ユニバーサル・ゼロ・トラスト ネットワークアクセスの概要

はじめに

ユニバーサル・ゼロ・トラスト・ネットワーク・アクセス（ZTNA）は、統一されたポリシー・モデルを通じて、デバイスや場所に関係なく、すべてのユーザーに対してゼロ・トラスト原則の一貫した適用を保証します。普遍的なZTNAの採用により、多様なネットワーク・インフラや環境にわたるVPN、MPLS、NACなどの従来のテクノロジーを統合して置き換えることで、セキュアなアクセス管理が簡素化されます。これにより企業は、エンドユーザーに複雑さをもたらすことなくネットワークセキュリティを維持し、運用コストと設備投資を削減しながら効率的な管理効率を実現することができます。

Appgate SDP ユニバーサル ZTNA

Appgate SDP は、検証されたIDとコンテキストに基づいて、ユーザーとリソース間の個別化されたセキュアな接続を動的に作成します。ダイレクトルートアーキテクチャを利用することで、このソリューションは最適なパフォーマンス、最小限のレイテンシーを提供し、すべてのユーザー間およびリソース間の接続を一元的にアクセス制御します。このアプローチにより、遠隔地やオンプレミス、マルチクラウド、レガシーインフラなど、多様な環境のセキュリティ確保に必要な汎用性と制御性を提供します。

Appgate SDP はマルチレイヤー認可を活用し、すべてのユーザーアクセス試行に対してコンテキストを考慮した制御を提供します：

- **シングルパケット認証 (SPA):** このレイヤーは、インフラストラクチャを隠蔽し、ポートを露出させることなく完全に不可視化し、単一のパケットで暗号的に検証されたユーザーのみが通信チャネルにアクセスできるようにします。
- **サインイン時の多要素認証:** ユーザーのデバイスを登録することで、2つ目の認証要素として機能し、盗まれた認証情報による不正アクセスの試みをブロックすることでセキュリティを強化します。
- **認証:** このレイヤーは、SAML や OIDC などの定義された信頼できるソースに対して、ユーザーとデバイスの認証情報を検証します。
- **認可:** ポリシーの割り当て基準は、ユーザー/デバイスの属性を評価し、各ユーザー/デバイスに特定の権限セットを割り当てることを可能にします。
- **アクセス制御:** このレイヤは、ユーザートラフィックをエンタイトルメントと比較し、アクセスポリシーを実施し、アクセス条件を検証し、必要に応じてユーザにアクション（MFAなど）を促します。Appgate SDPは、エンタイトルメントで定義された保護リソースのホスト、ポート、プロトコルに基づき、各ユーザ／デバイスのアクセスを動的に管理する。
- **アラートアクション:** このレイヤは、潜在的な脅威にプロアクティブに対処するために、未承認のポートスキャンなど、リスクの高い行動をブロックし、アラートとともにログに記録するトリガーシステムとして機能します。

使用例

完全なVPNの代替

サードパーティ・アクセス

MPLSからインターネットへのトラフィック移行

ソフトウェア定義広域ネットワーク（SD-WAN）の排除

ネットワーク・アクセス・コントロール（NAC）の置き換え

企業リソースへのブランチ接続

重要な機能

アイデンティティ中心のセキュリティ: 許可され認証されたエンティティのみが特定のネットワーク・リソースにアクセスできることを保証します。

アプリケーション層のアクセス制御: タスクの実行に必要な最小限のアクセスをユーザーに保証します。

ダイナミック・アクセス・ポリシー: ユーザーとデバイスの特定のコンテキストに基づいてアクセスを許可します。

適応型認証: ユーザの行動やコンテクスト要因の変化に対応し、アクセス権限が現在のセキュリティ態勢に適切であることを保証します。

スケーラビリティと高性能: 最適なパフォーマンスを維持しながら、ユーザー数やデバイス数の増加に対応するダイナミックな拡張性があります。

Appgate SDPは、統一されたポリシーエンジンを提供し、ハイブリッドIT、マルチクラウド、本社、支社、データセンターにわたるすべてのユーザー、レガシーアプリとカスタムアプリを含むリソース、ロケーションに対してユニバーサルなZTNAをサポートします。

仕組み

Appgate SDPには、許可されたリソースへのセキュアでダイナミックなアクセスを促進する3つの重要なコンポーネントがあります：

コントローラ:

- トラストブローカーおよびポリシー決定ポイントとして機能
- ユーザを認証し、コンテキストをチェックし、ライブエンタイトルメントトークンを生成します。
- デジタル署名されたトークンをクライアントに送信します。

ゲートウェイ:

- ポリシー実施ポイントとして機能
- クライアントからのエンタイトルメントトークンを検証し、保護されたリソースにアクセスするための動的なセッション固有のマイクロファイアウォールネットワークを確立します。

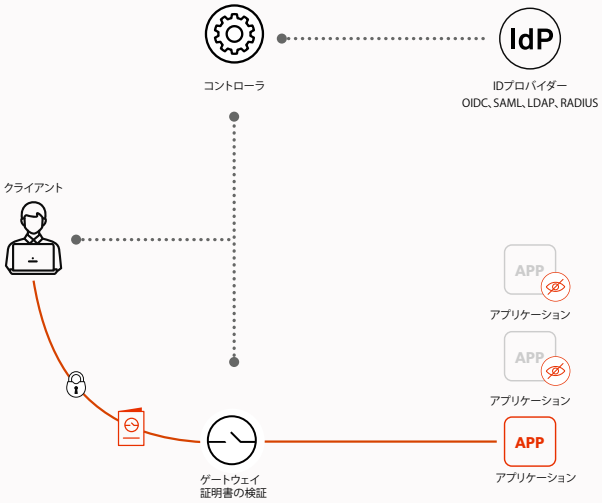
クライアント:

- ユーザー/デバイスを認可されたリソースに接続します。
- SPAエンタイトルメントトークンをコントローラとゲートウェイに送信し、通信を開始します。
- コントローラにアクセスを要求し、エンタイトルメントトークンをゲートウェイに送信して検証します。

クライアントはSPAで保護されたコントローラにアクセス要求を行います。コントローラはSPAパケットを検証し、ユーザーを認証してコンテキストをチェックし、ライブエンタイトルメントトークンを生成してクライアントに送信します。

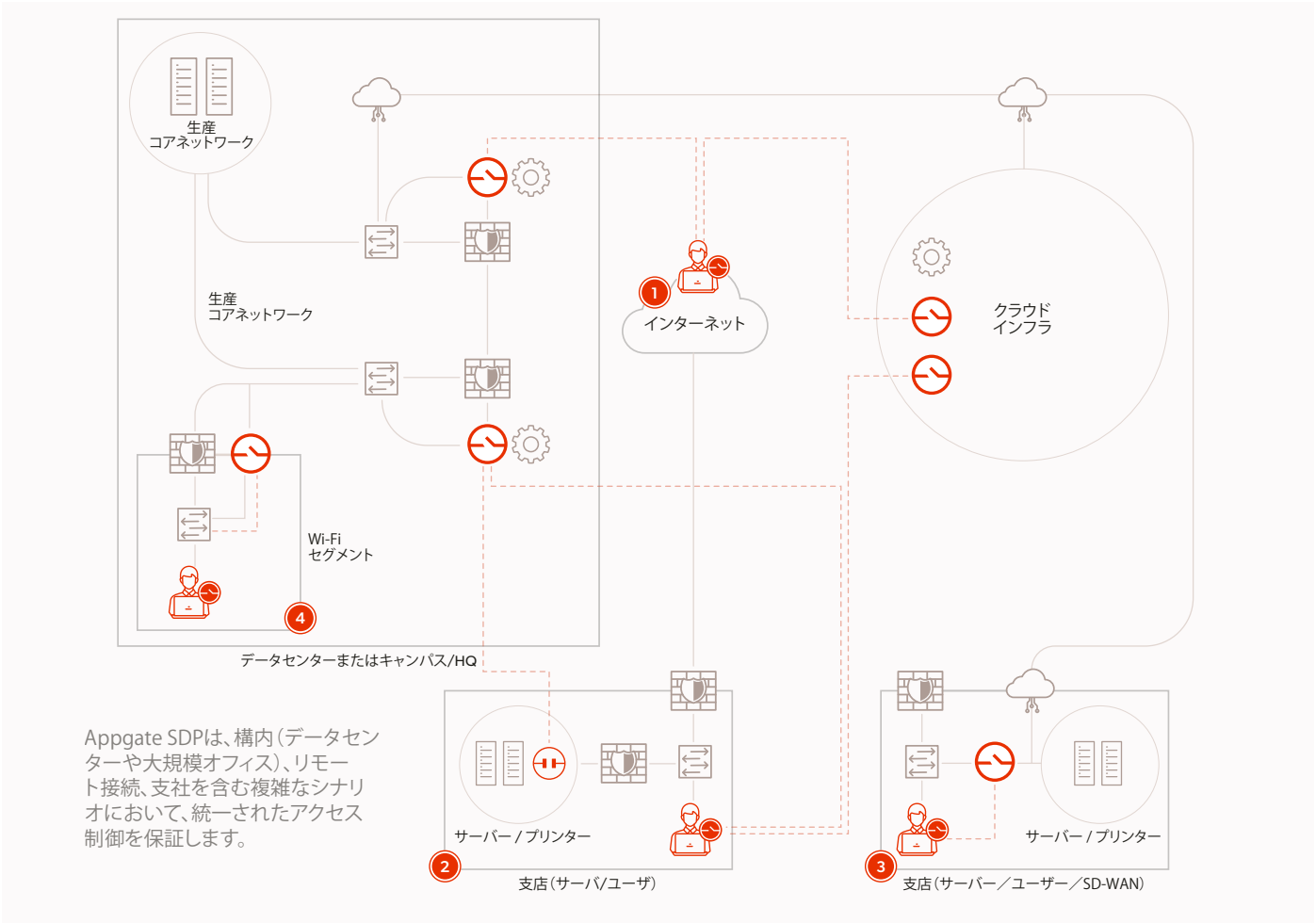
SPAを使用して、クライアントはエンタイトルメントをゲートウェイに送信し、検証されると、保護されたリソースにアクセスするための動的なセッションベースのマイクロファイアウォールネットワークを確立します。Appgate SDP はシステムを継続的に監視し、コンテキストの変更に応じてアクセスを適応または取り消します。

ログフォワーダーは、認証、承認、アクセス、ブロックされたイベントをセキュリティ情報およびイベント管理（SIEM）ツールに配信し、イベントの相関と集中管理を行います。Appgate SDPは、クラウドホスト、セルフホスト、または分離が可能で、さまざまなネットワーク・トポロジーにおける多様なセキュリティとコンプライアンスのニーズに対応します。



Appgate SDP には3 つの主要コンポーネントがある。トラストブローカーおよびポリシー決定ポイントとして機能するコントローラ、ポリシー実施ポイントとして機能するゲートウェイ、そしてユーザーを認可されたリソースに接続するクライアントである。

ユニバーサルZTNAのためのAppgate SDPエンタープライズアーキテクチャのサンプル



上の画像には4つのシナリオがあります：(1)Wi-Fiセグメントに接続された学内ユーザー、(2)リモートで接続されたインターネットユーザー、(3)ユーザーとデバイス（サーバー、IoTデバイス、プリンターなど）があるWAN接続されていないブランチオフィス、(4)同様のデバイスの組み合わせがあるWAN/SD-WAN接続されたブランチオフィス。Appgate SDPを使用すれば、動的なアクセス制御を各シナリオで一貫して適用できます。ユーザーは、異なるオフィスの場所や環境の間を自由に移動することができ、運用の変更を必要としない一貫したユーザー・エクスペリエンスを維持することができます。

Appgate SDPは、既存のセキュリティ制御やコンポーネントとシームレスに統合します。例えば、上記のシナリオ（4）では、ブランチオフィスからのトラフィックは、パフォーマンスに悪影響を与えることなく、既存のSD-WANのサービス品質（トラフィックのフィルタリング、パフォーマンスの強化など）やセキュリティポリシーによって強制されます。シナリオ(3)では、このブランチからSD-WANが排除され、ブランチからデータセンターへの接続がAppgate SDPに置き換えられています。このシナリオのユーザーは、Appgate SDPの直接ルーティングされたZTNAアーキテクチャにより、潜在的なヘアピンをバイパスして、どちらの側でも帯域幅に影響を与えることなく、データセンターのリソースとクラウドのリソースに直接アクセスできます。Appgate SDP Universal ZTNA

1. **すべてのユーザーとデバイスのアクセスを統一：**複数のソリューションを管理する手間を省き、すべてのユーザーとデバイスに対して一貫性のある統一されたアクセス制御を実現します。
2. **適応性と拡張性に優れたセキュリティ：**多様なユーザーやデバイスに対応するため、アクセスポリシーを動的に適応させ、幅広いユースケースやセキュリティ要件への適合性を確保します。
3. **生産性の向上：**トラブルチケットを削減し、許可されたユーザーのリソースへのアクセスを迅速化することで、より俊敏で生産性の高い環境を実現します。
4. **コンプライアンスの簡素化：**一貫したアクセス制御を適用することで、報告範囲を縮小し、業界規制へのコンプライアンスを確保します。
5. **コスト効率と投資収益率（ROI）：**
   複数のアクセス・コントロール・ツールを統合することで、運用効率を高め、大幅なROIを実現します。

Appgate について

Appgate は、セキュア アクセスを提供する企業です。当社は、ゼロ トラスト セキュリティの原則に基づいて構築されたソリューションを提供することで、人々の働き方とつながり方を強化します。この人によって定義されるセキュリティ アプローチにより、クラウド、オンプレミス、ハイブリッド環境のあらゆる IT インフラストラクチャのワークロードに、あらゆるデバイスと場所から高速でシンプルかつ安全な接続が可能になります。詳細についてはappgate.com をご覧ください。

appgate