



# 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 \(2 ページ\)](#)
- [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 \(3 ページ\)](#)
- [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 IKEv2 IPsec 接続をリモートユーザに提供します。これ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。

[Firepower Threat Defense のリモート アクセス VPN の管理](#)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/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 という形式でのログインは失敗します。(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 として参照します)。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 接続を介して一度認証されると、リモートユーザは VPN の ID を引き受けます。この VPN ID は、Firepower Threat Defense セキュア ゲートウェイ上のアイデンティティ ポリシーによって、そのリモートユーザに属するネットワーク トラフィックを認識してフィルタリングするために使用されます。

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。リモートユーザがネットワーク リソースからブロックされるか、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

[VPN の概要](#)

[Firepower Threat Defense リモートアクセス VPN について](#)

[VPN の基本](#)

[Firepower Threat Defense リモートアクセス VPN の機能](#)

[Firepower Threat Defense リモートアクセス VPN に関するガイドラインと制限事項](#)

[Firepower Threat Defense のリモートアクセス VPN の管理](#)

## 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	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	グローバルだけ	Admin/Access Admin/Network Admin

#### 始める前に

- [レルムの作成](#)の説明に従って、レルムを作成します。
- 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。

## 手順

- 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 [Firepower Threat Defense のリモート アクセス VPN の管理](#)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](#)の説明に従って、制御するユーザおよび他のオプションを、アイデンティティ ポリシーを使って指定します。
- [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、トラフィックのフィルタリングと、必要に応じて検査を実行します。
- [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。
- [Firepower Threat Defense VPN モニタリング](#)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لم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 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。

## RA VPN の履歴

機能	バージョン (Version)	詳細 (Details)
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。