Trey Research Corporation

仮想プライベート ネットワーク: Fabrikam, Inc. の技術概要

2023 年 12 月 15 日

仮想プライベート ネットワーク (VPN) は、ネットワーク トラフィックの暗号化に役立つ一般的なネットワーク セキュリティ ソリューションです。VPN は安全なトンネルとして機能し、インターネット トラフィックを暗号化することで、第三者がアクティビティを追跡したりデータを盗んだりすることを困難にします [1]。

VPN を導入する利点:

- VPN は、インターネット トラフィックを暗号化することにより、プライバシーとセキュリティの層を提供します。これにより、第三者がアクティビティを追跡したり、データを盗んだりすることが困難になります。
- VPN は、空港や図書館で公衆 Wi-Fi を使用しているときにハッキングされるのを防ぐのに役立ちます。これは、VPN が安全なトンネルとして機能し、インターネット トラフィックを暗号化するためです。
- VPN を使用すると、コンピューターに送受信されるトラフィックはすべて VPN のサーバー、または VPN が使用料を払って使用するサーバーを経由するため、インターネット サービス プロバイダーはユーザーがどのサイトにアクセスしたかを知ることができなくなります [1]。
- VPN は、IP アドレスをマスクし、インターネット接続を暗号化することで、コンテンツ [2] に対する地理的制限を回避できます。VPN サーバーに接続すると、インターネット トラフィック

は VPN サーバー経由でルーティングされ、新しい IP アドレスが割り当てられます。これにより、あたかも別の場所からインターネットにアクセスしているように見えるため、コンテンツに対する地理的制限を回避できます

VPN を導入する欠点:

- 接続速度は ISP よりも遅くなる場合があります。これは、VPN がインターネット トラフィックに暗号化とルーティングの追加層を追加するためです [2]。
- 一部の独裁国家では VPN の使用が禁止されています。一部の国では、VPN が禁止されているか、厳しく規制されています [2]。
- 無料の VPN を使用すると、広告、マルウェア、漏洩にさらされる危険があります。無料 VPN は、ユーザー データをサードパーティの広告主に販売したり、Web ページに広告を挿入したりする場合があります [2]。

インストールの詳細:

- VPN は、VPN クライアントを実行しているシステムと VPN サーバーの間に暗号化されたトンネルを確立し、VPN サーバーはトンネルを介して企業ネットワークの残りの部分にトラフィックをプロキシします [4]。手順は次のとおりです

    1. VPN クライアントはユーザーのデバイスにインストールされ、デバイスと VPN サーバー間のすべてのトラフィックを暗号化します。
    2. VPN サーバーはトラフィックを復号化し、目的の宛先に転送します。
    3. 宛先サーバーは、VPN サーバーにトラフィックを送り返すことでリクエストに応答します。
    4. VPN サーバーはトラフィックを暗号化し、VPN クライアントに送り返します。
    5. VPN クライアントはトラフィックを復号化し、ユーザーのデバイスに送信します [1]。

- VPN サーバーをインストールして構成するには、次の手順に従います。
    1. コンピューター上に VPN プロファイルを作成します。

2. [スタート] をクリックし、[設定] をクリックして設定メニューを開きます。
3. 設定メニューで、[ネットワークとインターネット] をクリックし、[VPN] をクリックします。
4. [VPN 接続を追加する] を選択します。
5. [VPN 接続の追加] ウィンドウでは、実行するタスクがいくつかあります。
6. 加えた変更を保存します [5]。

リスクと軽減策:

- 攻撃者は以前からリモート ワークが脅威ベクトルであることを認識していました。リモート ワーク環境は、いくつかの理由から攻撃者にとって特に魅力的です。まず、ホーム ネットワーク環境は専門的に管理されていません。最も重要なのは、これは、ホーム ネットワーク上のさらに多くのシステムに定期的にパッチが適用されておらず、その多くが脆弱性の軽減に関して時代遅れであることを意味します。システムを悪用した攻撃者が企業ネットワーク上で存続するには、検出を回避し、修復に抵抗する必要があります。ここでも、ホーム ネットワークは攻撃者にとってより友好的です。通常、脅威の検出はほとんど行われず、PC の動作が遅いために再インストールまたは廃止された場合などに、修復が偶発的に行われます。リモート ワーク環境を保護するには、ゼロトラストの前提をさらに拡張することが不可欠です。敵対的であると想定されるのはネットワークだけではなく、企業の管理下にないすべてのものです [4]。
- VPN、ネットワーク インフラストラクチャ デバイス、作業環境へのリモート接続に使用されているデバイスを、最新のソフトウェア パッチとセキュリティ構成で更新します [6]。

実装のベスト プラクティス:

企業ネットワークに VPN を実装するためのベスト プラクティスは次のとおりです。

- インターネット キー交換/インターネット プロトコル セキュリティ (IKE/IPSec) などの受け入れられた標準を使用する標準ベースの VPN を選択します。これは一般に、カスタム

コードを使用して TLS 1.2 経由でトラフィックを送信する Secure Sockets Layer/Transport Layer Security (SSL/TLS) VPN よりもリスクが低く、安全です [1][2]。

- 強力な暗号化を備えた VPN を使用します。VPN で使用される暗号化アルゴリズム、認証アルゴリズム、プロトコルが強力であり、FIP で検証されていることを検証します。多要素認証 (MFA) を使用するようにすべての VPN を構成し、可能であればパスワード ベースの認証をデジタル証明書 (スマートカードに保存されている) によるクライアント認証に置き換えます [1][2]。
- ソフトウェアの脆弱性を管理します。VPN の脆弱性の悪用は、サイバー犯罪者にとって一般的な攻撃ベクトルです。脆弱性パッチ適用の実績が豊富な VPN ベンダーを選択し、サードパーティのコードが最新で安全であることを検証するソフトウェア部品表 (SBOM) を要求します。また、潜在的な侵入を検出するために、実行時にコードの検証を実行できる製品を探してください。VPN を展開した後は、ソフトウェア更新プログラムを定期的に確認し、速やかに適用してください [1][2]。
- 使用時のサージに備えてください。IT セキュリティ担当者は、大量使用に備えて VPN の制限をテストする必要があります [2]。
- 無料の VPN は避けてください。無料の VPN を使用すると、広告、マルウェア、漏洩にさらされる危険があります [3]。