanagements • Ganzheitliche Übersicht des SD-WAN-Sicherheitsmanagements • Panorama-Management, API, syslog, SNMP • RBAC • Bis zu 5.000 Geräte pro Panorama • Automatisierte Bereitstellung (Zero Touch Provisioning, ZTP)* • Überwachung und Visualisierung • Dashboard-Ansicht der SD-WAN-betroffenen Anwendungen und Links mit Drilldown • Warnungen bei Ausfall des SD-WAN-Links zur Erkennung von Blackouts • SD-WAN-Berichte • Trendverläufe zu Link-Jitter, -Drop, -Delay
Flexible Bereitstellung	• Physische und virtualisierte Next-Generation Firewalls für Zweigstelle und Hub • Hub-and-Spoke • Mesh† • Cloudbasiert mit CloudGenix und Prisma Access

* Demnächst mit neuen Artikelnummern erhältlich.
† Demnächst erhältlich.

Tabelle 2: SD-WAN-Gerätespezifikationen				
	PA-220	PA-220R	PA-820	PA-850
Bandbreite in der Zweigstelle (empfohlener Bereich)	1/150 Mbit/s	1/150 Mbit/s	50/500 Mbit/s	50/700 Mbit/s
Max. Overlay der IPsec-Tunnel	1.000	1.000	1.000	1.000
IPsec-Overlay-Leistung mit App-ID	290 Mbit/s	290 Mbit/s	870 Mbit/s	1 Gbit/s
Max. simultane Sitzungen	64.000	64.000	128.000	19.000
Max. Routenanzahl	2.500	2.500	5.000	5.000
Appliancedatenblatt	Mehr erfahren	Mehr erfahren	Mehr erfahren	Mehr erfahren
Konnektivität				
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	—	—	—	—
Serieller Konsolenport USB-Konsolenport Managementport	1	1	1	1
HA – dualer Stromeingang	Optional	Optional	Nein	Ja

*Jede Appliance als Hub oder Zweigstelle nutzbar

Tabelle 3: SD-WAN-Geräte-Spezifikationen*										
	PA-3220	PA-3250	PA-3260	PA-5220	PA-5250	PA-5260	PA-5280	VM-300	VM-500	VM-700
IPsec Overlay-Leistung mit App-ID	2,0 Gbit/s	2,3 Gbit/s	3,5 Gbit/s	7,4 Gbit/s	15,2 Gbit/s	21,8 Gbit/s	21,8 Gbit/s	1,8 Gbit/s	4 Gbit/s	6,1 Gbit/s
Max. Overlay der IPsec-Tunnel	2.000	3.000	3.000	3.000	4.000	5.000	5.000	1.000	1.000	8.000
Max. simultane Sitzungen	1 Mio.	2 Mio.	3 Mio.	4 Mio.	8 Mio.	32 Mio.	32 Mio.	819.200	2 Mio.	10 Mio.
Max. Routenanzahl	16.000	16.000	44.000	100.000	100.000	100.000	100.000	10.000	32.000	100.000
Appliance-datenblatt	Mehr erfahren	Mehr erfahren	Mehr erfahren	Mehr erfahren	Mehr erfahren	Mehr erfahren	Mehr erfahren	Mehr erfahren	Mehr erfahren	Mehr erfahren
Konnektivität										
LAN/WAN 1G/10G SFP	8	8	8	16	16	16	16	—	—	—
LAN/WAN 40/100G QSFP28	—	—	4	4 (nur 40G)	4	4	4	—	—	—
Serieller Konsolenport Managementport	1	1	1	1	1	1	1	—	—	—
HA – dualer Stromeingang	Optional	Optional	Optional	Ja	Ja	Ja	Ja	—	—	—

*Jede Appliance als Hub oder Zweigstelle nutzbar.

PEinen Vergleich und Spezifikationen all unserer Firewalllösungen finden Sie unter paloaltonetworks.com/products/product-selection.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Zentrale: +1 408 75 34 000
Vertrieb: +1 866 32 04 788
Support: +1 866 898 9087

www.paloaltonetworks.com