Cisco AnyConnect VPN

適応型セキュリティアプライアンス（ASA）または FirePower Threat Defense（FTD）で Cisco AnyConnect VPN を使用している場合、Duo の多要素認証（MFA）ソリューションによって社内アプリケーションへのセキュアなリモートアクセスが可能になります。

課 題：

ユーザーログイン情報の窃取

Cisco AnyConnect VPN を使用すると、オンプレミス アプリケーションにユーザーがリモートからアクセスできます。ただし、AnyConnect VPN を使用しているからといって、内部アプリケーションにセキュアにアクセスできるとは限りません。VPN がトンネリングや暗号化を行うのは、リモートロケーションから企業データセンターへのトラフィックのみです。AnyConnect VPN にログインためのユーザー名とパスワードを発行するだけでは、ログイン情報が盗まれた場合、データが漏洩する危険性があります。

攻撃者は、フィッシングや総当たり攻撃など、さまざまな手法を使用してユーザーのログイン情報を盗むことができます。Verizon 社が発表した『2018 年データ漏洩 / 侵害調査報告書』によると、ハッキング関連のインシデントの 81% は、盗まれたパスワードや脆弱なパスワードを悪用したものです。AnyConnect VPN を用いて企業ネットワークにアクセスできれば、攻撃者は上位の権限を獲得や、他のシステム、アプリケーション、サーバーへの移動を試みます。さらに高度なケースでは、攻撃者が内部システムにマルウェアをインストールし、ネットワークにアクセスできる永続的なバックドアを手にする恐れもあります。

「Duo は、私がこれまで導入に携わった中で最も成功しているエンドユーザー向けソリューションです」

Lance Honer 氏
Day & Zimmerman 社 サイバーセキュリティ担当マネージャ

Cisco AnyConnect VPN

ソリューション：

Duo の多要素認証 (MFA)

Cisco AnyConnect VPN のユーザーにとって、Duo の MFA には次の 3 つの際立ったメリットがあります。

01

使いやすさ

AnyConnect の VPN ログインにおいて最も使いやすい多要素認証ソリューションです。Duo の多要素認証を使用すれば、ユーザーはワンタップ認証の Duo Push で本人確認を行えます。MFA によるセキュリティ制御は、ログイン情報が盗まれた場合に効果を発揮します。なぜなら、ユーザーのログイン情報を盗むだけでなく、ユーザーのデバイスに物理的にアクセスしなければ攻撃を実行することはできないからです。

02

柔軟な認証オプション

Duo はいくつかの認証方式を備えていて、すべてのユーザーが内部アプリケーションに簡単にアクセスできます。Duo によって、AnyConnect VPN で Duo Push、ワンタイムパスコード (OTP)、通話、SMS、ハードウェアトークンが利用可能になります。環境とユーザーの利便性に応じて、IT 管理者がこれらの認証オプションのうちの 1 つまたは複数を有効化できます。

03

ゼロトラストによるセキュリティの向上

Cisco ASA で AnyConnect v4.6 以降を使用している場合、Duo によってデバイスとそのセキュリティ態勢に関する情報を得ることができます。デバイスの健全性を確認してポリシーを適用することで、安全かつ正常なデバイスにのみ内部アプリケーションへのアクセスを許可することが可能になります。たとえば、企業が管理する最新のデバイスのみに VPN アクセスを許可するといったポリシーを適用できます。

「使いやすさは本当に素晴らしいものです。Cisco AnyConnect リモート アクセス ソリューションと組み合わせると、パフォーマンスが非常に良くなります」

William Turner 氏
World Vision US シニア ネットワーク エンジニア