

Auf einen Blick: Prisma Access

Die weltweite Ausdehnung der Geschäftstätigkeit, eine steigende Zahl mobiler Mitarbeiter und das Cloud Computing führen dazu, dass Unternehmensanwendungen und -daten verlagert und für Benutzer an immer mehr Standorten bereitgestellt werden. Das eröffnet Unternehmen neue Geschäftschancen, schafft aber möglicherweise auch neue Angriffsvektoren.

Prisma Access ...

- schützt Filialnetzwerke und mobile Mitarbeiter mit konsistenten Sicherheitsmaßnahmen, unabhängig vom Standort.
- sorgt für zuverlässigen, sicheren Zugriff auf alle Anwendungen.
- bietet die Flexibilität und cloudbasierte Skalierbarkeit, die zur Erfüllung immer neuer Anforderungen erforderlich sind.

Herausforderungen beim Schutz einer wachsenden Infrastruktur

Die Cloud und die steigende Anzahl der mobilen Benutzer führen zu Änderungen in Netzwerken und zu neuen Sicherheitsanforderungen. Bei dem Versuch, diese Änderungen durch das Aufsetzen zusätzlicher Komponenten auf die vorhandene Infrastruktur vorzunehmen, sind Unternehmen bereits auf zahlreiche Herausforderungen gestoßen:

- Die Umleitung von Datenverkehr über Virtual Private Networks (virtuelle private Netzwerke, VPN) oder MPLS-Leitungen (Multiprotocol Label Switching) ist ineffizient und beeinträchtigt die Benutzererfahrung.
- Die Einrichtung direkter, nicht überwachter Internetverbindungen für Filialen und mobile Benutzer untergräbt die Sicherheit.
- Die cloudbasierten Sicherheitslösungen der ersten Generation – wie Proxys, DNS-Filter und CASBs – bieten nur einen begrenzten Funktionsumfang.

All das führt zu höheren Kosten, mehr Administrationsaufwand und Schwierigkeiten im Betrieb. Dennoch müssen diese Änderungen vorgenommen werden, wenn das Unternehmen sich am Markt behaupten will. Im Jahr 2019 hat Gartner eine neue, über die Cloud bereitgestellte Architektur für Netzwerk- und Sicherheitsdienste definiert, die als „Secure Access Service Edge“ oder SASE bezeichnet wird und die Punktlösungen der ersten Generation in einem einheitlichen Servicemodell zusammenfasst.

Prisma Access

Prisma™ Access ist ein SASE, das Unternehmen und Institutionen in die Lage versetzt, die Netzwerk- und Sicherheitsdienste cloudbasiert bereitzustellen, die sie benötigen, um stärker von Cloud Computing und mobilem Arbeiten zu profitieren. Da immer mehr Benutzer, Zweigstellen, Daten und Services sich an Standorten befinden, die nicht von den traditionellen Netzwerksicherheitsappliances abgedeckt werden, benötigen moderne Unternehmen eine cloudbasierte Infrastruktur, die sowohl Netzwerk- als auch die dazugehörigen Netzwerksicherheitsfunktionen bereitstellt. Prisma Access nutzt ein und dasselbe Framework, um konsistente Sicherheitsdienste und Zugang zu Cloud-Anwendungen (in öffentlichen und privaten Clouds und SaaS-Umgebungen) zu bieten und sorgt damit für eine nahtlose Benutzererfahrung.

Alle Benutzer profitieren von sicherem Zugang zu Anwendungen in der Cloud, im Rechenzentrum und im Internet – unabhängig davon, ob sie in einer Niederlassung sind oder nicht. Prisma Access unterzieht sämtliche Datenübertragungen auf allen Ports konsistenten Sicherheitsprüfungen und stellt außerdem die bidirektionalen Netzwerkverbindungen bereit, die für den Datenverkehr zwischen Zweigstellen sowie zwischen Zweigstellen und Hauptsitz erforderlich sind.

Prisma Access wird von über 100 Standorten in 76 Ländern aus als Cloud-Service für Niederlassungen, Verkaufsstandorte und mobile Benutzer bereitgestellt.

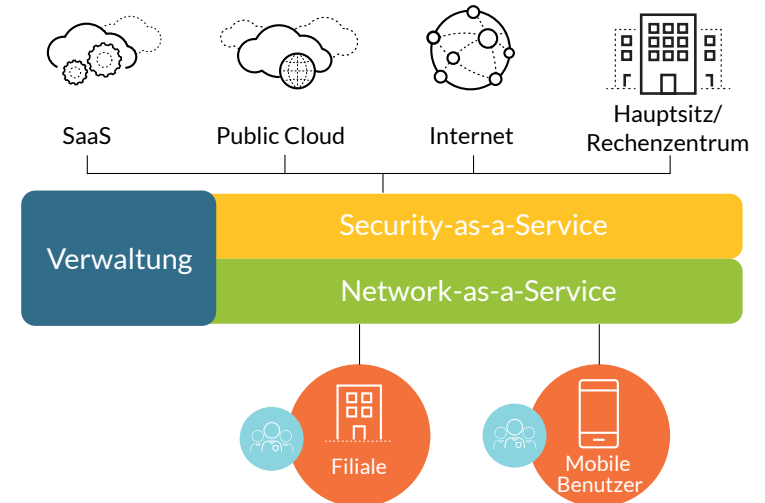


Abbildung 1: Prisma Access, ein Secure Access Service Edge

Prisma Access für Netzwerke

Viele Filialen und Verkaufsstellen sind geografisch weit vom Hauptsitz ihres Unternehmens entfernt und haben keine eigenen, in Vollzeit beschäftigten IT-Mitarbeiter. Das erschwert nicht nur die Installation, Pflege und Aktualisierung von Hardware, sondern auch das Änderungsmanagement.

Mit Prisma Access können Sie Remote-Netzwerke über normale IPsec-VPN-Tunnel miteinander verbinden. Dazu können Sie bereits vorhandene Router, SD-WAN-Edge-Geräte oder Firewalls verwenden, die IPsec unterstützen. Dadurch sichern Sie den gesamten Datenverkehr, schützen vertrauliche Informationen und erfüllen die relevanten Datenschutzanforderungen. Prisma Access unterstützt SD-WAN-Optionen mit den Next-Generation Firewalls von Palo Alto Networks und Produkten anderer Anbieter.

Prisma Access für Benutzer

Beim Zugriff auf unternehmensintern bereitgestellte Anwendungen und cloudbasierte Apps sind mobile Benutzer auf konsistenten Schutz angewiesen. VPN-Verbindungen über ein zentrales Gateway können sich hier als unzureichend erweisen, da sie vielfach nur für den Zugang zu den im unternehmenseigenen Rechenzentrum gehosteten Anwendungen genutzt werden. Etliche Benutzer melden sich vor dem Zugriff auf Cloud- und Web-Anwendungen aus dem VPN ab, weil sie sich davon eine bessere Leistung erhoffen – und nehmen damit Einbußen bei der Sicherheit in Kauf.

Prisma Access rückt die Schutzmaßnahmen näher an die Standorte der Benutzer, sodass der Cloud-Traffic nicht länger über das Rechenzentrum am Hauptsitz umgeleitet werden muss. Dabei arbeitet Prisma Access mit der App GlobalProtect™ zusammen, die auf dem Smartphone, Tablet oder Laptop des Benutzers installiert werden kann. Diese App baut automatisch einen IPsec/SSL-VPN-Tunnel zu Prisma Access auf, damit die Sicherheitsrichtlinien des Unternehmens angewendet werden können, ohne den Datenverkehr zum Hauptsitz oder Rechenzentrum des Unternehmens zu schicken. Auf diese Weise erhalten alle mobilen Benutzer sicheren und schnellen Zugriff auf sämtliche Anwendungen – unabhängig davon, ob diese in der Cloud, im Internet oder im Rechenzentrum gehostet werden.

Zudem unterstützt die GlobalProtect-App die Einrichtung von Zugangsrichtlinien, die ein bestimmtes Host Information Profile (HIP) vorschreiben. Das kann zum Beispiel bedeuten, dass Benutzer nur von Geräten aus auf kritische Anwendungen zugreifen können, die bestimmte Mindestanforderungen bezüglich der Betriebssystem- und Patch-Version oder der Endpunkt-Software erfüllen.

Es gibt Situationen, in denen sehr viele Benutzer den Standort wechseln müssen. Sie können sich beispielsweise versammeln, um an einer Großveranstaltung teilzunehmen, oder einen Standort aufgrund widriger Wetterverhältnisse oder Naturkatastrophen plötzlich verlassen. Prisma Access überwacht die Netzwerknutzung kontinuierlich und passt die verfügbaren Kapazitäten in den verschiedenen Regionen automatisch an den Bedarf an.

SASE-Services

Prisma Access bietet sowohl Netzwerk- als auch Sicherheitsdienste, darunter:

Netzwerkdienste

- **SD-WAN:** Unterstützung für die Next-Generation Firewalls von Palo Alto Networks und für die Anbindung an SD-WANs anderer Anbieter
- **VPN:** verschiedene Optionen für die Anbindung von Benutzern und Netzwerken, darunter IPsec, SSL/IPsec und clientloses VPN
- **Zero-Trust-Zugriff auf Netzwerke (ZTNA):** Zugriffskontrolle und Bedrohungsabwehr zum Schutz von Anwendungen
- **Quality of Service (Servicequalität, QoS):** bevorzugte Behandlung kritischer Anwendungen bei der Zuweisung von Bandbreite
- **Clean Pipe:** Schutz des ausgehenden Internet-Datenverkehrs für Anbieter von Managed Services

Sicherheitsdienste

- **Firewall-as-a-Service (FWaaS):** Sicherheitsdienste für Next-Generation Firewalls in Filialen und Verkaufsstellen
- **DNS-Sicherheit:** Nutzung modernster Analysen und maschineller Lernverfahren, um Bedrohungen im DNS-Datenverkehr abzuwehren
- **Bedrohungsprävention:** Einsatz von Bedrohungsdaten zum Blockieren von Exploits, Malware und Command-and-Control-Kommunikation
- **Cloud-SWG (Secure Web Gateway):** Blockierung schädlicher Websites mithilfe statischer Analysen und maschineller Lernverfahren
- **Schutz vor Datenverlusten:** Sicherheitsklassifizierung von Daten und Anwendung angemessener Zugangskontrollen
- **Cloud Access Security Broker (CASB):** Governance und Datenklassifizierung zur Bedrohungsabwehr mit Inline- und API-basierten Sicherheitsmaßnahmen

Lizenzoptionen

Bei **Prisma Access für Netzwerke** hängen die Lizenzkosten von der Gesamtbandbreite ab, die für alle Standorte bereitgestellt wird. Die Mindestgröße dieses gemeinsamen Bandbreitenpools beträgt 200 Mbit/s. Jedem Standort wird ein Teil dieses Bandbreitenpools zugewiesen.

Bei **Prisma Access für Benutzer** hängen die Lizenzkosten von der Anzahl der Benutzer ab. Es gibt mehrere Lizenzstufen, von Lizenzen für bis zu 200 Benutzer bis hin zu Lizenzen für über 100.000 Benutzer. Die Benutzer benötigen zudem die App GlobalProtect. Sie unterstützt Geräte mit Microsoft Windows®, Apple macOS® und iOS, Android®, Google Chrome® und Linux.