PRISMA ACCESS
BY PALO ALTO NETWORKS

Prisma Access

Die weltweite Ausdehnung der Geschäftstätigkeit, eine steigende Zahl mobiler Mitarbeiter und die zunehmende Nutzung von Cloud-Computing verändern die Art und Weise, wie Unternehmen Anwendungen implementieren und bereitstellen. Gleich bleibt jedoch, dass diese Anwendungen umfassend geschützt werden müssen. Dafür sorgt Prisma™ Access, ein Secure Access Service Edge (SASE) für weltweit verteilte Netzwerk- und Sicherheitsdienste, die für alle Benutzer und Anwendungen zugänglich sind.

Prisma Access gewährt allen Benutzern sicheren Zugang zu Anwendungen in der Cloud, im Rechenzentrum und im Internet – unabhängig davon, ob sie in einer Niederlassung sind oder nicht.

Was ist das Besondere an Prisma Access?

Prisma Access wurde entwickelt, um Cyberangriffe wirksam zu verhindern. Dazu reicht es nicht aus, Bedrohungen aus dem Internet zu blockieren. Der gesamte ein- und ausgehende Datenverkehr muss inspiziert werden. Jeder Kompromiss kann zu gefährlichen Sicherheitslücken führen.

Prisma Access schützt den gesamten Datenverkehr – an allen Ports und von und zu allen Anwendungen – konsequent. So kann Ihr Unternehmen:

- **Cyberangriffe vereiteln –** mit praxiserprobten Sicherheitskonzepten und Bedrohungsanalysen für umfassende Transparenz und präzise, unternehmensweite Kontrolle
- **allen ein- und ausgehenden Datenverkehr gründlich inspizieren –** an allen Ports und unabhängig davon, ob es sich um Kommunikation mit dem Internet, mit der Cloud oder zwischen verschiedenen Niederlassungen des Unternehmens handelt und ob die Daten mit TLS/SSL verschlüsselt sind oder nicht
- **von den umfassenden Erkenntnissen profitieren,** die Palo Alto Networks aus seinen eigenen automatisiert erfassten Bedrohungsdaten und denen Hunderter anderer Unternehmen gewonnen hat

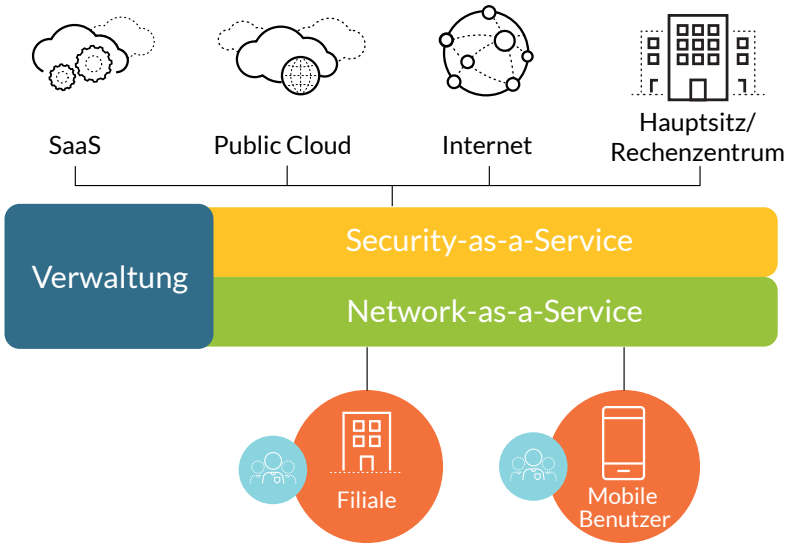

Abbildung 1: Die Architektur von Prisma Access

Network-as-a-Service

Prisma Access bietet zuverlässigen, sicheren Zugriff auf alle Anwendungen, in der Cloud, in Ihrem Rechenzentrum und im Internet.

Tabelle 1: Sicherer Zugang zu Anwendungen – von überall aus

	Zweigstelle	Hauptsitz/ regionaler Hauptsitz	Public Cloud	Private Cloud/ Rechen-zentrum	SaaS	Web	Internet
Entferntes/ Filialnetzwerk	✓	✓	✓	✓	✓	✓	✓
Mobiler Benutzer	✓	✓	✓	✓	✓	✓	✓

Konnektivität und Sicherheit für entfernte Netzwerke

- Verbinden Sie Ihre Zweigstellen über normale IPsec-VPN-Tunnel mit Prisma Access. Dazu können Sie bereits vorhandene Router, SD-WAN-Edge-Geräte, Firewalls anderer Anbieter oder andere handelsübliche, mit IPsec kompatible Geräte verwenden.
- Für das Routing von der Zweigstelle empfehlen wir das Border Gateway Protocol (BGP) oder statische Pfade.
- Wenn Sie mehrere Verbindungen zur Verfügung haben und die Leistung und Redundanz verbessern möchten, bietet sich das ECMP-Routing (Equal-Cost Multi-Path) an.

Konnektivität und Sicherheit für mobile Benutzer

- Stellen Sie Ihren mobilen Benutzern die App GlobalProtect zur Verfügung, die benutzerbasierte und loginbasierte Always-on-Verbindungen sowie On-Demand-Verbindungen unterstützt.
- Für stärkste Sicherheit empfehlen wir einen kompletten Always-on-Tunnel. Prisma Access unterstützt Split-Tunnelling (in Abhängigkeit vom Zugriffspfad), App-spezifische gesplittete VPN-Tunnel und Split-Tunnelling für Anwendungen mit geringem Risiko und großem Bandbreitebedarf wie dem Video-Streaming.

Bandbreitenmanagement

- Nutzen Sie App-ID™, um Richtlinien für das Whitelisting und Blockieren von Anwendungen zu aktivieren und Ihr Netzwerk von unnötigen, bandbreitenintensiven Anwendungen frei zu halten.
- Der von Prisma Access abgewickelte Datenverkehr kann mit Quality-of-Service-Richtlinien priorisiert und gelenkt werden.

Protokollierung

- Sie profitieren von einem zentralisierten, automatisierten und in der Cloud skalierbaren Speicher für Logdateien.
- Sie können die Verwaltung der Protokollierung und die Berichterstellung zentralisieren.
- Sie können Logdateien an Ihren Syslog-Server und/oder Ihr SIEM-System (Security Information and Event Management) weiterleiten.

Security-as-a-Service-Ebene

Firewall-as-a-Service

- Prisma Access beinhaltet nicht nur die Sicherheitsdienste, die Sie von einer Next-Generation Firewall erwarten, sondern auch Firewall-as-a-Service (FWaaS) zum Schutz Ihrer Zweigstellen vor Bedrohungen. Im Funktionsumfang von FWaaS sind unter anderem Bedrohungsprävention, URL Filtering und Sandboxing enthalten.

DNS-Sicherheit

- Prisma Access stellt unseren Service für die DNS-Sicherheit bereit, der vorausschauende Analysen, maschinelles Lernen und Automatisierung nutzt, um im DNS-Datenverkehr versteckte Bedrohungen abzuwehren. So können Sie die Kommunikation mit als schädlich bekannten Domains unterbinden, verdächtige Domains frühzeitig erkennen und das DNS-Tunneling verhindern.

Bedrohungsabwehr

- Wenn Sie Prisma Access für die Bedrohungsprävention nutzen, profitieren Sie nicht nur von den bewährten Technologien einer Plattform von Palo Alto Networks, sondern auch von Bedrohungsdaten aus aller Welt und von automatisierten Funktionen zur Abwehr bekannter und neuer Bedrohungen.

Cloud-SWG

- Zu den Designzielen für Prisma Access für sichere Internet-Gateways (Secure Web Gateway, SWG) gehörten die Transparenz für Datenverkehr aller Art und die Vereitelung von Tarnungsmanövern zur Verschleierung von Bedrohungen. Zudem nutzen wir unsere Funktionen für das Filtern von Internet-Datenverkehr, um das Versenden von Anmeldedaten an noch unbekannte Adressen (und damit ihren möglichen Diebstahl) zu verhindern.

Schutz vor Datenverlust

- Prisma Access kombiniert Integration und den API-basierten Schutz vor Datenverlusten (Data Loss Prevention, DLP) von Prisma SaaS mit seinen eigenen, Inline implementierten DLP-Funktionen. Das versetzt Unternehmen in die Lage, Daten zu kategorisieren und Richtlinien zur Verhinderung von Datenverlusten zu erstellen und durchzusetzen.

Cloud Access Security Broker (CASB)

- Mit Prisma Access und Prisma SaaS implementieren Sie eine Sicherheitsinfrastruktur, in der Inline implementierte, API-basierte und kontextabhängige Maßnahmen ineinander greifen und als CASB (Cloud Access Security Broker) fungieren, der den Zugang zu vertraulichen Daten regelt. Diese Maßnahmen werden als integriertes Ganzes implementiert und auf alle Cloud-Anwendungsrichtlinien angewendet.

Management

Prisma Access unterstützt zwei Managementoptionen:

- **Netzwerksicherheitsmanagement mit Panorama™** für die zentralisierte Verwaltung der Next-Generation Firewalls von Palo Alto Networks und Prisma Access.
- **Cloudbasiertes Management** über eine webbasierte Oberfläche mit vorkonfigurierten Profilen und straffen Workflows, mit der Prisma Access-App auf dem Hub.

Tabelle 2: Prisma Access: Details, Features und Spezifikationen			
	Prisma Access für Netzwerke	**Prisma Access für Benutzer**	**Prisma Access für Clean Pipe**

Anwendungsbereiche	• Zweig-/Verkaufsstellen
	• Virtual Private Cloud (VPC)
	• Palo Alto Networks SD-WAN-Hub
	• Andere SD-WAN-Sicherheitsmaßnahmen
		• Mobile Benutzer mit:
		  • Laptops
		  • Smartphones
		  • Tablets
		• Zero-Trust-Zugriff auf Netzwerke
			• Serviceanbieter/Telekommunikationsumgebungen mit mehreren Mandanten
			• Sicherung des ausgehenden Datenverkehrs

Lizenzierung			
Grundlage	Mbit/s Basiert auf Bandbreitenpool; jeder Verbindung kann bis zu 1 Gbit/s zugewiesen werden	Benutzer Basiert auf der Gesamtzahl unterschiedlicher Benutzer	Mbit/s Basiert auf Bandbreitenpool; bis zu 10 Gbit/s pro Mandant; aufteilbar
Minimale Umgebungsgröße	Bandbreitenpool von 200 Mbit/s	200 Benutzer	100 Mbit/s pro Mandant
Service-Tunnel			
Enthaltene Service-Tunnel	Bis zu drei Servicetunnel inklusive		n/a
Zusätzliche Service-Tunnel	Sie können bis zu 100 zusätzliche Service-Tunnel erstellen, indem Sie jedem neuen Tunnel 300 Mbit/s des Bandbreitepools zuweisen.		n/a
Konnektivität			
Standorte	über 100 in 76 Ländern		17 Standorte
Art der Verbindung	• Ipsec-Tunnel • SD-WAN (PAN-OS 9.1 oder höher)	GlobalProtect-App IPsec/SSL	Peering über Partner Interconnect (VLAN-Anbindung je Mandant)
Plattformunterstützung der GlobalProtect-App	n/a	Apple iOS Apple macOS Google Android Google Chrome OS Linux CentOS Red Hat Enterprise Linux Ubuntu Windows 7, 8, 10 und UWP	n/a
Management			
Panorama	• Panorama-Lizenz erforderlich • Für das Panorama-Plugin für Prisma Access ist keine Lizenz erforderlich. • Prisma Access wird bei der Anzahl der erforderlichen Panorama-Gerätelizenzen nicht mitgezählt.		
Cloud-Management	Für die Prisma Access-App auf dem Hub ist keine Lizenz erforderlich.		
Sicherheit			
URL Filtering	Inklusive		
Threat Prevention	Inklusive		
WildFire	Inklusive		
Host Information Profile	Inklusive		
DNS Security	Abonnement erforderlich		
Data Loss Prevention	Abonnement erforderlich		
Cortex XDR	Abonnement erforderlich		
Prisma SaaS	Abonnement erforderlich		
AutoFocus	Abonnement erforderlich		
Protokollierung			
Cortex Data Lake	Für die Protokollierung benötigt Prisma Access Cortex Data Lake (Abonnement erforderlich).		

PRISMA™ ACCESS
BY PALO ALTO NETWORKS

Oval Tower, De Entrée 99-197
1101 HE Amsterdam
Niederlande
Telefon: +31 20 888 1883
www.paloaltonetworks.de

prisma-access-ds-111219-de