



リモート アクセス VPN によるユーザの制御

次のトピックでは、リモート アクセス VPN によりユーザ認識とユーザ制御を実行する方法について説明します。

- [リモート アクセス VPN アイデンティティ ソース \(1 ページ\)](#)
- [ユーザ制御用 RA VPN の設定 \(3 ページ\)](#)
- [リモート アクセス VPN アイデンティティ ソースのトラブルシューティング \(4 ページ\)](#)
- [RA VPN の履歴 \(4 ページ\)](#)

リモート アクセス VPN アイデンティティ ソース

Firepower Threat Defense は、リモート アクセス SSL と IPsec-IKEv2 VPN をサポートするセキュアなゲートウェイ機能を提供します。完全なトンネルクライアントである AnyConnect Secure Mobility Client[`AnyConnectSecureMobilityClient`] は、セキュリティゲートウェイへのセキュアな SSL および IPsec-IKEv2 接続をリモート ユーザに提供します。AnyConnect はエンドポイントデバイスでサポートされている唯一のクライアントで、Firepower Threat Defense デバイスへのリモート VPN 接続が可能です。

[新しいリモート アクセス VPN ポリシーの作成](#)の説明に従って安全な VPN ゲートウェイを設定する場合、ユーザが Active Directory リポジトリ内にいる場合は、それらのユーザのアイデンティティポリシーを設定して、アクセスコントロールポリシーにアイデンティティポリシーを関連付けることができます。

リモートユーザから提供されるログイン情報は、LDAP または AD レルムまたは RADIUS サーバグループによって検証されます。これらのエンティティは、Firepower Threat Defense セキュアゲートウェイと統合されます。



- (注) ユーザが認証ソースとして **Active Directory** を使用して **RA VPN** で認証を受ける場合、ユーザは自分のユーザ名を使用してログインする必要があります。domain\username または username@domain 形式は失敗します。(Active Directory はこのユーザ名をログオン名、または場合によっては sAMAccountName と呼んでいます)。詳細については、MSDN で [ユーザの命名属性 \[英語\]](#) を参照してください。

認証に **RADIUS** を使用する場合、ユーザは前述のどの形式でもログインできます。

VPN 接続経路で認証されると、リモート ユーザには *VPN ID* が適用されます。この **VPN ID** は、そのリモート ユーザに属しているネットワーク トラフィックを認識し、フィルタリングするために **Firepower Threat Defense** のセキュア ゲートウェイ上のアイデンティティ ポリシーで使用されます。

アイデンティティ ポリシーはアクセス コントロール ポリシーと関連付けられ、これにより、誰がネットワーク リソースにアクセスできるかが決まります。リモート ユーザがブロックされるか、またはネットワーク リソースにアクセスできるかはこのようにして決まります。

関連トピック

[Firepower Threat Defense の VPN の概要](#)

[Firepower Threat Defense リモート アクセス VPN の概要](#)

[VPN の基本](#)

[リモート アクセス VPN の機能](#)

[リモート アクセス VPN のガイドラインと制限事項](#)

[新しいリモート アクセス VPN ポリシーの作成](#)

ユーザ制御用 RA VPN の設定

スマートライセンス	従来のライセンス	サポートされるデバイス数	サポートされるドメイン数	アクセス (Access)
エクスポート制御機能が有効なスマートライセンスアカウントに関連付けられている次の AnyConnect ライセンスのいずれか。 <ul style="list-style-type: none"> • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex 	該当なし	FTD	グローバルだけ	Admin/Access Admin/Network Admin

始める前に

- [レلمムの作成](#)の説明に従って、レلمムを作成します。
- 認証、認可、および監査 (AAA) を使用するには、[RADIUS サーバグループ](#)の説明に従って RADIUS サーバグループを設定します。

ステップ 1 Firepower Management Center にログインします。

ステップ 2 [デバイス (Devices)] > [VPN] > [リモートアクセス (Remote Access)] の順にクリックします。

ステップ 3 [新しいリモートアクセス VPN ポリシーの作成](#)を参照してください。

次のタスク

- [アイデンティティポリシーの作成](#)の説明に従い、アイデンティティポリシーを使用して、制御するユーザおよびその他のオプションを指定します。
- [アクセス制御への他のポリシーの関連付け](#)の説明に従って、アイデンティティルールをアクセスコントロールポリシーに関連付けます。このポリシーは、トラフィックをフィルタし、オプションで検査します。

- [設定変更の展開](#)の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- [VPNセッションとユーザ情報](#)の説明に従って、VPNユーザトラフィックをモニタします。

リモート アクセス VPN アイデンティティ ソースのトラブルシューティング

- 関連する他のトラブルシューティングについては、[レルムとユーザのダウンロードのトラブルシューティング](#)、[ユーザ制御のトラブルシューティング](#)、および [Firepower Threat Defense の VPN のトラブルシューティング](#) を参照してください。
- リモート アクセス VPN の問題が発生した場合は、Firepower Management Center と管理対象デバイスとの間の接続を確認します。接続に障害が発生している場合、ユーザが既に認識されて Firepower Management Center にダウンロードされている場合を除き、デバイスによって報告されたすべてのリモート アクセス VPN ログインはダウンタイム中に識別されません。
識別されていないユーザは、Firepower Management Center で [不明 (Unknown)] のユーザとして記録されます。ダウンタイム後、[不明 (Unknown)] ユーザはアイデンティティ ポリシーのルールに従って再び識別され、処理されます。
- アクティブ FTP セッションは、イベントの **Unknown** ユーザとして表示されます。これは正常な処理です。アクティブ FTP では、(クライアントではない) サーバが接続を開始し、FTP サーバには関連付けられているユーザ名がないはずだからです。アクティブ FTP の詳細については、[RFC 959](#) を参照してください。

RA VPN の履歴

機能	バージョン	詳細
リモート アクセス VPN	6.2.1	導入された機能。RA VPN により、インターネットに接続されたラップトップまたはデスクトップ コンピュータや、Android または Apple iOS モバイル デバイスを使用して、個々のユーザがリモート ロケーションからプライベート ビジネス ネットワークに接続することができます。リモートユーザは、共有メディアやインターネットを介してデータを転送するために不可欠な暗号化技術を使用して、セキュアに機密性を保持してデータを転送します。