アイデンティティ中心のマイクロペリメータでアクセスを制御

Appgate SDPを導入すべき1つの理由

物理的および静的な境界防御はもはや時代遅れですが、このブログでは、なぜそうなのかについては深く言及しません。その代わりに、ゼロトラスト・ネットワークアクセス（ZTNA）とも呼ばれる、ソフトウェア定義の境界が主導するネットワークセキュリティの未来のあり方について掘り下げていきます。

今日、境界はワークロードが存在するすべての場所（マルチクラウドまたはオンプレミス、マイクロサービスまたはレガシーアプリ）、および人やデバイスがネットワークに接続しているすべての場所（リモートまたはオフィス内、フルタイムまたはサードパーティ）にあります。

Appgate SDPは、ゼロトラストの原則を実施するように設計されており、NISTゼロトラスト・アーキテクチャの特別刊行物800-207に準拠しています。これは、アイデンティティ中心のマイクロ境界を提供することにより、セキュリティ専門家がアクセスを制御できるように設計されています。しかし...それはつまりどういうことなのでしょうか？

アイデンティティ中心のセキュリティ

ゼロトラスト・セキュリティの重要な側面は、「信頼してから認証」という古いルールを廃止し、「認証してから信頼」に置き換えていることです。トゥルーゼロトラスト・ネットワークアクセスソリューションは、これをさらに一歩進めており、ネットワーク中心のIPアドレスではなく、IDの広範な認証を必要とします。VPN、ファイアウォール、NACなどのレガシーネットワーク中心のセキュリティツールは、「認証してから信頼」するように設計されておらず、アクセス許可を付与するための中心的な基準としてIDを考慮していません。

Appgate SDPは、次の3つの主要な評価基準を使用してIDを検証することにより、条件付きの信頼できるアクセスをプロビジョニングします：

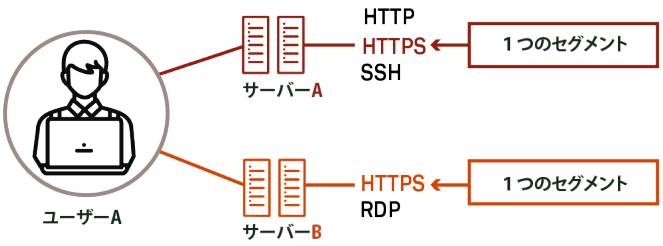
1. 役割変数：すべてのID管理システム（IdP、IAM、IGA）および/またはディレクトリサービス（LDAP）と統合することにより、Appgate SDPは企業のID管理戦略とシームレスに連携します。
2. 環境変数：日付、時刻、地理的位置などは、アクセス資格を付与するための評価で追加の属性およびリアルタイムのコンテキストデータとして使用されます。これらの追加の属性を使用して、MFAなどの追加の認証を要求したり、コンテキストリスクに基づいてアクセスを制限したりできます。
3. デバイス変数：Appgate SDPは、25以上の変数を用いた既製の広範なポスチャチェックを実行することにより、デバイスのリスクを評価します。これは、エンタープライズ・エンドポイント保護ツールと統合すると、さらに強力に機能します。現在では、アクセスはデバイスが信頼できるかどうかに基づいて、条件付きになっています。

これらの属性はすべて、多次元IDプロファイルにコンパイルされます。この360度IDプロファイルは、最初のアクセス要求時だけでなく、属性の変更を継続的に再評価される条件付き資格を評価および付与するために使用されます。

セグメント化されたアクセスのマイクロペリメータ

ゼロトラスト・ネットワークアクセスのもう1つの重要な側面は、信頼されたユーザーがアクセスできる対象を制限する機能です。これは、NACが私たちのためにできることと似ていますが、オンプレミスのみであり、アクセスの基準としてIDが含まれていません。トゥルーゼロトラスト・ネットワークアクセスの場合、アクセス制御はオンプレミスを超えて拡張し、ハイブリッド複合環境内のすべての場所を含む必要があります。アクセスはアイデンティティ中心であり、継続的に評価され、条件とリスクに基づいて動的に調整される必要があります。

Appgate SDPは、ユーザーと割り当てられたリソースの間に「1つのセグメント」を提供します。この「1つのセグメント」は、各ユーザー、ユーザーID、およびユーザーに割り当てられた前述の条件付き資格に固有のマイクロ境界です。IDが継続的に評価される信頼されたユーザーには、職務を遂行するために必要なリソースへのアクセスのみがプロビジョニングされます。そうしたマイクロ境界は、ユーザーごとにセッションベースのマイクロファイアウォールを使用して確立されます。これらはジャストインタイムで作成（あるいは変更、削除）され、特別に付与されたリソースへのアクセスのみを許可します。つまり、許可されていない横方向の移動は発生しません。



ユーザーAにはサーバーAおよびBのHTTPSへのアクセスが許可されましたが、サーバーAのHTTPまたはSSH、またはサーバーBのRDPへのアクセスは許可されませんでした。「1つのセグメント」は、特定のアクセス許可ごとに作成されます。ユーザーAは、サーバーAの他のリソースにアクセスできず、それらを表示することもできません。これにより、内部脅威のリスクを軽減できるだけでなく、ネットワーク全体へのマルウェアの拡散を阻止し、攻撃者が侵入ポイントを突破できた場合に重要なアプリケーションに到達するのを阻止することもできます。

新しいセッションの開始時、さらに重要なのは確立されたセッション中、上記で概説したID基準は継続的に監視され、動的アクセスポリシー、または状況に応じたリスクに基づいて資格を自動的に適応させる、更新された「1つのセグメント」が生成されます。つまり、場所、デバイスポスチャ、雇用状況など、ユーザーの状況に応じたリスクや条件が変化すると、ポリシーが動的に更新され、アクセス許可がさらに制限されたり、ネットワークアクセスが完全に取り消されたりすることがあります。

アイデンティティ中心のマイクロ境界でアクセスを制御することは、お客様がAppgate SDPを展開することを決定する理由の1つにすぎません。詳細については、以下をご覧ください：

1:1カスタムデモのスケジューリング

©2021 Appgate. All Rights Reserved. The Appgate logo and certain product names are the property of Appgate.
All other marks are the property of their respective owners.