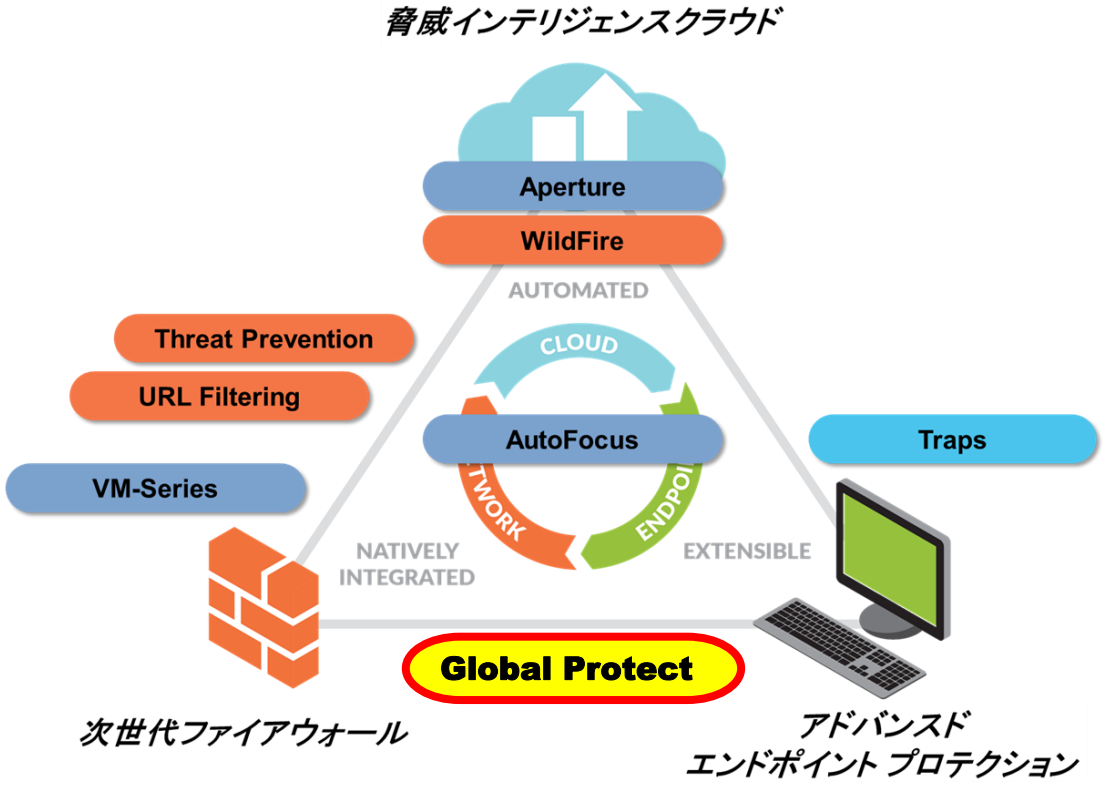
Global Protectのご紹介

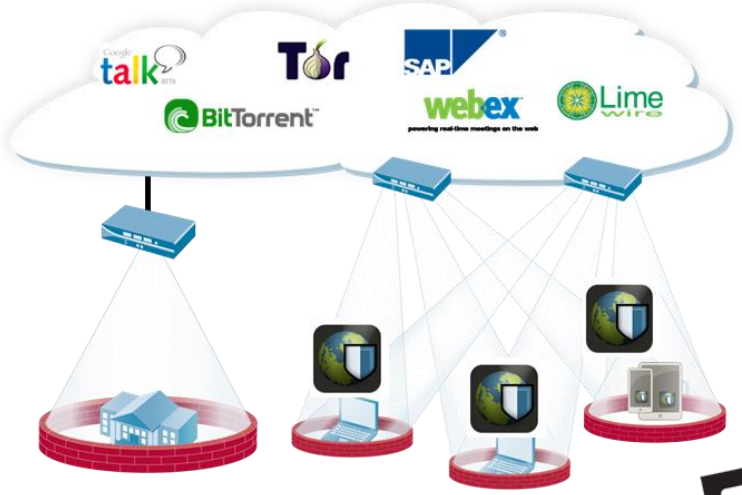
次世代 セキュリティ プラットフォーム



モバイル環境向けソリューション：Global Protect™

- ロケーションに依存しないデバイスの常時保護/可視化/制御をシンプルに実現
  - *対象OS： Windows, Mac OS X, Apple iOS, Google Android*
  - *エージェントがロケーション（内部/外部）を自動判別し、外部の場合にはVPN接続により強制的にPAシリーズ経由で通信を行うように経路変更*
  - *ホスト環境(プロファイル情報)を元にしたアクセス制御（AVソフトの有無, HDD暗号化有無など）*
  - *PAシリーズによるシンプルな一元管理*

- Global Protect の活用例
  - *リモートアクセスVPNからの置き換え(集約)*
  - *クライアント / モバイルデバイスのロケーションに依存しない通信/脅威の可視化と制御*
  - *ユーザ情報を元にしたきめ細やかなアクセス制御*
  - *セキュリティデバイス / 機能集約による TCO削減の実現*

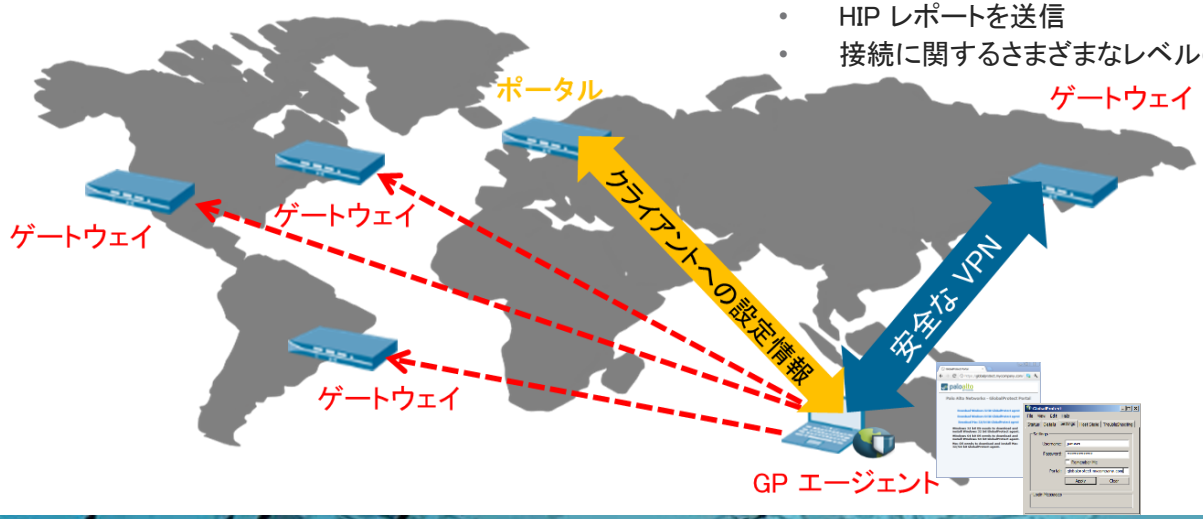


Global Protectのコンポーネント

- Global Protectゲートウェイ
  - 次世代ファイアウォール上で動作
  - モバイルデバイスにIPsec/SSL VPN 接続を提供
  - アプリケーション、ユーザー、コンテンツ、デバイス、デバイス状態でポリシー適用

- Global Protectポータル
  - Global Protectへ接続しようとするユーザーを認証
  - クライアントの設定を保存
  - 内部および外部ゲートウェイのリストを保持
  - GWにおけるクライアント認証用の CA 証明書を管理

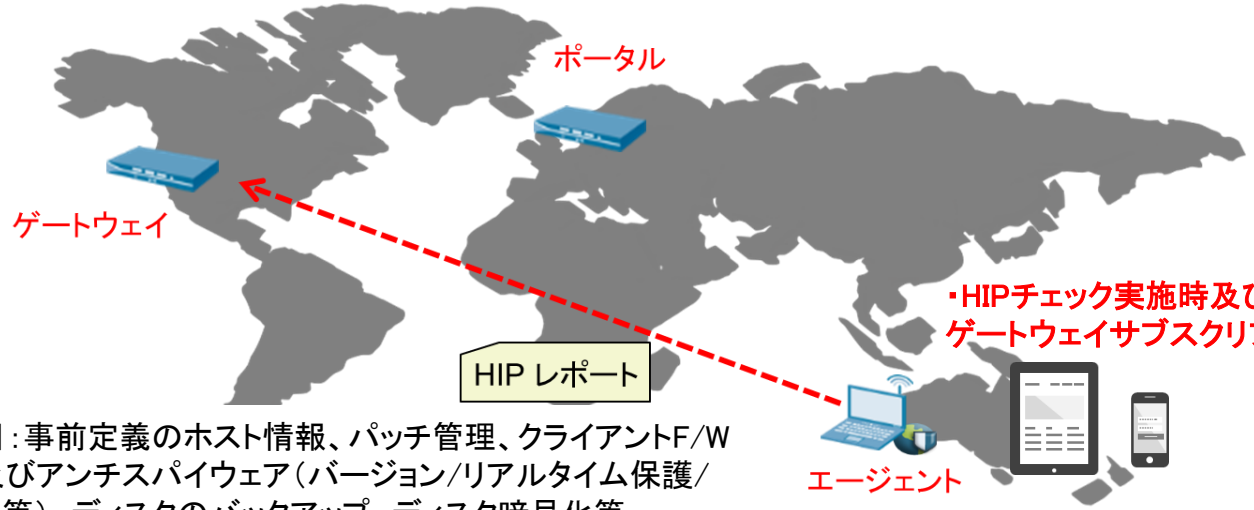
- Global エージェント
  - ポータルへの接続を認証
  - ゲートウェイとの接続を確立
  - HIP レポートを送信
  - 接続に関するさまざまなレベルの制御をユーザーに提供



Global Protectのライセンス体系

※利用ユーザ毎のライセンスも無く、次世代F/W利用時で、HIPチェック＆スマートデバイス無し時は、
ライセンス不要でGlobal Protectの利用が可能（PAN-OS7.0以降）

- ポータルライセンス：PAN-OS6.1まであったポータルライセンスはPAN-OS7.0以降では不要に。
- ゲートウェイサブスクリプション：
  - HIPチェック及び関連付けられたコンテンツ更新が可能な年間サブスクリプション。
  - HIPチェックを実行する各ゲートウェイファイアウォールにインストールする必要あり。
  - iOS及びAndroid用Global Protectモバイルアプリケーションもサポート

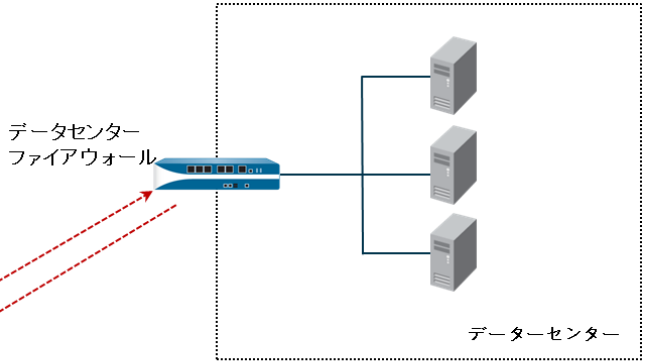


・HIPチェック実施時及び、iOS/Android利用時は、
ゲートウェイサブスクリプションが必要

※HIPチェック項目：事前定義のホスト情報、パッチ管理、クライアントF/W
アンチウイルス及びアンチスパイウェア（バージョン/リアルタイム保護/
最終スキャン時刻等）、ディスクのバックアップ、ディスク暗号化等

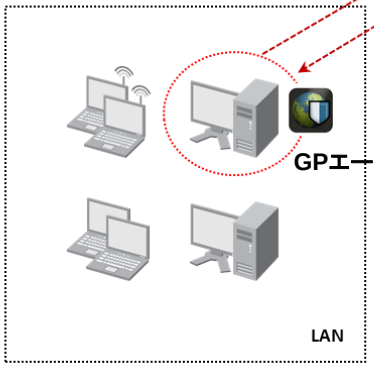
Global Protectエージェントの基本動作（社内LANからのアクセス例）

⑤GPゲートウェイ(PAシリーズファイアウォール)は
受信したユーザ情報や、ホストプロファイル情報を
元にアクセス制御を実行



④GPエージェントはGPゲートウェイに対して
ユーザとホスト情報プロファイルを送信

③GPエージェントは接続先ネットワーク
(内部/外部)の自動判別処理を実行



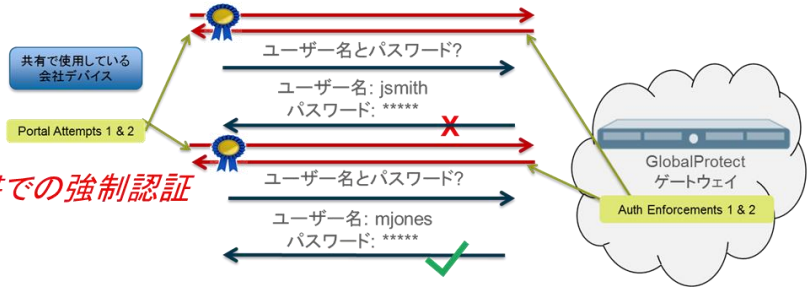
GP ポータル＆ゲートウェイ

②GPポータルはエージェントに以下をプッシュ
- 証明書情報
- 利用可能なGP GWリスト
- Agent S/W Updates(必要な場合)
- 内部/外部ネットワーク検出の必要情報
- ホストチェック実行項目

①GPエージェントはGPポータルに
接続しユーザ認証を実行

Global Protect接続形式

on-demand	user-logon	pre-logon
		
ユーザーは明示的にGlobalProtectに接続する必要がある。	ユーザーがログオンするとGlobalProtectへの接続が開始される。	GlobalProtectへの接続はユーザーがログインする前から実施される

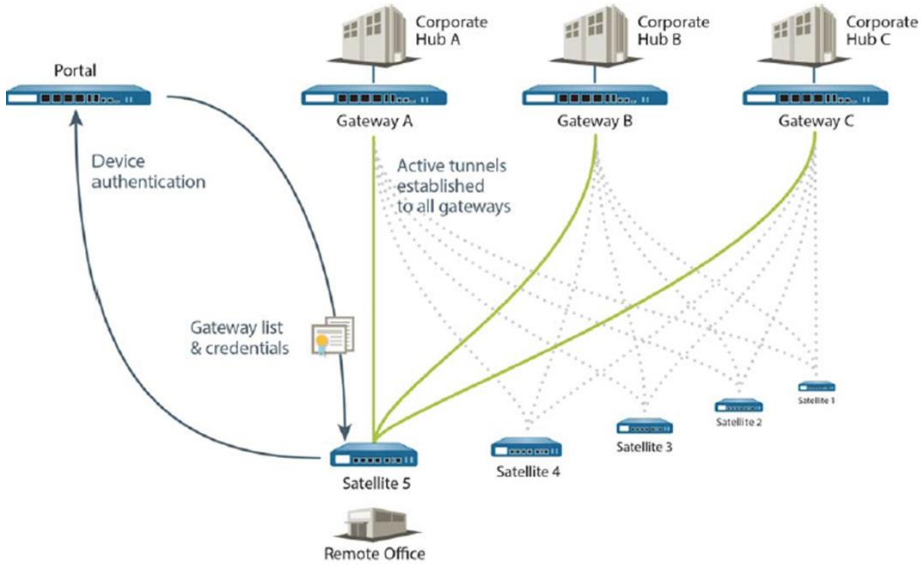


※ユーザー 証明書での強制認証

- GPポータルをシステムの認証局 (CA) として利用可能 (ポータル内自己署名orインポートした下位 CA 発行証明書を使用)。
- お客様独自の CA を使用して証明書を生成可能(ただしポータル、ゲートウェイ、クライアント は、同一CA の証明書利用が必要)。

Global Protectサテライトによる大規模VPN

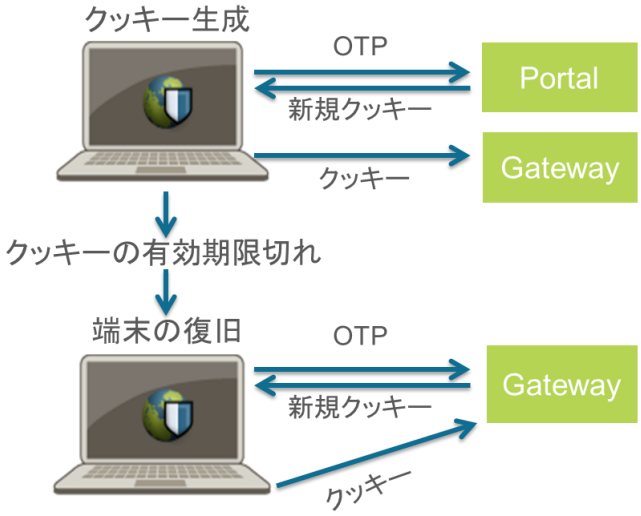
- Global Protect サテライトから既存のポータルとゲートウェイに接続
- 標準クライアントと同様にポータルからネットワークとルーティングの情報を受信
- サテライト デバイスでのデプロイメント タスクは最小限
- サテライトを複数のゲートウェイに同時に接続できる



参考情報：PAN-OS7.1で追加された新機能例（二要素認証の強化）

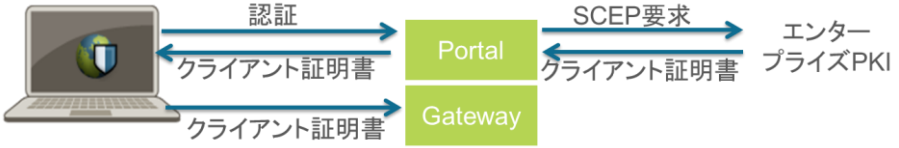
1.クッキー認証による利便性向上

- 二要素認証で、ユーザがOTP（ワンタイムパスワード）の入力回数を減らし、Global Protectポータルとゲートウェイへのユーザログインを一回のみに
- ユーザ認証後に、GlobalProtectは暗号化されたクッキーを作成。
- ユーザはクッキーを用いて、有効期間内のログイン保持が可能（24時間）。
- スリープ状態からの復旧時は、有効期間内であれば、ユーザが入力する認証情報の代わりにクッキーを用いて認証を実施。



2.SCEPによるクライアント証明書の配布

- エンタープライズPKIによるクライアント認証時に、証明書を簡単且つ安全にユーザに送付する為、Global Protectポータルが SCEP（Simple Certificate Enrollment Protocol）クライアントとなり、エンタープライズPKIからの証明書の入手と、クライアント端末へのインストールを透過的に行う機能を追加。
- 有効なクライアント証明書を持つ端末のみゲートウェイに接続可能。



参考情報：PAN-OS7.1で追加された新機能例
（WindowsおよびMac OS版Global Protectアプリ UIのシンプル化）

- WindowsおよびMac OS向けのGlobalProtectアプリ3.0で、ユーザインタフェースがより見やすくシンプルに
  - StatusタブとSettingsタブをHomeタブとして統合。GP Portalにログインしたり、接続状況の確認が可能に
  - 他タブでは接続の詳細や統計、ホストの状況、トラブルシューティング用の情報を提供