GlobalProtect

GlobalProtect erweitert die Schutzfunktionen der Palo Alto Networks Next-Generation Firewall. Nun sind auch Ihre mobilen Mitarbeiter immer und überall geschützt.

Da die Benutzer und Anwendungen sich zunehmend außerhalb der herkömmlichen Netzwerke bewegen, ergeben sich auch ständig neue Sicherheitsanforderungen. Sicherheitsteams stehen vor der Herausforderung, den gesamten Datenverkehr im Netzwerk zu überwachen und Bedrohungen abzuwenden, indem sie Sicherheitsrichtlinien durchsetzen. Herkömmliche Technologien zum Schutz mobiler Endpunkte, wie etwa Antivirensoftware am Hostendpunkt oder VPN-Fernzugriff, können die heutigen Angreifer mit ihren ausgefeilten Strategien nicht aufhalten.

GlobalProtect™ ist eine Netzwerksicherheitslösung für Endpunkte, mit der Sie Ihre mobilen Mitarbeiter schützen können. Dazu werden die Funktionen der Next-Generation Firewall auf alle Benutzer ausgedehnt, unabhängig von deren Gerät oder Standort. GlobalProtect™ sichert den Datenverkehr auf mehrere Arten: Es analysiert mit plattformeigenen Funktionen, wie Anwendungen genutzt werden, ordnet den Datenverkehr Benutzern und Geräten zu und stellt mit innovativen Technologien sicher, dass Richtlinien eingehalten werden.

Typische Anwendungsfälle und Vorteile

VPN-Fernzugriff
- Sicherer Zugriff auf interne und cloudbasierte Business-Apps

Erweiterte Abwehr von Bedrohungen
- Sicherung des Datenverkehrs im Internet
- Abwehr von Bedrohungen am Endpunkt
- Schutz vor Phishing und Diebstahl von Anmeldedaten
- Quarantäne für Geräte mit Sicherheitsproblemen; Entscheidung über Quarantäne anhand unveränderlicher Kriterien

URL-Filtering
- Durchsetzung annehmbarer Benutzerrichtlinien
- Gefilterter Zugriff auf bösartige Domains und nicht jugendfreie Inhalte
- Verhinderung des Gebrauchs von Vermeidungs- und Umgehungstools
- Sicherer Zugriff auf SaaS-Anwendungen
- Zugriffskontrolle und Durchsetzung von Richtlinien für SaaS-Anwendungen bei gleichzeitigem Blockieren unzulässiger Anwendungen

Richtlinien für eigene Geräte der Benutzer (Bring Your Own Device)
- VPN-Unterstützung auf Anwendungsebene zum Schutz der Benutzerdaten
- Sicherer, clientloser Zugriff für Partnerunternehmen, Geschäftspartner und Auftragnehmer
- Unterstützung der automatischen Identifizierung privater Geräte
- Unterstützung individuell angepasster Authentifizierungsmechanismen für verwaltete und private Geräte

Zero-Trust-Implementierung
- Ermöglicht verlässliche Benutzeridentifizierung
- Liefert unmittelbare und genaue Hostinformationen für eine bessere Übersicht und Durchsetzung von Richtlinien
- Durchsetzung fortschrittlicher Mehrfaktorauthentifizierung (MFA) beim Zugriff auf sensible Ressourcen

Externe Ausweitung des Plattformschutzes

GlobalProtect schützt Ihre mobilen Mitarbeiter: Unsere Next-Generation Firewalls überprüfen den gesamten Datenverkehr und dienen als Internetgateways im Perimeter, in der Entmilitarisierten Zone (DMZ) oder in der Cloud. Laptops, Smartphones und Tablets mit der GlobalProtect App richten automatisch eine sichere IPsec/SSL-VPN-Verbindung mit der Next-Generation Firewall ein. Dabei wird stets das beste Gateway verwendet, sodass Netzwerkdatenverkehr, Anwendungen, Ports und Protokolle uneingeschränkt sichtbar sind. Wenn Ihre Organisation die blinden Flecken im Datenverkehr der mobilen Mitarbeiter ausleuchtet, kann sie systematisch erfassen, wie Anwendungen genutzt werden.

Die Implementierung von Zero Trust in Ihrem Netzwerk

Es ist nicht notwendig, dass alle Benutzer auf alle Ressourcen im Netzwerk Ihrer Organisation zugreifen können. Daher verfolgen Sicherheitsteams einen Zero-Trust-Ansatz. Sie segmentieren also ihre Netzwerke und unterwerfen den Zugriff auf interne Ressourcen einer genauen Kontrolle. Mit GlobalProtect erhalten Sie eine Lösung, die Standards setzt. Die Lösung ermöglicht die schnellste Benutzeridentifikation für die Plattform, sodass Sie anhand präziser Richtlinien bedarfsorientiert festlegen können, wer welchen Zugriff erhält. Darüber hinaus liefert GlobalProtect Hostinformationen, anhand derer gerätebezogene Compliancekriterien erstellt und mit Sicherheitsrichtlinien verknüpft werden. Diese Maßnahmen ermöglichen Ihnen präventive Schritte zur Sicherung Ihrer internen Netzwerke, die Einführung von Zero-Trust-Netzwerkkontrollen und eine Minimierung der Angriffsfläche.

Wenn Sie GlobalProtect in dieser Weise einsetzen, können die internen Netzwerkgateways mit oder ohne VPN-Tunnel konfiguriert werden. Darüber hinaus können Sie mit GlobalProtect angegriffene Geräte unter Quarantäne stellen, indem Sie die unveränderlichen Merkmale eines Endpunkts verwenden. So können die Administratoren den Netzwerkzugriff einschränken und verhindern, dass der befallene Endpunkt weitere Benutzer und Geräte infiziert. Bei einem Angriff können Quarantäneregeln bei Geräten innerhalb und außerhalb des Netzwerks angewendet werden.

Überprüfung des Datenverkehrs und Durchsetzung von Sicherheitsrichtlinien

Mit GlobalProtect können Sicherheitsteams eine konsistente Richtlinienumsetzung gewährleisten. Dabei spielt es keine Rolle, ob sich Benutzer in externen oder internen Netzwerken befinden. Alle Möglichkeiten der Plattform stehen zur Verfügung, um Cyberattacken zu verhindern:

- **App-ID™** ist eine Technologie, die den Datenverkehr durch Anwendungen unabhängig von der Portnummer identifiziert und Organisationen in die Lage versetzt, mithilfe geeigneter Richtlinien die Nutzung von Anwendungen nach Benutzern und Geräten zu verwalten.
- **User-ID™** schafft Transparenz durch die Identifizierung von Benutzern und Gruppenmitgliedern und ermöglicht die Durchsetzung rollenbasierter Richtlinien zur Netzwerksicherheit.
- **SSL-Entschlüsselung** prüft und kontrolliert Anwendungen, die mit SSL/TLS/SSH verschlüsselt sind und wendet Bedrohungen innerhalb des verschlüsselten Datenverkehrs ab.
- **WildFire®**-Malwareschutz automatisiert die Inhaltsanalyse und identifiziert so neue, bisher unbekannte und äußerst zielgerichtete Malware anhand ihres Verhaltens. So können die notwendigen Informationen gesammelt werden, um die Bedrohung nahezu in Echtzeit zu stoppen.

- **Threat Prevention** für IPs und Antivirus blockiert netzwerkbasierte Exploits, die sich mit Denial-of-Service-Angriffen (Nichtverfügbarkeit des Dienstes, DoS) und Portscans gegen Anwendungen und Betriebssysteme mit Sicherheitslücken richten. Antivirusprofile verhindern, dass Spyware und Malware über eine datenstrombasierte Engine zum Endpunkt vordringen.
- **URL-Filtering mit PAN-DB:** URLs werden nach Content auf der Domain-, Datei- und Seitenebene kategorisiert; sie erhalten Updates von WildFire, damit sich bei Änderungen am Web-Content auch die Kategorisierungen anpassen.
- **Dateiblockaden:** stoppen die Übertragung unerwünschter oder gefährlicher Dateien und überprüft zulässige Dateien mit WildFire.
- **Das Filtern von Daten** ermöglicht Administratoren die Implementierung von Richtlinien gegen unzulässigen Datenverkehr, wie etwa die Übertragung von Kundendaten oder anderer vertraulicher Daten.

Sichere Zugriffskontrolle

Benutzerauthentifizierung

GlobalProtect unterstützt alle vorhandenen PAN-OS®-Authentifizierungsmethoden, einschließlich Kerberos, RADIUS, LDAP, SAML 2.0, Clientzertifikate, biometrische Anmeldung und lokale Benutzerverzeichnisse. Sobald GlobalProtect den Benutzer authentifiziert hat, liefert es der Next-Generation Firewall sofort eine Zuordnung des Benutzers zur IP-Adresse für User-ID.

Leistungsfähige Authentifizierungsoptionen

GlobalProtect unterstützt verschiedene Mehrfaktor-authentifizierungsmethoden (MFA) von Drittanbietern, einschließlich One-Time-Password (Einmalkennwort, OTP), Zertifikat und Smartcard über eine RADIUS- und SAML-Integration.

Mit diesen Optionen können Unternehmen ihre Identitätskontrolle beim Zugriff auf interne Rechenzentrums- oder Software-as-a-Service-(SaaS-)Anwendungen stärken.

Mit den Optionen von GlobalProtect ist eine leistungsfähige Authentifizierung noch leichter nutzbar und einsetzbar:

- **Cookiebasierte Authentifizierung:** Nach der Authentifizierung können Sie über ein verschlüsseltes Cookie auf ein Portal oder ein Gateway zugreifen, solange dieses Cookie gültig ist.
- **Unterstützung für Simplified Certificate Enrollment Protocol (SCCP):** GlobalProtect kann die Interaktion mit der Public Key Infrastructure (PKI) eines Unternehmens für die Verwaltung, Ausgabe und Verteilung von Zertifikaten an GlobalProtect-Clients automatisieren.
- **MFA:** Ehe ein Benutzer auf eine Anwendung zugreifen kann, muss er oder sie sich möglicherweise auf eine weitere Art authentifizieren.

Host Information Profile

GlobalProtect prüft die Konfiguration des Endpunkts und erstellt ein Host Information Profile (HIP). Dieses wird mit der Next-Generation Firewall geteilt. Die Next-Generation Firewall nutzt das HIP zur Durchsetzung von Anwendungsrichtlinien, die einen Zugriff nur erlauben, wenn der Endpunkt korrekt konfiguriert und abgesichert ist. Diese Prinzipien erleichtern die Durchsetzung von Richtlinien, die den Zugang eines bestimmten Benutzers über ein bestimmtes Gerät genauer definieren.

HIP-Richtlinien können auf einer ganzen Reihe von Attributen beruhen, wie etwa:

- Identifizierung verwalteter oder privater Geräte
- Maschinenzertifikate auf dem Gerät
- Vom Mobilgerätemanager erhaltene Geräteinformationen
- Betriebssystem- und Anwendungspatchebene
- Version und Status der Hostantimalware
- Version und Status der Hostfirewall
- Konfiguration der Festplattenverschlüsselung
- Back-up-Produktkonfiguration
- Individuell angepasste Hostbedingungen (z. B. Registrierungseinträge, laufende Software)

Zugriffskontrolle für Anwendungen und Daten

Sicherheitsteams können Richtlinien anhand der Anwendung, des Benutzers, des Inhalts oder der Hostinformationen erstellen. So behalten sie die detaillierte Kontrolle des Zugriffs auf eine bestimmte Anwendung. Diese Richtlinien können mit bestimmten, in einem Verzeichnis festgehaltenen Benutzern oder Gruppen verknüpft werden, damit Organisationen den Zugriff nach Bedarf justieren können. Darüber hinaus kann das Sicherheitsteam Richtlinien für eine verbesserte MFA festlegen, sodass vor dem Zugriff auf besonders sensible Ressourcen und Anwendungen ein zusätzlicher Identitätsnachweis abgefragt wird.

Bessere Fehlerbehebung und Transparenz

Die Widgets des GlobalProtect Application Command Center (ACC), die Berichte und das neue GlobalProtect-Protokoll schaffen Transparenz über die GlobalProtect-Nutzung in Ihrem Bereich. Ein genaues Protokoll des Verbindungsworkflows in verschiedenen Stadien vereinfacht die Fehlerbehebung bei Verbindungsproblemen von Benutzern deutlich. Mit dem Protokoll können Administratoren ganz einfach den Status/das Event bei dem Verbindungsvorgang identifizieren, der einem bestimmten Benutzer Probleme bereitet.

Sicheres und aktiviertes BYOD

Durch die BYOD-Richtlinien (BYOD = Bring Your Own Device) ändert sich die Anzahl der Anwendungsfälle, in denen Sicherheitsteams Support leisten müssen. Eine breiteres Spektrum an Mitarbeitern und Auftragnehmern benötigt Zugriff auf Anwendungen, wobei die verschiedensten Mobilgeräte verwendet werden.

Die Integration mit einer mobilen Geräteverwaltung wie AirWatch® oder MobileIron® unterstützt Sie dabei, GlobalProtect zu nutzen sowie durch den Austausch von Erkenntnissen und die richtige Hostkonfiguration zusätzliche Sicherheit zu gewährleisten. So kann Ihre Organisation mit GlobalProtect und weiteren Maßnahmen die notwendige Transparenz sicherstellen und Sicherheitsrichtlinien für jede einzelne Anwendung durchsetzen. Zugleich ist bei privaten Aktivitäten die separate Datenverarbeitung gewährleistet, sodass die Privatsphäre des Benutzers auch im BYOD-Einsatz gewahrt ist.

GlobalProtect unterstützt clientlose SSL-VPN-Verbindungen, die im Rechenzentrum und in der Cloud auch über private Geräte einen sicheren Zugriff auf Anwendungen ermöglichen. So können Kunden über ein Web-Interface den eigenen Angestellten und externen Benutzern den sicheren BYOD-Zugriff auf bestimmte Anwendungen anbieten. Die Benutzer müssen weder einen Client installieren noch benötigen sie einen VPN-Tunnel.

Auf die Infrastruktur kommt es an

Die flexible GlobalProtect-Infrastruktur mit ihren vielfältigen Ressourcen hilft Ihnen, eine ganze Reihe von Sicherheitsproblemen zu lösen. Grundsätzlich kann GlobalProtect das herkömmliche VPN-Gateway ersetzen, was Ihnen die komplexe und mitunter nervenaufreibende Verwaltung eines separaten Drittanbietergateways erspart.

In den Optionen können Sie die manuellen Verbindungen und die Gatewayauswahl optimal an Ihre Bedürfnisse anpassen.

Sie können Ihren Datenverkehr auch noch umfassender mit GlobalProtect schützen, indem Sie eine dauerhaft aktive VPN-Verbindung mit einem vollständigen Tunnel nutzen. So ist ein permanenter und für den Benutzer transparenter Schutz gewährleistet. Für latenzempfindlichen Datenverkehr über bestimmte Anwendungen, Domainnamen und Routen, oder auch bei der Videoübertragung, sind Ausnahmen möglich.

Cloudbasierte Gateways

Wenn Mitarbeiter ihren Standort wechseln, intensiviert sich der Datenverkehr. Das gilt besonders in bestimmten Szenarien der Unternehmensentwicklung, je nachdem, ob diese vorübergehend (etwa nach einer Naturkatastrophe) oder dauerhaft (z. B. beim Eintritt in neue Märkte) stattfindet.

Prisma™ Access von Palo Alto Networks bietet eine gemeinsam verwaltete Lösung, die überall dort, wo das Unternehmen es benötigt, den Zugriff unter Einhaltung der Sicherheitsrichtlinien ermöglicht. Sie kann mit Ihren vorhandenen Firewalls kombiniert werden, sodass sich Ihre Infrastruktur flexibel an Veränderungen anpassen kann.

Prisma Access unterstützt die automatische Skalierung, bei der regional je nach Last und Nachfrage die Firewall gewechselt wird.

Fazit

Die Next-Generation Firewall von Palo Alto Networks trägt wesentlich zum Schutz vor Sicherheitslücken bei. GlobalProtect erweitert für Sie den Schutz der Plattform, und zwar unabhängig vom Standort der Benutzer. Mit GlobalProtect können Sie Ihre Sicherheitsrichtlinien konsequent durchsetzen. Selbst wenn Benutzer das Gebäude verlassen, bleiben sie vor Cyberattacken geschützt.

Tabelle 1: Funktionen von GlobalProtect

Kategorie	Spezifikation
VPN-Verbindung	IPSec
	SSL
	Clientlose VPN-Verbindung
	Per-App-VPN unter Android oder iOS
Gatewayauswahl	Automatische Auswahl
	Manuelle Auswahl
	Bevorzugte Gatewayauswahl
	Externe Gatewayauswahl anhand des Quellenstandorts
	Interne Gatewayauswahl anhand der Quellen-IP
Verbindungsmethoden	Benutzeranmeldung (dauerhaft aktiv)
	Bei Bedarf
	Vor der Anmeldung (dauerhaft aktiv)
	Vor der Anmeldung, anschließend nach Bedarf
	Vor der Anmeldung, durch den Benutzer
Verbindungsart	Interner Modus
	Externer Modus
Layer-3-Protokolle	IPv4
	IPv6
Single Sign-On (einmaliges Anmelden, SSO)	SSO (Windows Credential Provider)
	Kerberos SSO
	SSO für MacOS
Split Tunneling	Routen, Domains und Anwendungen einbeziehen
	Routen, Domains und Anwendungen ausschließen

Tabelle 1: Funktionen von GlobalProtect (Fortsetzung)	
Authentifizierungsmethoden	SAML 2.0
	LDAP
	Clientzertifikate
	Kerberos
	RADIUS
	Zwei-Faktor-Authentifizierung
	Auswahl der Authentifizierungsmethode je nach Betriebssystem oder Geräteeigentümer
HIP-Berichte, Durchsetzung von Sicherheitsrichtlinien, Benachrichtigungen	Patchmanagement
	Hostantispyware
	Hostantimalware
	Hostfirewall
	Festplattenverschlüsselung
	Festplattenbackup
	Data Loss Prevention (Schutz vor Datenverlust, DLP)
	Individuell angepasste HIP-Bedingungen (z. B. Registrierungseinträge, laufende Software)
Identifizierung verwalteter Geräte	Durch Maschinenzertifikate
	Durch Hardwareseriennummern
MFA	Zum Verbindungszeitpunkt und zum Zeitpunkt des Zugriffs auf die Ressource
Sonstige Merkmale	User-ID
	IPsec-Rückgriff auf SSL-VPN
	Erzwingen der GlobalProtect-Verbindung beim Netzwerkzugang
	Tunnelkonfiguration anhand Benutzerstandort
	Weitergabe von HIP-Berichten
	Zertifikatsprüfung in HIP
	SCEP-basiertes automatisches Management von Benutzerzertifikaten
	Scripthandlungen vor und nach Sitzungen
	Individuelle Anpassung der Dynamic GlobalProtect App
	Anwendungskonfiguration je nach Benutzer, Gruppe und/oder Betriebssystem
	Automatische interne/externe Erkennung
	Manuelles/automatisches Upgrade der GlobalProtect App
	Zertifikatsauswahl durch OID
	Zugriff sperren für verlorene, gestohlene oder unbekannte Geräte
	Smartcard-Unterstützung beim Verbinden/Trennen
	Transparente Distribution vertrauenswürdiger Root-CAs für die SSL-Entschlüsselung
	Deaktivierung des direkten Zugriffs auf lokale Netzwerke
	Anpassbare Begrüßungs- und Hilfeseiten
	RDP-Verbindung mit Remoteclient
	Betriebssystemeigene Benachrichtigungen
	Beschränkung der Benutzerabmeldung
	Proxyunterstützung
	Durchsetzung der GlobalProtect-Ausschlussregeln
	Verbindung ausschließlich via SSL
	RSA-Softwaretokenintegration
	Quarantänemaßnahmen für Geräte

Tabelle 1: Funktionen von GlobalProtect (Fortsetzung)	
MDM-/EMM-Integration	AirWatch
	MobileIron
	Microsoft Intune
Verwaltungstools und -APIs	Next-Generation Firewalls von Palo Alto Networks, einschließlich physischer und virtueller Appliances
	Prisma Access
	Panorama-Netzwerksicherheitsmanagement
Von der GlobalProtect App unterstützte Plattformen	Microsoft Windows und Windows UWP
	Apple macOS
	Apple iOS und iPadOS
	Google Chrome OS
	Android
	Linux (Red Hat, CentOS, Ubuntu)
	IoT-Geräte
IPsec XAuth	Apple iOS IPsec Client
	Android OS IPsec Client
	Drittanbieter-VPNC und strongSwan-Client
GlobalProtect App-Lokalisierung	Chinesisch, Englisch, Französisch, Deutsch, Japanisch, Spanisch

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

© 2020 Palo Alto Networks, Inc. Palo Alto Networks ist eine eingetragene Marke von Palo Alto Networks. Eine Liste unserer Marken ist unter https://www.paloaltonetworks.com/company/trademarks.html abrufbar. Alle anderen hier erwähnten Marken können Markenzeichen der jeweiligen Unternehmen sein.. strata-globalprotect-ds-060120