GlobalProtect

GlobalProtect は、Palo Alto Networks Next-Generation Firewall による保護を、あらゆる場所に移動するモバイル ワーカーにまで拡張します。

ユーザーやアプリケーションの場所が従来のネットワーク境界を越えるようになるにつれ、保護を必要とする領域はますます広がっています。セキュリティ チームは、ネットワーク トラフィックに対する可視性を維持し、セキュリティ ポリシーを適用して、脅威を阻止しようとしていますが、難しい問題に直面しています。ホスト エンドポイントのアンチウイルス ソフトウェアやリモート アクセス仮想プライベート ネットワーク (VPN) など、モバイル エンドポイントの保護に使用されていた従来のテクノロジでは、高度な技術を持つ今日の攻撃者が利用する高度なテクニックを阻止することはできません。

エンドポイント向け GlobalProtect™ネットワーク セキュリティは、場所に関係なくすべてのユーザーに Palo Alto Networks Next-Generation Firewall を拡張することによって、モバイル ワーカーを保護できるようにします。さらに、アプリケーションの用途の把握、トラフィックとユーザーやデバイスの関連付け、次世代テクノロジによるセキュリティ ポリシーの適用といったプラットフォームの機能を使用して、トラフィックを保護します。

主な使用シナリオと利点

リモート アクセス VPN

- 社内およびクラウドベースのビジネス アプリケーションへの安全なアクセスを提供します。

高度な脅威に対する防御

- インターネット トラフィックを保護します。
- 脅威がエンドポイントに到達するのを阻止します。
- フィッシングと認証情報の盗難から保護します。
- 変わることのない特性を利用して、侵害されたデバイスを隔離します。

URL フィルタリング

- 利用規定を適用します。
- 悪意のあるドメインとアダルト コンテンツへのアクセスをフィルタリングします。
- 回避ツールの使用を阻止します。
- SaaS アプリケーションへのアクセスを保護します。
- 未認可アプリケーションをブロックしながら、SaaS アプリケーションに対するアクセスを制御し、ポリシーを適用します。

BYOD (Bring-Your-Own-Device) ポリシー

- ユーザーのプライバシーを保護するためのアプリケーションレベルの VPN をサポートします。
- パートナー、提携業者、下請業者からの安全なクライアントレス アクセスを実現します。
- 管理対象外デバイスの自動識別をサポートします。
- 管理対象デバイスと管理対象外デバイス向けにカスタマイズされた認証メカニズムをサポートします。

ゼロトラストの実装

- 信頼性の高い User-ID を提供します。
- 可視性を向上させ、ポリシーを適用するための、正確なホスト情報を迅速に提供します。
- 機密リソースへのアクセスにステップアップ多要素認証を適用します。

プラットフォームの保護を外部まで拡張

GlobalProtect は、境界、DMZ (非武装地帯)、またはクラウドのいずれであろうと、インターネット ゲートウェイとして配置されている次世代ファイアウォールを使用してすべてのトラフィックを検査することで、モバイル ワーカーを保護します。GlobalProtect アプリケーションが動作しているノートパソコン、スマートフォン、タブレットは自動的に最適なゲートウェイを使用して次世代ファイアウォールへの安全な IPsec/SSL VPN 接続を確立し、すべてのネットワーク トラフィック、アプリケーション、ポート、プロトコルを完全に可視化します。モバイル ワーカーのトラフィックの盲点を解消することによって、組織はアプリケーションを一貫して監視し続けることができるようになります。

ネットワークでのゼロ トラストの実装

必ずしもすべてのユーザーが企業ネットワーク内のすべての資産にアクセスする必要があるわけではありません。セキュリティ チームは、ゼロ トラストの原則に基づいてネットワークを分割し、内部リソースへのアクセスを詳細に制御します。GlobalProtect は、最も高速で信頼できる User-ID をプラットフォームに提供して、ビジネス ニーズに基づいてアクセスを許可または制限するための詳細なポリシーを記述できるようにします。また、GlobalProtect は、セキュリティ ポリシーに関連付けるデバイス コンプライアンス基準を定めるホスト情報を提供します。これにより、内部ネットワークの保護、ゼロ トラストによるネットワーク制御の採用、攻撃のリスクの軽減を目的とする再発防止策を講じることができます。

ここで説明したような方法で GlobalProtect が導入されている場合、内部ネットワーク ゲートウェイは、VPN トンネルあり、または VPN トンネルなしのいずれでも設定できます。

さらに、GlobalProtect を使用すると、エンドポイントの変わることのない特性を利用して、侵害されたデバイスを隔離できます。これにより、管理者は、ネットワークへのアクセスを限定し、侵害されたエンドポイントが他のユーザーやデバイスを感染させるのを防ぐことができます。隔離による制限は、侵害されたデバイスが外部ネットワークと内部ネットワークのどちらにある場合でも、適用できます。

トラフィックの検査と セキュリティ ポリシーの適用

GlobalProtect を使用すると、セキュリティ チームは、内部ユーザーまたはリモート ユーザーのどちらにも一貫して適用されるポリシーを作成できます。セキュリティ チームは、次に示すプラットフォームの機能をすべて活用して、サイバー攻撃を防ぐことができます。

- App-ID™テクノロジは、ポート番号に関係なくアプリケーション トラフィックを識別し、組織がユーザーとデバイスに基づいてアプリケーションの使用を管理するポリシーを設定できるようにします。
- User-ID™テクノロジは、ユーザーとグループ メンバーシップを識別して、可視性を向上するとともに、ロールベースのネットワーク セキュリティ ポリシーを適用することができるようにします。
- **SSL 復号化**は、SSL/TLS/SSH トラフィックで暗号化されているアプリケーションを検査および制御して、暗号化されているトラフィック内の脅威を阻止します。
- **WildFire® マルウェア防御サービス**は、コンテンツの分析を自動化して、標的を絞り込んだこれまで知られていない新しいマルウェアをその振る舞いに基づいて識別し、脅威インテリジェンスを生成してほぼリアルタイムに阻止します。

- IPS やアンチウイルス向けの **Threat Prevention** は、脆弱性のあるアプリケーションやオペレーティング システムを標的とするネットワークベースのエクスプロイト、サービス拒否 (DoS) 攻撃、ポート スキャンをブロックします。アンチウイルス プロファイルは、ストリームベースのエンジンを使用して、マルウェアやスパイウェアがエンドポイントに到達するのを阻止します。
- **PAN-DB による URL Filtering** は、URL をコンテンツに基づいてドメイン レベル、ファイル レベル、ページ レベルで分類し、Web コンテンツが変更された場合に分類も変更されるように WildFire から更新を受け取ります。
- **ファイル ブロック**は、許可されたファイルについて WildFire を使用して詳しく調べると同時に、不要かつ危険なファイルの転送を阻止します。
- **データ フィルタリング**は、管理者が、顧客情報や他の機密コンテンツの転送など、データの不正な移動を阻止するために使用できるポリシーを適用できるようにします。

安全なアクセス制御

ユーザー認証

GlobalProtect は、Kerberos、RADIUS、LDAP、SAML 2.0、クライアント証明書、バイオメトリック サインイン、ローカル ユーザー データベースなど、既存の PAN-OS® 認証メソッドをすべてサポートします。GlobalProtect は、ユーザーを認証するとすぐに、User-ID で使用するユーザーと IP アドレスのマッピングを次世代ファイアウォールに提供します。

強力な認証オプション

GlobalProtect は、RADIUS と SAML の統合により、ワンタイム パスワード トークン、証明書、スマート カードなど、幅広いサードパーティ多要素認証 (MFA) 方法をサポートします。

これらのオプションは、組織が内部のデータセンターまたは SaaS (Software-as-a-Service) のアプリケーションにアクセスするための身分証明の強化に役立ちます。

GlobalProtect には、強力な認証の使用と導入をより簡単にするためのオプションがあります。

- **Cookie を使用した認証**: 認証後に、Cookie が有効な間は暗号化された Cookie が以降のポータルまたはゲートウェイへのアクセスで使用されるようにすることができます。
- **SCEP (Simple Certificate Enrollment Protocol) のサポート**: GlobalProtect は、証明書を管理、発行し、GlobalProtect クライアントに配布するための、エンタープライズ公開鍵インフラストラクチャ (PKI) とのやりとりを自動化できます。
- **MFA**: アプリケーションにアクセスするユーザーに別の形式の認証も提示するよう要求できます。

ホスト情報プロファイル

GlobalProtect は、エンドポイントをチェックしてその設定内容のインベントリを取得し、次世代ファイアウォールと共有するホスト情報プロファイル (HIP) を構築します。次世代ファイアウォールはこの HIP を使用して、正しく設定されて保護されているエンドポイントにのみアクセスを許可するアプリケーション ポリシーを適用します。これらの原則は、特定のユーザーの特定のデバイスに対するアクセスの量を管理するポリシーを順守するのに役立ちます。

HIP ポリシーでは、次のような多数の属性を使用できます。

- 管理対象 / 非管理対象デバイスの識別
- デバイスに存在するマシン証明書
- モバイル デバイス マネージャから受信するデバイス情報
- オペレーティング システムとアプリケーションのパッチ レベル
- ホストのアンチマルウェアのバージョンと状態
- ホストのファイアウォールのバージョンと状態
- ディスク暗号化の設定
- データ バックアップ製品の設定
- カスタマイズされたホスト条件 (レジストリ エントリ、実行中のソフトウェアなど)

アプリケーションとデータへのアクセスを制御

セキュリティ チームは、特定のアプリケーションへのアクセスを詳細に制御し続けるために、アプリケーション、ユーザー、コンテンツ、ホストの情報に応じてポリシーを確立することができます。これらのポリシーをディレクトリに定義されている特定のユーザーまたはグループと関連付けることによって、組織がビジネス ニーズに基づいて適切なレベルでのアクセスを許可できるようになります。セキュリティ チームはさらに、ステップアップ MFA のポリシーを設定して、特に機密性の高いリソースやアプリケーションにアクセスする前に追加で身分証明を提供させることができます。

トラブルシューティングと可視性の強化

GlobalProtect Application Command Center (アプリケーション コマンド センター - ACC) のウィジェット、レポート、新しい GlobalProtect ログは、導入環境での GlobalProtect の使用状況を完全に可視化します。ステージごとに接続ワークフローの詳細なログが記録されるので、ユーザーの接続の問題に関するトラブルシューティングが大幅に簡素化されます。管理者はこのログを使用して、特定のユーザーに問題が発生している接続プロセスのステージ / イベントを簡単に特定できます。

保護された有効な BYOD

BYOD (Bring-Your-Own-Device) ポリシーの影響により、セキュリティ チームが優先順位を付けてサポートする必要があるユースケースの数は変化しています。さまざまなモバイル デバイスを使用するより広範囲の従業員や請負業者がアプリケーションにアクセスできるようにする必要があります。

AirWatch® や MobileIron® などのモバイル デバイス管理製品と統合されているので、インテリジェンスの交換とホストの設定を通じて新たなセキュリティ対策を講じることができるほか、GlobalProtect を導入するのにも役立ちます。これらの製品を GlobalProtect と連携させることで、組織は可視性を維持しながらアプリケーションごとのセキュリティ ポリシーを適用し続けることができる一方で、データを個人の活動から分離したまま、ユーザーが BYOD シナリオで期待するプライバシーを尊重することができます。

GlobalProtect は、クライアントレス SSL VPN をサポートし、管理対象外デバイスからデータセンターやクラウドのアプリケーションへの安全なアクセスを実現します。この方法では、Web インターフェイス経由で特定のアプリケーションへのアクセスを許可することによって、BYOD デバイスから接続するサードパーティ ユーザーと従業員が安全にアクセスできるようにするため、ユーザーはクライアントをインストールしたり VPN トンネルをセットアップしたりする必要がありません。

アーキテクチャの重要性

GlobalProtect の柔軟なアーキテクチャは、さまざまなセキュリティの課題の解決に役立つ多くの機能を提供します。最も基本的なレベルでは、従来の VPN ゲートウェイの代わりに GlobalProtect を使用して、スタンドアロンのサードパーティ VPN ゲートウェイの管理という複雑で頭の痛い問題を解消することができます。

手動接続やゲートウェイ選択のオプションがあるので、必要に応じて設定を調整しながらビジネス要件を満たすことができます。

GlobalProtect は、トラフィックの保護を目的としてより包括的に導入する場合には、フル トンネルの常時 VPN 接続で導入できます。これにより、ユーザーの操作が常に透過的に保護されるようになります。レイテンシの影響を受けるトラフィックには、アプリケーション、ドメイン名とルート、またはビデオ トラフィックによる例外を定義できます。

クラウドベースのゲートウェイ

従業員が作業する場所を変えることによって、トラフィックの負荷に変化が生じます。そうした変化は、一時的 (自然災害の後など) なものであろうと、永続的 (新市場に参入する場合など) なものであろうと、企業をどのようにして発展させていったらよいかを考えるときにはついて回る問題です。

パロアルトネットワークスの Prisma™ Access は、セキュリティ ポリシーを使用して組織が必要とする場所を導入対象とする共同管理オプションを提供します。既存のファイアウォールと併用できるので、条件の変化にアーキテクチャを適応させることができます。

Prisma Access は、オートスケールをサポートしており、特定の地域の負荷と需要に基づいて新しいファイアウォールを動的に割り当てます。

結論

Palo Alto Networks Next-Generation Firewall は、侵害の防止に重要な役割を果たします。GlobalProtect を使用して、ユーザーがどこで作業していても保護されるように、プラットフォームの保護範囲を拡大します。GlobalProtect を使用すると、セキュリティ ポリシーを一貫して適用し、ユーザーが建物から離れていてもサイバー攻撃から保護されるようにすることができます。

表 1: GlobalProtect の特徴

カテゴリ	仕様
VPN 接続	IPsec
	SSL
	クライアントレス VPN
	Android、iOS ではアプリケーションごとの VPN
ゲートウェイ選択	自動選択
	手動選択
	優先ゲートウェイ選択
	送信元の場所による外部ゲートウェイ選択
	送信元 IP による内部ゲートウェイ選択
接続方式	ユーザー ログオン (常にオン)
	オンデマンド
	事前ログオン (常にオン)
	事前ログオンの後はオンデマンド
	ユーザーが開始する事前ログオン
接続モード	内部モード
	外部モード
レイヤー 3 プロトコル	IPv4
	IPv6
シングル サインオン	SSO (Windows 認証プロバイダ)
	Kerberos SSO
	SSO for macOS
スプリット トンネル設定	ルート、ドメイン、アプリケーションを包含
	ルート、ドメイン、アプリケーションを除外

表 1: GlobalProtect の特徴 (続き)	
認証方法	SAML 2.0
	LDAP
	クライアント証明書
	Kerberos
	RADIUS
	2 要素認証
	オペレーティング システムまたはデバイスの所有権に基づいて認証方法を選択
HIP レポート作成、ポリシーの適用、通知	パッチ管理
	ホスト アンチスパイウェア
	ホスト アンチマルウェア
	ホスト ファイアウォール
	ディスク暗号化
	ディスク バックアップ
	データ損失防止 (DLP)
	カスタマイズされた HIP 条件 (レジストリ エントリ、実行中のソフトウェアなど)
管理対象デバイスの識別	マシン証明書を使用
	ハードウェア シリアル番号を使用
MFA	接続時およびリソース アクセス時
他の特徴	User-ID
	IPSec から SSL VPN へのフォールバック
	ネットワーク アクセスに GlobalProtect 接続を適用
	ユーザーの場所に基づくトンネル設定
	HIP レポートの再配信
	HIP で証明書のチェック
	SCEP ベースの自動ユーザー証明書管理
	セッション前後に実行されるスクリプト アクション
	GlobalProtect アプリケーションの動的なカスタマイズ
	ユーザー、グループ、オペレーティング システムに基づくアプリケーション設定
	内部 / 外部の自動検出
	GlobalProtect アプリケーションの手動 / 自動アップグレード
	OID による証明書の選択
	紛失、盗難にあった、または未知のデバイスによるアクセスのブロック
	接続 / 切断のためのスマート カードのサポート
	SSL 復号化を目的とする信頼されたルート CA の透過的な配布
	ローカル ネットワークへの直接アクセスの無効化
	カスタマイズ可能なウェルカム ページとヘルプ ページ
	リモート クライアントへの RDP 接続
	オペレーティング システム ネイティブの通知
	ユーザーのサインアウトの制限
	プロキシのサポート
	GlobalProtect による除外の適用
	SSL 接続のみ
	RSA ソフトウェア トークンの統合
	デバイスの隔離

表 1: GlobalProtect の特徴 (続き)	
MDM/EMM の統合	AirWatch
	MobileIron
	Microsoft InTune
管理ツールと API	Palo Alto Networks Next-Generation Firewall (物理アプライアンスとバーチャル アプライアンスを含む)
	Prisma Access
	Panorama ネットワーク セキュリティ管理
GlobalProtect App がサポートされているプラットフォーム	Microsoft Windows および Windows UWP
	Apple macOS
	Apple iOS および iPadOS
	Google Chrome OS
	Android OS
	Linux OS (Red Hat、CentOS、Ubuntu)
	IoT デバイス
IPsec XAuth	Apple iOS IPsec クライアント
	Android OS IPsec クライアント
	サードパーティ VPNC と strongSwan クライアント
GlobalProtect App のサポート言語	中国語、英語、フランス語、ドイツ語、日本語、スペイン語

paloalto NETWORKS

〒 100-0011
東京都千代田区内幸町 2 丁目 1 番 6 号
日比谷パークフロント 15 階
電話番号 : 03-6205-8061
www.paloaltonetworks.jp

strata-globalprotect-ds-060120