Duo Network Gateway

オンプレミスやパブリッククラウドにあるアプリケーションにゼロトラストアクセスを拡張

2020 年の世界的なパンデミックにより多くの人々の働き方や働く場所が変わった一方で、アプリケーションへの接続方法には変化が見られません。それほど遠くない過去において、組織はアクセス管理に二元的な方法でアプローチしていました。人はオフィス内にいるかオフィス外にいるかのどちらかであり、オフィス外の人が内部のアプリケーションにアクセスするには、たいていは、企業が管理するデバイス上で仮想プライベートネットワーク（VPN）を使用するしかありませんでした。ただし、VPN には課題がないわけではありません。操作性が悪く管理が困難で、ユーザーエクスペリエンスを損なう可能性があります。さらにポリシーの適用に、ユーザーやデバイスといったコンテキストの変化を反映させることもできません。

幸いなことに代替策があります。ユーザーエクスペリエンスを損なわず、VPN より拡張性が高い方法で、内部アプリケーションへのアクセスを保護できます。それが、Duo Network Gateway（DNG）です。このリモートアクセスプロキシのセキュリティソリューションを利用すれば、生産性が向上しストレスを感じさせない操作が実現します。その結果、従業員、リモートワーカー、請負業者が、仕事に必要なアプリケーションに容易にアクセスできるようになります。DNG によって、Web アプリケーション、Secure Shell（SSH）サーバー群、Remote Desktop Protocol（RDP）サーバー、ユーザーグループごとに詳細なアクセス制御が可能になります。信頼できるユーザーとエンドポイントだけが内部サービスにアクセスできるようにさまざまなポリシーを指定することができます。

Duo のメリット

- ネットワークに直接つながっているかのようにストレスを感じることなくアクセスできます。これまでと何も変わらず、再トレーニングは不要です。
- アプリケーションへのアクセスを許可する前にデバイストラストを確立します。
- 多要素認証（MFA）でユーザーの本人確認を行います。
- ハイブリッド環境とマルチクラウド環境へのアクセスを保護します。

Duo Network Gateway が選ばれる理由

セキュリティ

- 場所を問わずアプリケーションレベルのアクセスを実現することにより、重要なアプリケーションがリスクにさらされる可能性を軽減します。
- 特定の内部アプリケーションへのアクセスを制御して、ラテラルムーブメントや権限の悪用のリスクを回避します。
- 企業が管理するデバイスと個人所有（BYO）デバイスをすべて可視化して機密情報を保護します。
- きめ細かいポリシーの適用を可能にします。たとえば、より機密性の高いアプリケーションにアクセスする場合は、FIDO2 セキュリティキー（WebAuthn）または Duo Push を使用した多要素認証（MFA）によってユーザー認証のアシュアランスレベルを高め、企業管理デバイスからのアクセスに限定するといったポリシーが可能です。

使いやすさ

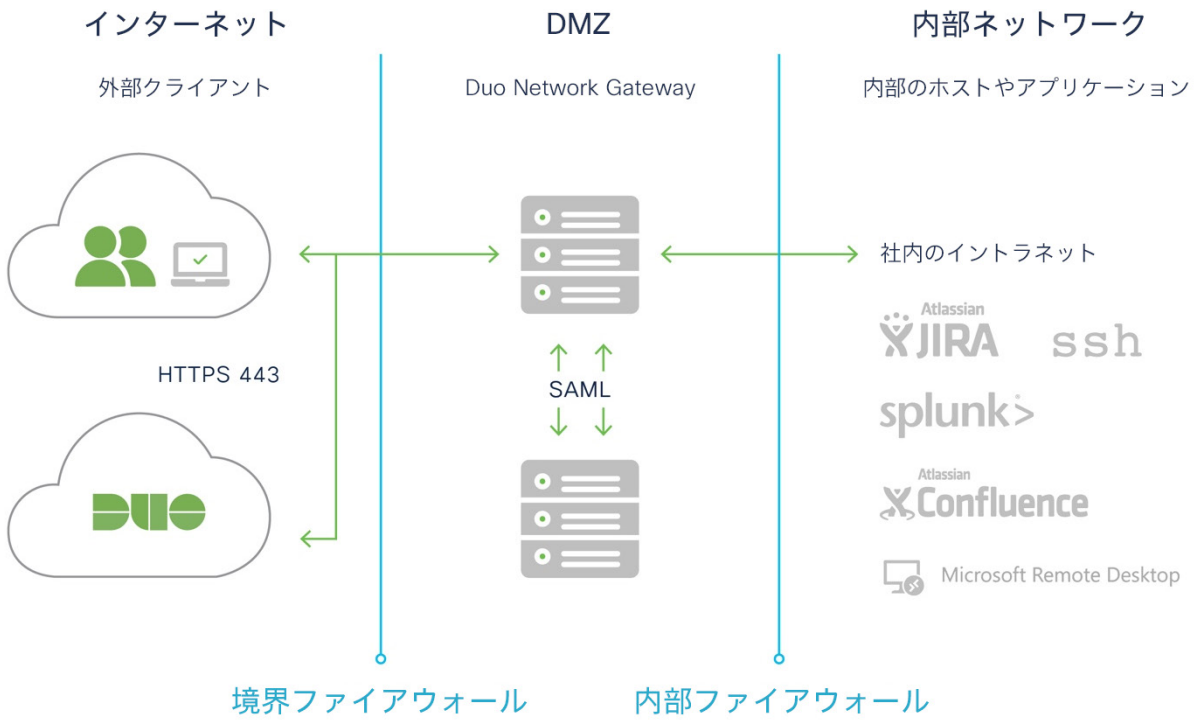
- ソリューションは、簡単に導入できるように設計されています。従来の VPN アクセスソリューションと比較して、セットアップが簡単になり、ハードウェアと帯域幅に関する要件も緩和されています。
- アプリケーション全体で一貫したログインの操作性を実現し、ハイブリッド環境やマルチクラウド環境（オンプレミス、Azure、AWS、Google Cloud Platform）へのセキュアなアクセスを提供します。
- ブラウザベースのアプリケーションに対しては VPN を使用しないセキュアなリモートアクセスが可能になります。
- オンプレミス アプリケーションでもクラウドのようなエンド ユーザー エクスペリエンスが実現します。そのため、ワークフォースがクラウドベースのアプリケーション（Salesforce、Dropbox など）へ容易に移行できるようになります。
- IT 管理者は、アプリケーションごとのポリシーと最小権限モデルを簡単に実装できます。

TCO を削減

- シンプルなユーザー単位のサブスクリプションモデルを提供します。保護できる内部リソースの数に上限はありません。
- 適応型認証、エンドポイントに対する可視性と制御、リモートアクセス、シングルサインオン（SSO）など、多くのセキュリティツールの機能を 1 つのプラットフォームに統合します。

「**Duo Beyond を実装することにしたのは、ゼロトラストセキュリティという当社のビジョンに沿っているものだからです。**Sophos Mobile コントロールと統合すると、従業員にセキュアなモバイルアクセスを安心して提供できるようになり、さらに企業リソースにアクセスしているすべての資産に対する可視性も向上します」

Ross McKerchar 氏
Sophos 社 最高情報セキュリティ責任者



Duo Network Gateway の仕組み

DNG がリバースプロキシとして機能しているため、VPN ログイン情報の管理を気にせずにオンプレミスの Web サイトや Web アプリケーション、ある種の Transmission Control Protocol（TCP）サービス（RDP、SSH）にセキュアにアクセスできるうえ、Duo Prompt でログインセキュリティを強化できます。ユーザーは、好みのブラウザやデバイスを用いて、世界のあらゆる場所から内部 Web アプリケーションにセキュアにアクセスできます。リモート アクセス ソフトウェアをデバイスにインストールしたり設定したりする必要はありません。また、Duo の接続ツールをインストールすると Duo Network Gateway を介して設定済みのホストにリモートで SSH 接続できます。ユーザーはまず DNG に対して認証を行い、続いて二要素認証の要求を承認すると、保護されているさまざまなサービスにアクセスできます。

セッション認識機能があるため、ユーザーがゲートウェイ経由で別のサービスやホストにアクセスしたときに MFA プロンプトが再度表示される可能性は最小限になっています。さらに、信頼できるユーザーとエンドポイントだけが内部サービスにアクセスできるようにさまざまなポリシーを指定することができます。

DNG の前提条件は以下の 2 つです。

- DNG ではプライマリ認証ソースとして使用する SAML 2.0 ID プロバイダー（IdP）が必要です。Duo Single Sign-On (SSO) または Microsoft AD FS、OneLogin、Okta などのサードパーティ プロバイダーを使用できます。
- 最新の物理もしくは仮想の 64 ビット Linux サーバーを境界ネットワーク（DMZ）に導入する必要があります。

価格設定

	Duo Free	Duo MFA	Duo Access	Duo Beyond
多要素認証	✓	✓	✓	✓
シングルサインオン (SSO)	✓	✓	✓	✓
SSO アプリケーション (Duo またはサードパーティ製) へのパスワードレス認証	✓	✓	✓	✓
ポリシーの適用		✓	✓	✓
適応型認証			✓	✓
デバイスの可視性			✓	✓
デバイスの修復			✓	✓
Device Health アプリケーション			✓	✓
信頼できるエンドポイント				✓
Duo Network Gateway				✓
月額	10 人のユーザーまで無料	$3/ ユーザー	$6/ ユーザー	$9/ ユーザー

Duo Network Gateway の実装方法については、duo.com/docs/dng にアクセスしてください。

まとめ

従業員が業務用のアプリケーションやサービスにどこからアクセスしていても生産性が変わらないようにするには、強力なゼロトラストベースのセキュリティに支えられたシームレスなユーザーエクスペリエンスを提供するリモート アクセス ソリューションが必要です。Duo Network Gateway の採用によって、世界中の何百もの企業がすでにこれを実現しています。お客様の企業での実現もお手伝いさせてください。

Duo 製品の機能詳細については、duo.com/product にアクセスしてください。