# GLOBALPROTECT

## Abwehr von Angriffen und Schutz Ihrer mobilen Mitarbeiter

GlobalProtect dehnt den Schutz der Next-Generation-Sicherheitsplattform von Palo Alto Networks auf Ihre mobilen Mitarbeiter aus, ungeachtet von deren Standort.

### *Wichtige Nutzungsszenarien und Vorteile*

**Remote Access VPN**

- Sicherer Zugriff auf interne und cloudbasierte Geschäftsanwendungen

**Schutz vor komplexen Bedrohungen (Advanced Threat Prevention)**

- Sicherer Internetdatenverkehr
- Verhindert, dass Bedrohungen Endpunkte erreichen
- Schützt vor Phishing und dem Missbrauch von Nutzerdaten

**URL-Filterung**

- Setzt akzeptable Nutzungsrichtlinien durch
- Filtert den Zugriff auf schädliche Domains und nicht jugendfreie Inhalte
- Verhindert die Nutzung von Vermeidungs- und Umgehungstools zur Tarnung von schädlichem Datenverkehr

**Sicherer Zugriff auf SaaS-Anwendungen**

- Steuert den Zugriff und setzt Richtlinien für SaaS-Anwendungen durch, während nicht genehmigte Anwendungen blockiert werden

**BYOD**

- Unterstützt zur Gewährleistung des Datenschutzes App-spezifische VPN-Verbindungen
- Ermöglicht Partnern, Kollegen und Auftragnehmern den sicheren Zugriff

**Förderung der internen Netzwerksegmentierung**

- Sorgt für eine zuverlässige Benutzeridentifizierung
- Liefert sofort präzise Hostinformationen zu Transparenzzwecken und zur Durchsetzung von Richtlinien
- Erzwingt für den Zugriff auf sensible Ressourcen eine verstärkte Multifaktor-Authentifizierung

Die zu schützende Umgebung nimmt an Umfang zu, da sich sowohl Ihre Benutzer als auch Ihre Anwendungen zunehmend außerhalb der herkömmlichen Netzwerkperimeter befinden. Sicherheitsteams stehen vor der Herausforderung, die Transparenz des Netzwerkdatenverkehrs aufrecht zu erhalten und Sicherheitsleitlinien durchzusetzen, um Bedrohungen abzuwehren. Herkömmliche Technologien zum Schutz mobiler Endpunkte, wie etwa Antivirensoftware auf Host-Endpunkten und Remote Access VPN, sind nicht in der Lage, die fortschrittlichen Techniken moderner Angreifer abzuwehren.

Schützen Sie Ihre mobilen Mitarbeiter mit dem GlobalProtect™-Netzwerksicherheitsclient von Palo Alto Networks®, indem Sie die Next- Generation-Sicherheitsplattform standortunabhängig auf alle Benutzer ausdehnen. Der Client schützt den Datenverkehr mithilfe der Plattformfunktionen, indem er die Nutzung von Anwendungen ermittelt, den Datenverkehr Benutzern und Geräten zuordnet und Sicherheitsleitlinien mit innovativen Techniken durchsetzt.

### Externe Erweiterung des Plattformschutzes

GlobalProtect schützt mobile Mitarbeiter mithilfe der innovativen Firewalls des Unternehmens, die Sie als Internetgateways am Perimeter, in der DMZ oder in der Cloud bereitstellen, um den gesamten Datenverkehr zu untersuchen. Notebooks, Smartphones und Tablets, auf denen die GlobalProtect-App installiert ist, stellen automatisch eine sichere SSL/IPsec-VPN-Verbindung zur leistungsstärksten innovativen Firewall an einem gegebenen Standort her. Ihr Unternehmen profitiert dadurch von der vollständigen Transparenz des gesamten Netzwerkdatenverkehrs sowie aller Anwendungen, Ports und Protokolle. Indem Sie die blinden Flecken im Datenverkehr Ihrer mobilen Mitarbeiter eliminieren, halten Sie den konsistenten Einblick in Anwendungen aufrecht.

### Interner Schutz für Ihr Netzwerk

Nicht alle Benutzer benötigen Zugriff auf alle Bereiche des Unternehmensnetzwerks. Sicherheitsteams partitionieren Netzwerke vermehrt und setzen präzise Zugriffssteuerungen für interne Ressourcen durch. GlobalProtect ermöglicht eine extrem schnelle, maßgebende Benutzeridentifizierung für die Plattform, sodass Sie genaue Richtlinien für geschäftsspezifische Zugriffsberechtigungen erstellen können. Darüber hinaus bietet GlobalProtect Hostinformationen, um mit Sicherheitsleitlinien verbundene Gerätekriterien zu erstellen. Sie können dadurch Sicherheitsmaßnahmen zum Schutz Ihrer internen Netzwerke ergreifen, Zero Trust-Netzwerksteuerfunktionen einsetzen und die Angriffsoberfläche reduzieren.

Indem Sie GlobalProtect auf diese Weise nutzen, können Sie interne Netzwerkgateways für die Nutzung mit oder ohne VPN Tunnel konfigurieren.

### Untersuchen des Datenverkehrs und Durchsetzen von Sicherheitsleitlinien

GlobalProtect bietet Sicherheitsteams die Möglichkeit, konsequent durchsetzbare Richtlinien zu erstellen, ungeachtet dessen, ob sich Benutzer innerhalb oder außerhalb des Unternehmensnetzwerks befinden. Sicherheitsteams können zum Schutz vor Cyberattacken sämtliche Funktionen der Plattform nutzen, einschließlich:

- **App-ID™-Technologie**: Identifiziert Anwendungsdatenverkehr ungeachtet der Portnummer und bietet Unternehmen die Möglichkeit, Richtlinien zur Verwaltung der Anwendungsnutzung auf Benutzer- und Gerätebasis einzuführen
- **User-ID™-Technologie**: Identifiziert Benutzer und Gruppenmitglieder zu Transparenzzwecken sowie zur Durchsetzung rollenbasierter Netzwerksicherheitsleitlinien
- **Entschlüsselung**: Untersucht und steuert Anwendungen, deren SSL/TLS/SSH-Datenverkehr verschlüsselt ist. Bedrohungen in verschlüsseltem Datenverkehr werden dadurch abgewehrt.
- **WildFire™**: Dank cloudbasierter Malware-Analyse werden Inhalte automatisch analysiert, um neue, bislang unbekannte und extrem zielgerichtete Malware anhand ihres Verhaltens zu identifizieren. Durch die gleichzeitige Integration der erforderlichen Threat Intelligence lassen sich derartige Angriffe nahezu in Echtzeit abwehren.
- **Threat Prevention für IPS und Antivirensoftware**: Netzwerkbasierte Exploits anfälliger Anwendungen und Betriebssysteme, DoS-Angriffe und Port-Scans werden mittels Intrusion Prevention blockiert. Antivirenprofile verhindern, dass Malware und Spyware Endpunkte über eine Stream-basierte Engine erreichen.
- **URL-Filterung mit PAN-DB**: PAN-DB kategorisiert URLs entsprechend ihres Inhalts auf Domain-, Datei- und Seitenebene und wird mit Daten von WildFire aktualisiert, sodass bei Änderungen an Webinhalten auch die Kategorisierungen angepasst werden.
- **Datei-Blockade**: Unterbinden Sie die Übertragung unerwünschter oder gefährlicher Dateien, während Sie die Integrität zulässiger Dateien weiter mit WildFire hinterfragen.
- **Datenfilterung**: Mithilfe der Datenfilterung können Administratoren Richtlinien implementieren, mit denen sich nicht autorisierte Datenbewegungen wie etwa die Übertragung benutzerdefinierter Informationen oder anderer vertraulicher Inhalte unterbinden lassen.

### Benutzerdefinierten Host-Bedingungen (z. B. das Identifizieren von Benutzern und Geräten)

#### *Benutzerauthentifizierung*

GlobalProtect unterstützt alle vorhandenen PAN-OS®-Authentifizierungsmethoden, einschließlich Kerberos, RADIUS, LDAP, SAML 2.0, Clientzertifikate und lokale Benutzerdatenbanken. Nachdem GlobalProtect den Benutzer authentifiziert hat, wird der innovativen Firewall für User-ID sofort die Zuordnung zwischen Benutzer und IP-Adresse bereitgestellt.

#### *Starke Authentifizierungsoptionen*

GlobalProtect unterstützt durch die Integration von RADIUS eine Reihe von Multifaktor-Authentifizierungsmethoden von Drittanbietern, wie etwa OTP-Token (One-Time Password, Einmalkennwort), Zertifikate und Smartcards.

Unternehmen können damit die Identitätsüberprüfung für den Zugriff auf interne Rechenzentren oder SaaS-Anwendungen verstärken.

Die in GlobalProtect bereitgestellten Optionen erleichtern die Bereitstellung und Nutzung starker Authentifizierungsmethoden:

- **Cookie-basierte Authentifizierung:** Sie können nach der Authentifizierung der Benutzer ein verschlüsseltes Cookie für den weiteren Zugriff auf ein Portal oder Gateway verwenden. Der Zugriff gilt für die Lebensdauer dieses Cookies.
- **SCEP-Unterstützung (Simple Certificate Enrollment Protocol):** GlobalProtect kann die Interaktion mit einer Unternehmens-PKI zum Verwalten, Ausstellen und Verteilen von Zertifikaten an GlobalProtect-Clients automatisieren.

#### *Host Information Profile (Host-Informationsprofil, HIP)*

GlobalProtect prüft die Konfiguration eines Endpunkts und erstellt daraufhin ein Host Information Profile (HIP), das mit der innovativen Firewall geteilt wird. Die innovative Firewall setzt mithilfe des Host Information Profiles Richtlinien durch, die den Zugriff auf Anwendungen nur zulassen, wenn der Endpunkt ordnungsgemäß konfiguriert und geschützt ist. Sie können dadurch die Einhaltung von Richtlinien erzwingen, mit denen Sie den Umfang der Zugriffsberechtigungen jedes Benutzers für ein bestimmtes Gerät regeln.

Host Information Profile-Richtlinien können auf verschiedenen Attributen basieren, wie etwa:

- Betriebssystem- und Anwendungspatch-Ebene
- Version und Zustand der Anti-Malware-Software eines Hosts
- Version und Zustand der Firewall eines Hosts
- Konfiguration der Datenträgerverschlüsselung
- Konfiguration des Datensicherungsprodukts
- Benutzerdefinierte Host-Bedingungen (z. B. Registrierungseinträge, ausgeführte Software)

#### *Steuerung des Zugriffs auf Anwendungen und Daten*

Sicherheitsteams können Richtlinien basierend auf Anwendungen, Benutzern, Inhalten und Hostinformationen erstellen, um eine kontinuierliche detaillierte Zugriffssteuerung für eine gegebene Anwendung zu ermöglichen. Diese Richtlinien können mit bestimmten, in einem Verzeichnis definierten Benutzern oder Gruppen verknüpft werden, um die jeweils geschäftsrelevanten Zugriffsebenen bereitzustellen. Durch die Einführung weiterer Richtlinien zur Verstärkung der Multifaktor-Authentifizierung kann der Zugriff auf besonders sensible Ressourcen und Anwendungen mithilfe eines zusätzlichen Identitätsnachweises geschützt werden.

### Sichere BYOD-Aktivierung

Durch den BYOD-Trend müssen Sicherheitsteams immer mehr Anwendungsfälle unterstützen. Ein immer breiteres Spektrum an Mitarbeitern und Auftragnehmern muss über verschiedenste Mobilgeräte auf Anwendungen zugreifen können.

Die Integration in Mobile Device Management-Lösungen wie AirWatch® und MobileIron® erleichtert es Unternehmen, GlobalProtect sowie zusätzliche Sicherheitsmaßnahmen durch den Austausch von Informationen und Host-Konfigurationen bereitzustellen. Das Unternehmen kann in Verbindung mit GlobalProtect die Transparenz und die Durchsetzung von Sicherheitsrichtlinien für jede App individuell aufrechterhalten erhalten. Gleichzeitig bleiben die Daten weiterhin von privaten Aktivitäten getrennt, um den BYOD-Erwartungen der Benutzer gerecht zu werden.

GlobalProtect unterstützt eine clientlose SSL VPN-Verbindung, um auch für nicht verwaltete Geräte den sicheren Zugriff auf Anwendungen im Rechenzentrum und in der Cloud zu gewährleisten. Der Zugriff auf spezielle Anwendungen erfolgt dabei bequem über eine sichere Weboberfläche. Benutzer müssen vorab weder einen Client installieren noch einen vollständigen Tunnel einrichten.

### Die Bedeutung der Architektur

Dank der flexiblen Architektur bietet GlobalProtect zahlreiche Funktionen, die es Ihnen erleichtern, eine Reihe von sicherheitsrelevanten Herausforderungen zu meistern. Grundsätzlich können Sie GlobalProtect als Ersatz für das herkömmliche VPN-Gateway verwenden. Sie reduzieren dadurch die Komplexität und die Problematiken, welche die Verwaltung eines eigenständigen VPN-Gateways eines Drittanbieters mit sich bringt.

Dank des optionalen manuellen Verbindungsaufbaus und der Möglichkeit der Gatewayauswahl können Unternehmen die Lösung passend zu ihren Geschäftsanforderungen konfigurieren.

Bei einer umfangreicheren Bereitstellung haben Sie die Möglichkeit, GlobalProtect zum Schutz des Datenverkehrs mit einer permanenten VPN-Verbindung über einen vollständigen Tunnel bereitzustellen. Sie sorgen dadurch für einen stets gegenwärtigen und für Benutzer unauffälligen Schutz.

#### *Cloudbasierte Gateways*

Da Mitarbeiter zunehmend von unterschiedlichen Standorten aus arbeiten, kommt es zu schwankenden Datenverkehrsbelastungen. Dabei spielt insbesondere auch die Art und Weise, wie sich Unternehmen weiterentwickeln, eine Rolle – sei es vorübergehend (etwa aufgrund einer Naturkatastrophe in einer Region) oder permanent (durch die Erschließung neuer Märkte).

Der GlobalProtect-Cloud-Dienst ermöglicht die gemeinsam verwaltete Abdeckung der für Ihr Unternehmen erforderlichen Standorte unter Anwendung Ihrer Sicherheitsrichtlinien. Er kann in Verbindung mit Ihren bestehenden Firewalls genutzt werden, um Ihre Architektur an die sich ändernden Bedingungen anzupassen.

Der GlobalProtect-Cloud-Dienst unterstützt die automatische Skalierung, wobei neue Firewalls entsprechend der Last und des Bedarfs in einer Region dynamisch zugewiesen werden.

### Fazit

Die von der Next-Generation-Sicherheitsplattform von Palo Alto Networks bereitgestellten Schutzmaßnahmen spielen bei der Vermeidung von Sicherheitsverletzungen eine wichtige Rolle. Mit GlobalProtect erweitern Sie den Schutz der Plattform auf alle Benutzer, ungeachtet ihres Standorts. GlobalProtect bietet Ihnen die Möglichkeit, Sicherheitsleitlinien konsistent durchzusetzen, sodass Benutzer auch außerhalb des Unternehmensnetzwerks vor Cyberattacken geschützt sind.

## Merkmale von GlobalProtect

| Kategorie | Spezifikation |
|---|---|
| **VPN-Verbindung** | IPsec |
| | SSL |
| | Clientloses VPN |
| | App-spezifische VPN-Verbindungen auf Android™, iOS und Windows® 10 |
| **Gatewayauswahl** | Automatisches Auswahl |
| | Manuelle Auswahl |
| | Externe Gatewayauswahl nach Quellstandort |
| | Interne Gatewayauswahl nach Quell-IP |
| **Verbindungsmethoden** | Benutzeranmeldung (permanent) |
| | Bei Bedarf |
| | Vorabanmeldung (permanent) |
| | Vorabanmeldung, anschließend bei Bedarf |
| **Verbindungsmodus** | Interner Modus |
| | Externer Modus |
| **Layer-3-Installation** | IPv4 |
| | IPv6 |
| **Single Sign-On** | SSO (Windows-Anmeldeinformationsanbieter) |
| | Kerberos SSO |

| Kategorie | Spezifikation |
|---|---|
| **Getrennte Tunnel** | Routen einschließen |
| | Routen ausschließen |
| **Authentifizierungsmethoden** | SAML 2.0 |
| | LDAP |
| | Client-Zertifikate |
| | Kerberos |
| | RADIUS |
| | Zwei-Faktor-Authentifizierung |
| **Host Information Profile, Berichterstattung, Richtliniendurchsetzung und Benachrichtigungen** | Patch-Management |
| | Host-Anti-Spyware |
| | Host-Antivirensoftware |
| | Host-Firewall |
| | Datenträgerverschlüsselung |
| | Datenträger-Backup |
| | Data Loss Prevention (Schutz vor Datenverlust, DLP) |
| | Benutzerdefinierte Host Information Profile-Bedingungen (z. B. Registrierungseinträge, ausgeführte Software) |
| **Multifaktor-Authentifizierung** | Erweiterte Authentifizierung für den Zugriff auf sensible Ressourcen |
| **Weitere Merkmale** | User-ID |
| | IPsec-zu-SSL VPN-Fallback |
| | Erzwingung des Netzwerkzugriffs über eine GlobalProtect-Verbindung |
| | SCEP-basierte automatische Benutzerzertifikatverwaltung |
| | Vor und nach Sitzungen ausgeführte Skriptaktionen |
| | Dynamische GlobalProtect App-Anpassung |
| | App-Konfiguration basierend auf Benutzern, Gruppen bzw. Betriebssystemen |
| | Automatische interne/externe Erkennung |
| | Manuelles/automatisches Upgrade der GlobalProtect App |
| | Zertifikatauswahl nach OID |
| | Zugriffssperre für verlorene, gestohlene und unbekannte Geräte |
| | Smartcard-Unterstützung für Verbindungsaufbau/-trennung |
| | Transparente Verteilung vertrauenswürdiger Stamm-CAs für die SSL-Entschlüsselung |
| | Deaktivierung des Direktzugriffs auf lokale Netzwerke |
| | Anpassbare Begrüßungs- und Hilfeseiten |
| | RDP-Verbindung zu Remote-Client |

| Kategorie | Spezifikation |
|---|---|
| **MDM/EMM-Integration** | AirWatch |
| | MobileIron |
| **Verwaltungstools und APIs** | Next-Generation-Sicherheitsplattform von Palo Alto Networks einschließlich physischer Formfaktoren (z. B. die PA-7000 Series, PA-3000 Series und PA-200) und virtueller Formfaktoren (VM-Series) |
| | Microsoft InTune® |
| | GlobalProtect-Cloud-Dienst |
| **Von GlobalProtect App unterstützte Plattformen** | Microsoft® Windows und Windows UWP |
| | Apple® Mac® OS X® |
| | Apple iOS |
| | Google® Chrome® OS |
| | Android® OS |
| | Linux®-Unterstützung unter Verwendung von Drittanbieter-VPNC und StrongSwan-Client |
| **IPsec Xauth** | Apple iOS IPsec-Client |
| | Android OS IPsec-Client |
| **GlobalProtect App-Sprachen** | Englisch |
| | Spanisch |
| | Deutsch |
| | Französisch |
| | Japanisch |
| | Chinesisch |

3000 Tannery Way
Santa Clara, CA 95054, USA

Zentrale: +1/408/75 34 000
Vertrieb: +1/866/320/4788
Support: +1/866/89 89 087

www.paloaltonetworks.com


globalprotect-ds-082817