のリモート アクセス VPN Firepower Threat Defense

Firepower Threat Defense リモート アクセス VPN の概要

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。このクライアントにより、ネットワーク管理者がリモート コンピュータにクライアントをインストールして設定しなくても、リモート ユーザは SSL または IPsec-IKEv2 VPN クライアントを活用できます。Windows、Mac、および Linux 用の AnyConnect モバイル クライアントは、接続時にセキュア ゲートウェイから展開されます。Apple iOS デバイスおよび Android デバイス用の AnyConnect アプリは、当該プラットフォームのアプリ ストアからインストールされます。

Firepower Management Center の [リモートアクセスVPNポリシー（Remote Access VPN Policy）] ウィザードを使用して、SSL と IPsec-IKEv2 リモート アクセス VPN を基本機能とともに迅速かつ容易にセットアップします。次に、必要に応じてポリシー設定を強化し、Firepower Threat Defense セキュア ゲートウェイ デバイスに展開します。

リモート アクセス VPN ポリシーを使用して、次の設定を構成できます。

- Two-Factor Authentication （49 ページ）
- Secondary Authentication （55 ページ）
- 承認を得るための LDAP または Active Directory の設定 （63 ページ）
- VPN セッションでのパスワード変更の管理 （62 ページ）
- RADIUS サーバへのアカウンティング レコードの送信 （64 ページ）
- 許可サーバによるグループ ポリシーまたはその他の属性の選択のオーバーライド （66 ページ）
  - ユーザ グループへの VPN アクセスの拒否 （67 ページ）
  - ユーザ グループに対する接続プロファイルの選択の制限 （67 ページ）

次の例を使用して、VPN ユーザに限定帯域幅を割り当てたり、ユーザ ID ベースのアクセス コントロール ルールに VPN ID を使用したりできます。

- ユーザあたりの AnyConnect 帯域幅を制限する方法 （70 ページ）
- ユーザ ID ベースのアクセス コントロール ルールに VPN アイデンティティを使用する方法 （73 ページ）

リモート アクセス VPN の機能

次の項では、Firepower Threat Defense のリモート アクセス VPN の機能について説明します。

- Cisco AnyConnect セキュア モビリティ クライアントを使用した SSL および IPsec-IKEv2 リモート アクセス。
- Firepower Management Center IPv4 トンネル上の IPv6 など、すべての組み合わせがサポートされています。
- FMC と FDM の両方での設定サポート。デバイス固有のオーバーライド。
- Firepower Management Center および FTD 両方の HA 環境をサポート。
- 複数のインターフェイスと複数の AAA サーバのサポート。
- Rapid Threat Containment では、RADIUS CoA または RADIUS ダイナミック認証の使用がサポートされています。

AAA

- 自己署名または CA 署名のアイデンティティ証明書を使用したサーバ認証。
- RADIUS サーバ、LDAP、または AD を使用する AAA ユーザ名とパスワードベースのリモート認証。

- RADIUS グループとユーザ承認属性、および RADIUS アカウンティング。
- 二重認証では、セカンダリ認証での他の AAA サーバの使用がサポートされています。
- VPN ID を使用した NGFW アクセス制御の統合。

VPN トンネリング

- アドレス割り当て
- スプリット トンネリング
- スプリット DNS
- クライアント ファイアウォール ACL
- 最大接続およびアイドル時間のセッション タイムアウト

モニタリング（Monitoring）

- 期間、クライアント アプリケーションなどのさまざまな特性によって VPN ユーザを表示する新しい VPN ダッシュボード ウィジェット。
- ユーザ名やOSプラットフォームなどの認証情報を含むリモートアクセスVPNイベント。
- FTD 統合 CLI により利用可能なトンネル統計。

AnyConnect のコンポーネント

AnyConnect Secure Mobility Client[AnyConnectSecureMobilityClient]導入

リモート アクセス VPN ポリシーに、接続エンドポイントに配布するための AnyConnect クライアントイメージおよび AnyConnect クライアント プロファイルを含めることができます。または、クライアント ソフトウェアを他の方法で配布できます。『Cisco AnyConnect Secure Mobility Client Administrator Guide』の該当するバージョンで、「*Deploy AnyConnect*」の章を参照してください。

事前にクライアントがインストールされていない場合、リモート ユーザは、SSL または IPsec-IKEv2 VPN 接続を受け入れるように設定されているインターフェイスの IP アドレスをブラウザに入力します。セキュリティ アプライアンスが http:// 要求を https:// にリダイレクトするように設定されている場合を除いて、リモート ユーザは https://*address* の形式で URL を入力する必要があります。URL を入力すると、ブラウザがそのインターフェイスに接続して、ログイン画面が表示されます。

ユーザ ログイン後、セキュア ゲートウェイは VPN クライアントを必要としているとユーザを識別すると、リモート コンピュータのオペレーティング システムに一致するクライアントをダウンロードします。ダウンロード後、クライアントは自動的にインストールと設定を行い、セキュアな接続を確立します。接続の終了時には、（セキュリティ アプライアンスの設定に応じて）そのまま残るか、または自動的にアンインストールを実行します。以前にインストール

されたクライアントの場合、ログイン後、Firepower Threat Defense セキュリティ ゲートウェイはクライアントのバージョンを検査し、必要に応じてアップグレードします。

AnyConnect Secure Mobility Client[AnyConnectSecureMobilityClient] 操作

クライアントがセキュリティアプライアンスとの接続をネゴシエートする場合、クライアントは、Transport Layer Security（TLS）、および任意で Datagram Transport Layer Security（DTLS）を使用して接続します。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

IPsec-IKEv2 VPN クライアントがセキュア ゲートウェイへの接続を開始すると、インターネットキーエクスチェンジ（IKE）によるデバイスの認証と、続く IKE 拡張認証（Xauth）によるユーザ認証からなるネゴシエーションが行われます。グループ プロファイルが VPN クライアントにプッシュされ、IPsec セキュリティ アソシエーション（SA）が作成されて VPN が完了します。

AnyConnect クライアント プロファイル およびエディタ

AnyConnect クライアント プロファイルは、設定パラメータのグループで、動作や表示の設定に VPN クライアントが使用する XML ファイル内に保存されます。これらのパラメータ（XML タグ）には、ホストコンピュータの名前とアドレス、および追加のクライアント機能を有効にする設定が含まれています。

AnyConnectプロファイルエディタを使用してプロファイルを設定できます。このエディタは、AnyConnect ソフトウェア パッケージの一部として利用できる便利な GUI ベースの設定ツールです。これは、Firepower Management Center の外部から実行する独立したプログラムです。

リモート アクセス VPN 認証

リモート アクセス VPN サーバ認証

Firepower Threat Defense セキュア ゲートウェイは、VPN クライアントのエンドポイントに対して自身を特定し、認証するために必ず証明書を使用します。

ウィザードを使用してリモート アクセス VPN 構成を設定するときに、選択した証明書を対象の Firepower Threat Defense デバイスに登録できます。ウィザードの [アクセスおよび証明書（Access & Certificate）] フェーズで、[選択した証明書オブジェクトをターゲットデバイスに登録する（Enroll the selected certificate object on the target devices）] オプションを選択します。証明書の登録は、指定したデバイス上で自動的に開始されます。リモート アクセス VPN の構成が完了すると、デバイス証明書のホームページで登録した証明書のステータスを確認できます。ステータスは、証明書の登録が成功したかどうかを明確に示します。これで、リモートアクセス VPN の設定が完了し、導入の準備ができました。

PKI の登録とも呼ばれる、セキュア ゲートウェイの証明書の取得については、Firepower Threat Defense Certificate ベースの認証で説明しています。この章には、ゲートウェイ証明書の設定、登録、および管理の詳細な説明が含まれています。

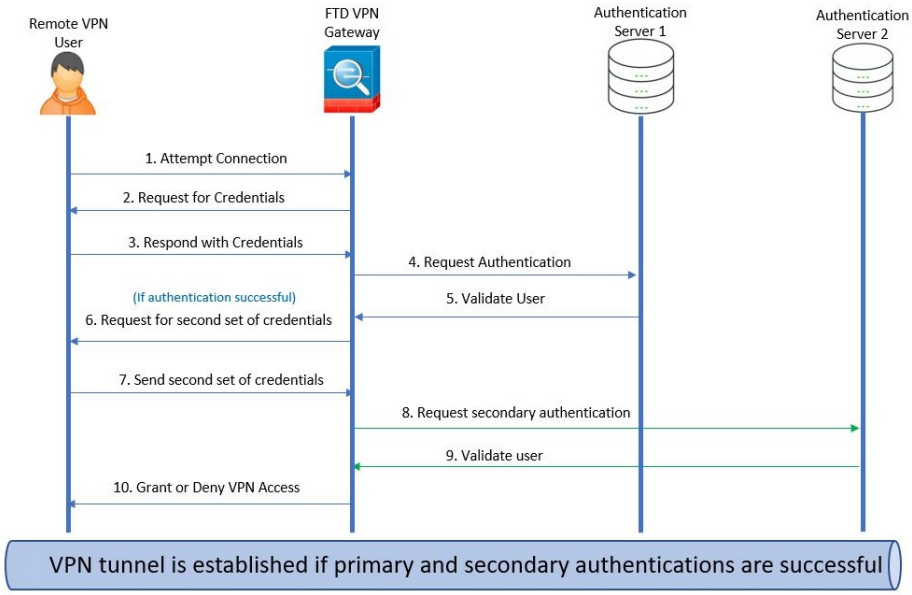
リモート アクセス VPN のクライアント AAA

SSL と IPsec-IKEv2 の両方について、リモート ユーザ認証はユーザ名とパスワードのみ、証明書のみ、あるいはこの両方を使用して実行されます。

（注） 展開でクライアント証明書を使用している場合は、Firepower Threat Defense または Firepower Management Center に関係なく、クライアントのプラットフォームにこれらの証明書を追加する必要があります。クライアントに証明書を入力するために、SCEP や CA サービスなどの機能は提供されません。

AAA サーバでは、セキュア ゲートウェイとして機能する管理対象デバイスが、ユーザの身元（認証）、ユーザが許可されていること（認可）、およびユーザが行ったこと（アカウンティング）を確認できます。AAA サーバの例としては、RADIUS、LDAP/AD、TACACS+、Kerberos などがあります。Firepower Threat Defense デバイス上のリモート アクセス VPN では、AD、LDAP、および RADIUS AAA サーバが認証のためにサポートされています。認証サーバとアカウンティング サーバには、RADIUS サーバのみを構成して使用できます。リモート アクセス VPN の認可の詳細については、「権限および属性のポリシー実施の概要」の項を参照してください。

図 *1 :* リモート アクセス *VPN AAA* 認証



（注） リモート アクセス VPN ポリシーを追加または編集する前に、指定するレルムおよび RADIUS サーバ グループを設定する必要があります。詳細については、レルムの作成およびRADIUS サーバ グループを参照してください。

DNS が設定されていないと、デバイスは AAA サーバ名、名前付き URL、および FQDN またはホスト名を持つ CA サーバを解決できません。解決できるのは IP アドレスのみです。

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 接続経由で認証されると、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。

詳細については、アイデンティティ ポリシーについておよびアクセス コントロール ポリシーの開始のセクションを参照してください。

権限および属性のポリシー実施の概要

Firepower Threat Defense デバイスは、外部認証サーバおよび/または承認 AAA サーバ（RADIUS）から、あるいは Firepower Threat Defense デバイス上のグループ ポリシーから、ユーザ承認属性（ユーザの権利または権限とも呼ばれる）を VPN 接続に適用することをサポートしています。Firepower Threat Defense デバイスがグループ ポリシーに設定されている属性と競合する外部 AAA サーバから属性を受信した場合は、AAA サーバからの属性が常に優先されます。

Firepower Threat Defense デバイスは次の順序で属性を適用します。

1. **外部 AAA サーバ上のユーザ属性**：ユーザ認証や認可が成功すると、サーバからこの属性が返されます。
2. **Firepower Threat Defense デバイス上で設定されているグループ ポリシー**：RADIUS サーバからユーザの RADIUS CLASS 属性 IETF-Class-25（OU=group-policy）の値が返された場

合は、Firepower Threat Defense デバイスはそのユーザを同じ名前のグループ ポリシーに入れて、そのグループ ポリシーの属性のうち、サーバから返されないものを適用します。

3. **接続プロファイル（トンネル グループと呼ばれる）で割り当てられたグループ ポリシー**：接続プロファイルには、接続の事前設定と、認証前にユーザに適用されるデフォルトのグループ ポリシーが含まれています。

（注） Firepower Threat Defense デバイスは、デフォルトのグループ ポリシー *DfltGrpPolicy* から継承したシステム デフォルト属性をサポートしていません。前述のとおり、ユーザ属性または AAA サーバのグループ ポリシーによって上書きされない場合、接続プロファイルに割り当てられたグループ ポリシーの属性がユーザ セッションに使用されます。

AAA サーバ接続の概要

LDAP、AD、および RADIUS AAA サーバは、ユーザ識別処理のみの場合、VPN 認証のみの場合、またはそれら両方の場合に、Firepower Threat Defense デバイスから到達できる必要があります。AAA サーバは、次のアクティビティのためにリモートアクセス VPN で使用されます。

- **ユーザ識別処理**：サーバは管理インターフェイスを介して到達できる必要があります。

  Firepower Threat Defense デバイスの管理インターフェイスには、VPN で使用される通常のインターフェイスとは別のルーティング プロセスと設定があります。

- **VPN 認証**：サーバは通常のインターフェイス（診断インターフェイスまたはデータ インターフェイス）のいずれかを介して到達できる必要があります。

  通常のインターフェイスでは、2 つのルーティング テーブルが使用されます。診断インターフェイス用および管理専用に設定されたその他のインターフェイス用の管理専用ルーティング テーブルと、データ インターフェイスに使用されるデータ ルーティング テーブルです。ルート ルックアップが完了すると、管理専用ルーティング テーブルが最初にチェックされ、次にデータ ルーティング テーブルがチェックされます。最初の照合は、AAA サーバに到達するように選択されます。

  （注） データ インターフェイスに AAA サーバを配置する場合は、管理専用ルーティング ポリシーがデータ インターフェイス宛てのトラフィックと一致しないようにしてください。たとえば、診断インターフェイスを介するデフォルトルートがある場合、トラフィックが決してデータ ルーティング テーブルにフォールバックしないように注意してください。**show route management-only** コマンドと **show route** コマンドを使用してルーティングの決定を確認します。

同じ AAA サーバ上の両方のアクティビティについて、ユーザ識別処理用の管理インターフェイスを介してサーバに到達可能にすることに加え、次のいずれかを実行して、同じ AAA サーバへの VPN 認証アクセスを確保します。

- 管理インターフェイスと同じサブネット上の IP アドレスを使用して診断インターフェイスを有効にして設定し、インターフェイスを介した AAA サーバへのルートを設定します。診断インターフェイスのアクセスは、VPN アクティビティ、識別処理のための管理インターフェイスのアクセスに使用されます。

（注） このように構成すると、診断インターフェイスおよび管理インターフェイスと同じサブネット上にデータ インターフェイスを設定することもできません。管理インターフェイスとデータ インターフェイスが同じネットワーク上に必要な場合（たとえば、デバイス自体をゲートウェイとして使用する場合）でも、診断インターフェイスは無効のままでなければならないため、このソリューションを使用できません。

- AAA サーバへのデータ インターフェイスを介してルートを設定します。データ インターフェイスのアクセスは、VPN アクティビティ、ユーザ識別処理のための管理インターフェイスのアクセスに使用されます。

さまざまなインターフェイスの詳細については、Firepower Threat Defense の通常のファイアウォール インターフェイスを参照してください。

展開後、次の CLI コマンドを使用して、Firepower Threat Defense デバイスからの AAA サーバ接続をモニタおよびトラブルシューティングします。

- **show aaa-server** AAA サーバの統計情報を表示します。
- **show route management-only** 管理専用ルーティング テーブル エントリを表示します。
- **show route** データ トラフィックのルーティング テーブル エントリを表示します。
- **ping** *system* と **traceroute** *system* は管理インターフェイスを介して AAA サーバへのパスを確認します。
- **ping interface** *ifname* と **traceroute** *destination* は診断インターフェイスとデータインターフェイスを介して AAA サーバへのパスを確認します。
- **test aaa-server authentication** と **test aaa-server authorization** は AAA サーバでの認証と許可をテストします。
- **clear aaa-server statistics** *groupname* または **clear aaa-server statistics protocol** *protocol* はグループ別またはプロトコル別に AAA サーバの統計情報をクリアします。
- **aaa-server** *groupname* **active host** *hostname* は障害が発生した AAA サーバをアクティブ化します。または、 **aaa-server** *groupname* **fail host** *hostname* で AAA サーバを不合格にします。

- **debug ldap level**、**debug aaa authentication**、 **debug aaa authorization**、**debug aaa accounting**。

リモート アクセス VPN のガイドラインと制限事項

リモート アクセス VPN ポリシーの設定

- 新しいリモートアクセスVPNポリシーは、ウィザードを使用してのみ追加できます。ウィザードのすべての手順を実行して新しいポリシーを作成する必要があります。ウィザードを完了する前にキャンセルすると、ポリシーは保存されません。
- 2 人のユーザが同時にリモート アクセス VPN ポリシーを編集することは**できません**。ただし、Webインターフェイスでは同時編集が防止されません。これが発生した場合、最後に保存された設定が保持されます。
- リモート アクセス VPN ポリシーがそのデバイスに割り当てられている場合、あるドメインから別のドメインに Firepower Threat Defense デバイスを移動することはできません。
- クラスタ モードの Firepower 9300 および 4100 シリーズは、リモート アクセス VPN の設定をサポートしていません。
- 誤って設定された FTD NAT ルールがあると、リモート アクセス VPN 接続が失敗する可能性があります。
- IKE ポート 500/4500 または SSL ポート 443 が使用されている場合、またはアクティブな PAT 変換がある場合は、これらのポートでサービスを開始できないため、AnyConnect IPSec-IKEv2 または SSL リモート アクセス VPN を同じポートに設定することはできません。これらのポートは、リモート アクセス VPN を設定する前に Firepower Threat Defense デバイスで使用しないようにする必要があります。
- ウィザードを使用してリモート アクセス VPN を設定しているときは、インライン証明書登録オブジェクトを作成できますが、それらを使用してアイデンティティ証明書をインストールすることはできません。証明書登録オブジェクトは、リモート アクセス VPN ゲートウェイとして設定されている Firepower Threat Defense デバイスでアイデンティティ証明書を生成するために使用されます。デバイスにリモート アクセス VPN 設定を展開する前に、デバイスにアイデンティティ証明書をインストールします。証明書登録オブジェクトに基づいてアイデンティティ証明書をインストールする方法の詳細については、オブジェクト マネージャを参照してください。
- リモート アクセス VPN ポリシーの設定を変更した後は、Firepower Threat Defense デバイスに変更を再展開します。設定変更の展開にかかる時間は、ポリシーとルールの複雑さ、デバイスに送信する設定のタイプと量、メモリとデバイス モデルなど、複数の要因によって異なります。リモート アクセス VPN ポリシーの変更を展開する前に、設定変更の展開に関する注意事項を確認してください。

同時 VPN セッションのキャパシティ プランニング

同時 VPN セッションの最大数は、プラットフォーム固有の制限に準拠し、ライセンスには依存しません。デバイス モデルに基づいて、1 台のデバイスで許可される同時リモート アクセス VPN セッション数に上限が設けられます。この制限は、システム パフォーマンスが許容できないレベルに低下しないように設計されています。これらの制限は、キャパシティ プランニングに使用します。

デバイス モデル	最大同時リモート アクセス VPN セッション数
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10000

他のハードウェア モデルの容量については、セールス担当者にお問い合わせください。

（注） プラットフォームごとのセッション数の上限に達すると、FTD デバイスが VPN 接続を拒否します。Syslog メッセージが示され、接続が拒否されます。Syslog メッセージ ガイドで Syslog メッセージ「%ASA-4-113029」と「and %ASA-4-113038」を参照してください。詳細については、http://www.cisco.com/c/en/us/td/docs/security/asa/syslog-guide/syslogs.htmlを参照してください。

VPN の暗号使用方法の制御

DES よりも高度な暗号方式を使用しないようにするため、Firepower Management Center の次の場所で、展開前チェックを使用することもできます。

[デバイス（Devices）] > [プラットフォーム設定（Platform Settings）] > [SSL 設定（SSL Settings）]

[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] > [詳細（Advanced）] > [IPsec]

SSL 設定と IPsec の詳細については、SSL 設定およびリモート アクセス VPN の [IPsec/IKEv2パラメータ（IPsec/IKEv2 Parameters）] の設定 （45 ページ）を参照してください。

認証、認可、アカウンティング

- Firepower Threat Defense デバイスは、システム統合認証サーバのみを使用するリモート アクセス VPN ユーザの認証をサポートしており、ローカル ユーザ データベースはサポートされていません。
- LDAP または AD の認可とアカウンティングは、リモート アクセス VPN ではサポートされていません。リモート アクセス VPN ポリシーでは、RADIUS サーバ グループのみを承認サーバまたはアカウンティング サーバとして構成できます。

- リモート アクセス VPN を使用するには、トポロジ内の各デバイスで DNS を設定します。DNS がないと、デバイスは AAA サーバ名、名前付き URL、および FQDN またはホスト名を持つ CA サーバを解決できません。解決できるのは IP アドレスのみです。

  プラットフォームの設定を使用して DNS を設定できます。詳細については、DNS の設定およびDNS サーバ グループ オブジェクトを参照してください。

クライアント証明書

- 展開でクライアント証明書を使用している場合は、Firepower Threat Defense または Firepower Management Center に関係なく、クライアントのプラットフォームにこれらの証明書を追加する必要があります。クライアントに証明書を入力するために、SCEP や CA サービスなどの機能は提供されません。

AnyConnect のサポート対象外の機能

サポートされている VPN クライアントは、Cisco AnyConnect セキュア モビリティ クライアントのみです。それ以外のクライアントまたはネイティブ VPN はサポートされていません。クライアントレス VPN は、Web ブラウザを使用して AnyConnect クライアントの展開に使用されるだけで、VPN 接続としてはサポートされていません。

FTD セキュア ゲートウェイに接続する場合、次の AnyConnect 機能はサポートされていません。

- セキュア モビリティ、ネットワーク アクセス管理、およびコア VPN 機能と VPN クライアント プロファイルを超えたその他のすべての AnyConnect モジュールとそのプロファイル。
- Hostscan およびエンドポイント ポスチャ アセスメント と、クライアント ポスチャに基づくダイナミック アクセス ポリシーなどのポスチャ派生機能。
- AnyConnect のカスタマイズとローカリゼーションのサポート。FTD デバイスは、これらの機能のために AnyConnect を設定するために必要なファイルを設定または展開しません。
- AnyConnect クライアントのカスタム属性は、FTD ではサポートされません。したがって、デスクトップ クライアントでの遅延アップグレード、モバイル クライアントでのアプリケーションごとの VPN といった、カスタム属性を使用するすべての機能はサポートされません。
- ローカル認証では、VPN ユーザを FTD セキュア ゲートウェイで設定することはできません。

  ローカル CA では、セキュア ゲートウェイは認証局として動作できません。
- SAML 2.0 を使用したシングル サインオン
- TACACS、Kerberos（KCD 認証および RSA SDI）
- LDAP 認証（LDAP 属性マップ）
- ブラウザ プロキシ

- VPN ロード バランシング。

新しいリモート アクセス VPN 接続の設定

ここでは、VPN ゲートウェイとして Firepower Threat Defense デバイスを使用したり、VPN クライアントとして Cisco AnyConnect を使用したりして、新しいリモート アクセスを設定する手順について説明します。

	操作内容	詳細
ステップ 1	ガイドラインと前提条件を確認します。	リモート アクセス VPN のガイドラインと制限事項 （9 ページ） リモート アクセス VPN を設定するための前提条件 （13 ページ）
ステップ 2	ウィザードを使用して新しいリモート アクセス VPN ポリシーを作成します。	新しいリモート アクセス VPN ポリシーの作成 （13 ページ）
ステップ 3	デバイスに展開されているアクセス コントロール ポリシーを更新します。	Firepower Threat Defense デバイスのアクセス コントロール ポリシーの更新 （16 ページ）
ステップ 4	（オプション）NAT がデバイスで設定されている場合は、NAT 免除ルールを設定します。	（オプション）NAT 免除の設定 （17 ページ）
ステップ 5	DNS を設定します。	DNS の設定 （18 ページ）
ステップ 6	AnyConnect クライアント プロファイルを追加します。	AnyConnect クライアント プロファイル XML ファイルの追加 （18 ページ）
ステップ 7	リモート アクセス VPN ポリシーを展開します。	設定変更の展開
ステップ 8	（オプション）リモート アクセス VPN ポリシー設定を確認します。	設定の確認 （20 ページ）

リモート アクセス VPN を設定するための前提条件

- Firepower Threat Defense デバイスを展開し、Firepower Management Center を設定して、輸出規制対象の機能を有効にした必要なライセンスを持つデバイスを管理します。詳細については、VPN ライセンスを参照してください。
- リモート アクセス VPN ゲートウェイとして機能する各 Firepower Threat Defense デバイスにアイデンティティ証明書を取得するために使用する証明書登録オブジェクトを設定します。
- RADIUS サーバ グループ オブジェクトと、リモート アクセス VPN ポリシーで使用されている AD または LDAP レルムを設定します。
- リモート アクセス VPN 設定が機能するように AAA サーバに Firepower Threat Defense デバイスからアクセスできることを確認します。AAA サーバへの接続を確実にするために、ルーティングを設定します（[デバイス（Devices）]>[デバイス管理（Device Management）]>[デバイスの編集（Edit Device）]>[ルーティング（Routing）]）。

  リモート アクセス VPN の二重認証の場合は、二重認証設定が機能するようにプライマリとセカンダリの両方の認証サーバに Firepower Threat Defense デバイスからアクセスできることを確認します。
- Firepower Threat Defense のリモート アクセス VPN を有効にするため、AnyConnect Plus、AnyConnect Apex、または AnyConnect VPN Only のうちいずれかの Cisco AnyConnect ライセンスを購入します。
- シスコのソフトウェア ダウンロード センターから最新の AnyConnect イメージ ファイルをダウンロードします。

  Firepower Management Center の Web インターフェイスで、[オブジェクト（Objects）]>[オブジェクト管理（Object Management）]>[VPN]>[AnyConnect ファイル（AnyConnect File）]に移動し、新しいAnyConnect クライアント イメージ ファイルを追加します。
- ユーザが VPN 接続のためにアクセスするネットワーク インターフェイスを含む、セキュリティ ゾーンまたはインターフェイス グループを作成します。インターフェイス オブジェクト：インターフェイス グループとセキュリティ ゾーンを参照してください
- AnyConnect プロファイル エディタをシスコのソフトウェア ダウンロード センターからダウンロードし、AnyConnect クライアント プロファイルを作成します。スタンドアロン プロファイル エディタを使用して、新しい AnyConnect プロファイルを作成したり、既存の AnyConnect プロファイルを変更したりできます。

新しいリモート アクセス VPN ポリシーの作成

新しいリモートアクセス VPN ポリシーを追加できるのはリモートアクセス VPN ポリシー ウィザードを使用する場合のみです。このウィザードは、基本的な機能を持つリモート アクセス VPN をすばやく、簡単にセットアップできるようにします。さらに、必要に応じて追加の属性

を指定することでポリシー設定を強化して Firepower Threat Defense のセキュア ゲートウェイ デバイスに展開できます。

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。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

始める前に

- リモート アクセス VPN を設定するための前提条件 （13 ページ） に示されているすべての前提条件を満たしていることを確認します。

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 [追加（Add）]（  ） をクリックし、基本的なポリシー設定を行うウィザードを使用して新しいリモート アクセス VPN ポリシーを作成します。

ウィザードのすべての手順を実行して新しいポリシーを作成する必要があります。ウィザードを完了する前にキャンセルすると、ポリシーは保存されません。

ステップ 3 [ターゲット デバイス（Target Devices）] と [プロトコル（Protocols）] を選択します。

選択した Firepower Threat Defense デバイスは、VPN クライアント ユーザのリモート アクセス VPN ゲートウェイとして機能します。リストからデバイスを選択するか、または新しいデバイスを追加します。

SSL または IPSec-IKEv2、あるいはその両方の VPN プロトコルを選択できます。Firepower Threat Defense は、VPN トンネルを経由するパブリック ネットワークを介してセキュアな接続を確立するために両方のプロトコルをサポートしています。SSL 設定については、SSL 設定を参照してください。

ステップ 4 [接続プロファイル（Connection Profile）] および [グループポリシー（Group Policy）] 設定を設定します。

接続プロファイルでは、リモート ユーザが VPN デバイスに接続する方法を定義するパラメータ セットを指定します。パラメータには、認証、VPN クライアントへのアドレスの割り当てとグループ ポリシーの設定および属性が含まれています。Firepower Threat Defense デバイスは、リモート アクセス VPN ポリシーを設定する際の *DefaultWEBVPNGroup* というデフォルトの接続プロファイルを提供します。

詳細については、接続プロファイルの設定 （21 ページ）を参照してください。

グループ ポリシーはグループ ポリシー オブジェクト内に保存される属性と値の一連のペアで、VPN ユーザに対してリモート アクセス VPN のエクスペリエンスを定義します。グループ ポリシーを使用して、ユーザ認証プロファイル、IP アドレス、AnyConnect 設定、VLAN マッピング、およびユーザ セッション設定などの属性を設定します。RADIUS 承認サーバがグループ ポリシーを割り当てるか、または現在の接続プロファイルから取得されます。

詳細については、グループ ポリシーの設定 （39 ページ）を参照してください。

ステップ 5 VPN ユーザがリモート アクセス VPN への接続に使用する [AnyConnect クライアント イメージ（AnyConnect Client Image）] を選択します。

Cisco AnyConnect セキュア モビリティ クライアントは Firepower Threat Defense デバイスへのセキュアな SSL 接続または IPSec（IKEv2）接続を提供し、これにより、リモート ユーザによる企業リソースへのフル VPN プロファイリングが可能となります。Firepower Threat Defense デバイスにリモート アクセス VPN ポリシーを展開したら、VPN ユーザは設定したデバイス インターフェイスの IP アドレスをブラウザに入力し、AnyConnect クライアントをダウンロードしてインストールできるようになります。

ステップ 6 [ネットワーク インターフェイスとアイデンティティ証明書（Network Interface and Identity Certificate）] を選択します。

インターフェイス オブジェクトは、ネットワークをセグメント化してトラフィック フローを管理し、分類しやすくします。セキュリティ ゾーン オブジェクトは単にインターフェイスをグループ化します。これらのグループは複数のデバイスにまたがることがあります。また、単一のデバイスに複数のゾーンインターフェイス オブジェクトを設定することもできます。インターフェイス オブジェクトには次の 2 つのタイプがあります。

- セキュリティ ゾーン：インターフェイスは、1 つのセキュリティ ゾーンにのみ属することができます。
- インターフェイス グループ：インターフェイスは複数のインターフェイスグループ（および 1 つのセキュリティ ゾーン）に属することができます。

ステップ 7 リモート アクセス VPN ポリシー設定の [概要（Summary）] を表示します。

[概要（Summary）] ページには、これまでに設定したすべてのリモート アクセス VPN 設定が表示され、選択したデバイスにリモート アクセス VPN ポリシーを展開する前に実行する必要がある追加設定へのリンクが示されます。

必要に応じて、[戻る（Back）] をクリックして設定に変更を加えます。

ステップ 8 リモート アクセス VPN ポリシーの基本設定を完了するには、[終了（Finish）] をクリックします。

ウィザードを使用してリモート アクセス VPN ポリシーを完了すると、ポリシー リスト ページに戻ります。DNS 設定をセットアップし、VPN ユーザのアクセス制御を設定し、NAT の免除を有効にして（必要

な場合）、基本的な RA VPN のポリシー設定を完了します。次に、設定を展開し、VPN 接続を確立します。

Firepower Threat Defense デバイスのアクセス コントロール ポリシーの更新

リモート アクセス VPN ポリシーを展開する前に、VPN トラフィックを許可するルールを使用してターゲットの Firepower Threat Defense デバイス上でアクセス コントロール ポリシーを更新する必要があります。ルールは、定義済み VPN プール ネットワークの送信元と社内ネットワークの宛先を持つ外部インターフェイスを通過するすべてのトラフィックを許可する必要があります。

（注） [復号されたトラフィックのアクセス コントロール ポリシーをバイパスする（sysopt permit-vpn）（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）] オプションを選択した場合は、リモート アクセス VPN のアクセス コントロール ポリシーを更新する必要はありません。詳細については、リモートアクセス VPN のアクセス インターフェイスの設定 （31 ページ）を参照してください。

始める前に

リモート アクセス VPN ポリシー ウィザードを使用してリモート アクセス VPN ポリシーの設定を実行します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[ポリシー（Policies）] > [アクセス制御（Access Control）] を選択します。

ステップ 2 リモート アクセス VPN ポリシーが展開されるターゲット デバイスに割り当てられているアクセス コントロール ポリシーを選択し、[編集（Edit）] をクリックします。

ステップ 3 新しいルールを追加するには、[ルールの追加（Add Rule）] をクリックします。

ステップ 4 ルールの [名前（Name）] を指定し、[有効（Enabled）] を選択します。

ステップ 5 [アクション（Action）]、[許可（Allow）]、または [信頼（Allow）] を選択します。

ステップ 6 [ゾーン（Zones）] タブで次の項目を選択します。

a) [使用可能なゾーン（Available Zones）] から外部ゾーンを選択し、[送信元に追加（Add to Source）] をクリックします。

b) [使用可能なゾーン（Available Zones）] から内部ゾーンを選択し、[宛先に追加（Add to Destination）] をクリックします。

ステップ 7 [ネットワーク（Networks）] タブで次の項目を選択します。

a) 使用可能なネットワークから内部ネットワーク（内部インターフェイスまたは社内ネットワーク）を選択し、[宛先に追加（Add to Destination）] をクリックします。

b) **使用可能なネットワーク**から VPN アドレス プール ネットワークを選択し、[送信元ネットワークに追加（Add to Source Networks）] をクリックします。

ステップ 8 その他の必要なアクセス制御ルールを設定して [追加（Add）] をクリックします。

ステップ 9 ルールとアクセス コントロール ポリシーを保存します。

（オプション）NAT 免除の設定

NAT 免除を使用すると、アドレスは変換から除外され、変換済みのホストとリモート ホストの両方が保護されたホストとの接続を開始できるようになります。アイデンティティ NAT と同様に、特定のインターフェイスでホストの変換を制限するのではなく、すべてのインターフェイスを経由する接続に NAT 免除を使用する必要があります。ただし、NAT 免除では変換対象の実際のアドレスを決定するときに実際のアドレスおよび宛先アドレスを指定できます（ポリシー NAT と類似）。アクセス リストのポートを考慮するには、スタティック アイデンティティ NAT を使用します。

始める前に

リモート アクセス VPN ポリシーが展開されているターゲット デバイスに NAT が設定されているかどうかを確認します。NAT がターゲット デバイスで有効になっている場合、NAT ポリシーを定義して VPN トラフィックを対象外にする必要があります。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [NAT] をクリックします。

ステップ 2 更新する NAT ポリシーを選択するか、または [新しいポリシー（New Policy）] > [脅威対策NAT（Threat Defense NAT）] をクリックし、すべてのインターフェイスへの接続を許可する NAT ルールを含む NAT ポリシーを作成します。

ステップ 3 [ルールの追加（Add Rule）] をクリックして NAT ルールを追加します。

ステップ 4 [NAT ルールの追加（Add NAT Rule）] ウィンドウで、次を選択します。

a) [NAT ルール（NAT Rule）] に [手動 NAT ルール（Manual NAT Rule）] を選択します。

b) [タイプ（Type）] に [スタティック（Static）] を選択します。

c) [インターフェイスオブジェクト（Interface Objects）] タブで、送信元と宛先のインターフェイス オブジェクトを選択します。

（注） このインターフェイス オブジェクトは、リモートアクセス VPN ポリシーで選択したインターフェイスと同じである必要があります。

詳細については、リモートアクセス VPN のアクセス インターフェイスの設定 （31 ページ）を参照してください。

a) [変換（Translation）] タブで送信元と宛先のネットワークを選択します。

- [元の送信元（Original Source）] および [変換済み送信元（Translated Source）]
- [元の宛先（Original Destination）] および [変換済み宛先（Translated Destination）]

ステップ 5 [詳細（Advanced）] タブで [宛先インターフェイスでプロキシ ARP を使用しない（Do not proxy ARP on Destination interface）] を選択します。

[宛先インターフェイスでプロキシ ARP を使用しない（Do not proxy ARP on Destination Interface）]：マッピング IP アドレスへの着信パケットのプロキシ ARP を無効にします。マッピング インターフェイスと同じネットワーク上のアドレスを使用した場合、システムはプロキシ ARP を使用してマッピング アドレスのすべての ARP 要求に応答することで、マッピング アドレスを宛先とするトラフィックを代行受信します。この方法では、デバイスがその他のネットワークのゲートウェイである必要がないため、ルーティングが簡略化されます。必要に応じてプロキシ ARP をディセーブルにできます。その場合は、アップストリーム ルータの適切なルートがあることを確認する必要があります。

ステップ 6 [OK] をクリックします。

DNS の設定

リモート アクセス VPN を使用するには、Firepower Threat Defense の各デバイスで DNS を設定します。DNS がないと、デバイスは AAA サーバ名、名前付き URL、FQDN またはホスト名を持つ CA サーバを解決できません。IP アドレスのみを解決できます。

ステップ 1 DNS サーバの詳細とドメインルックアップ インターフェイスを [プラットフォーム設定（Platform Settings）] を使用して設定します。詳細については、DNS の設定およびDNS サーバ グループ オブジェクトを参照してください。

ステップ 2 VNP ネットワーク経由で DNS サーバに到達可能な場合は、リモート アクセス VPN トンネルを介して DNS トラフィックを許可するためのスプリット トンネルをグループ ポリシーに設定します。詳細については、「グループ ポリシー オブジェクトの設定」を参照してください。

AnyConnect クライアント プロファイル XML ファイルの追加

AnyConnect クライアント プロファイルは、設定パラメータのグループで、動作や表示の設定にクライアントが使用する XML ファイル内に保存されます。これらのパラメータ（XML タグ）には、ホスト コンピュータの名前とアドレス、および追加のクライアント機能を有効にする設定が含まれています。

AnyConnect プロファイル エディタを使用すると、AnyConnect クライアント プロファイルを作成できます。このエディタは、AnyConnect ソフトウェア パッケージの一部として利用できる GUI ベースの設定ツールです。これは、Firepower Management Center の外部で実行する独立したプログラムです。AnyConnect プロファイル エディタの使用の詳細については、『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』を参照してください。

始める前に

Firepower Threat Defense リモート アクセス VPN ポリシーには VPN クライアントに割り当てる AnyConnect クライアント プロファイルが必要です。クライアント プロファイルはグループ ポリシーに関連付けられます。

AnyConnect プロファイル エディタはシスコのソフトウェア ダウンロード センターからダウンロードします。

ステップ 1 [デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）]。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。
リモート アクセス VPN のポリシーに設定されている接続プロファイルのリストが表示されます。

ステップ 3 AnyConnect クライアント プロファイルを更新する接続プロファイルを選択し、[編集（Edit）] アイコンをクリックします。

ステップ 4 [追加（Add）] アイコンをクリックしてグループ ポリシーを追加するか、または [グループ ポリシーの編集（Edit Group Policy）] > [全般（General）] > [AnyConnect] をクリックします。

ステップ 5 リストからクライアント プロファイルを選択するか、または [追加（Add）] アイコンをクリックして新しいプロファイルを追加します。

a) AnyConnect プロファイルの [名前（Name）] を指定します。

b) [参照（Browse）] をクリックし、AnyConnect プロファイルの XML ファイルを選択します。

（注） 二要素認証の場合、AnyConnect クライアント プロファイル XML ファイルでタイムアウトが 60 秒以上に更新されていることを確認してください。

c) **[保存（Save）]** をクリックします。

（オプション）スプリット トンネリングの設定

スプリット トンネルではセキュア トンネル経由のリモート ネットワークへの VPN 接続が可能ですが、VPN トンネル外のネットワークにも接続できます。VPN ユーザがリモートアクセス VPN に接続されている間、外部ネットワークにアクセスできるようにするには、スプリット トンネルを設定します。スプリットトンネル リストを設定するには、標準アクセス リストまたは拡張アクセス リストを作成する必要があります。

詳細については、グループ ポリシーの設定 （39 ページ）を参照してください。

ステップ 1 [デバイス（Devices）] > [VP] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リストから既存のリモート アクセス ポリシーを選択し、対応する編集アイコンをクリックします。

ステップ 3 接続プロファイルを選択して [編集（Edit）] アイコンをクリックします。

ステップ 4 [追加（Add）] アイコンをクリックしてグループ ポリシーを追加します。または、[グループポリシーの編集（Edit Group Policy）] > [全般（General）] > [スプリットトンネリング（Split Tunneling）] をクリックします。

ステップ 5 [IPv4スプリットトンネリング（IPv4 Split Tunneling）] または [IPv6スプリットトンネリング（IPv6 Split Tunneling）] リストから、[以下に指定したネットワークを除外する（Exclude networks specified below）] を選択し、VPN トラフィックから除外するネットワークを選択します。
スプリットトンネリングオプションをこのままにした場合、エンドポイントからのすべてのトラフィックは VPN 接続経由で送信されます。

ステップ 6 [標準アクセスリスト（Standard Access List）] または [拡張アクセスリスト（Extended Access List）] をクリックし、ドロップダウンからアクセス リストを選択するか、新しいアクセス リストを追加します。

ステップ 7 新しい標準アクセス リストまたは拡張アクセス リストを追加する場合は、次の手順を実行します。

a) 新しいアクセス リストの [名前（Name）] を指定し、[追加（Add）] をクリックします。

b) [アクション（Action）] から [許可（Allow）] を選択します。

c) VPN トンネル上で許可するネットワーク トラフィックを選択し、[追加（Add）] をクリックします。

ステップ 8 **[保存（Save）]** をクリックします。

関連トピック

アクセス リスト

設定の確認

ステップ 1 外部ネットワークのマシンで Web ブラウザを開きます。

ステップ 2 リモート アクセス VPN ゲートウェイとして設定されている FTD デバイスの URL を入力します。

ステップ 3 プロンプトが表示されたらユーザ名とパスワードを入力し、[ログオン（Logon）] をクリックします。

（注） システムに AnyConnect がインストールされている場合は、VPN に自動的に接続されます。

AnyConnect がインストールされていない場合は、AnyConnect クライアントをダウンロードするように求められます。

ステップ 4 まだインストールされていない場合は AnyConnect をダウンロードし、VPN に接続します。
AnyConnect クライアントは自身をインストールします。認証が成功すると、Firepower Threat Defense リモート アクセス VPN ゲートウェイに接続されます。該当するアイデンティティ ポリシーまたは QoS ポリシーは、リモート アクセス VPN ポリシーの設定に従って適用されます。

オプションのリモート アクセス VPN 設定

接続プロファイルの設定

リモート アクセス VPN ポリシーには、特定のデバイスを対象とする接続プロファイルが含まれています。これらのポリシーはトンネル自体の作成に関連しています。たとえば AAA を行う方法、アドレス（DHCP やアドレス プール）を VPN クライアントに割り当てる方法などです。また、Firepower Threat Defense デバイスで設定された（または AAA サーバから得られる）グループ ポリシーで識別されるユーザ属性も、これらに含まれます。また、デバイスには *DefaultWEBVPNGroup* という名前のデフォルト接続プロファイルもあります。ウィザードを使って設定された接続プロファイルがリストに表示されます。

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 接続プロファイルを選択し、対応する編集アイコンをクリックします。
[接続プロファイルの編集（edit connection profile）] ページが表示されます。

ステップ 4 （オプション）複数の接続プロファイルを追加します。
複数の接続プロファイルの設定 （21 ページ）

ステップ 5 VPN クライアントの IP アドレスを設定します。
VPN クライアントの IP アドレスの設定 （22 ページ）

ステップ 6 （オプション）リモート アクセス VPN の AAA 設定を更新します。
リモート アクセス VPN 認証 （4 ページ）

ステップ 7 （オプション）エイリアスを作成または更新します。
接続プロファイルのエイリアスの作成または更新 （30 ページ）

ステップ 8 接続プロファイルを保存します。

複数の接続プロファイルの設定

別のグループの VPN ユーザに異なる権限を付与する場合は、各ユーザ グループの特定の接続プロファイルまたはグループ ポリシーを設定することができます。たとえば、経理グループ、カスタマー サポート グループ、および MIS（経営情報システム）グループが、プライベート ネットワークのそれぞれ異なる部分にアクセスできるようにする場合が考えられます。また、MIS に所属する特定のユーザには、他の MIS ユーザにはアクセスできないシステムにアクセスを許可する場合があります。接続プロファイルとグループ ポリシーにより、このような柔軟な設定を安全に実行することができます。

リモート アクセス ポリシー ウィザードを使用して VPN ポリシーを作成する場合に設定できる接続プロファイルは 1 つのみです。接続プロファイルは後で追加できます。また、デバイスには *DfaultWEBVPNGroup* というデフォルトの接続プロファイルもあります。

始める前に

リモートアクセス ポリシー ウィザードを使用し、接続プロファイルでリモートアクセス VPN が設定されていることを確認します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。
既存のリモート アクセス ポリシーがリストされます。

ステップ 2 リストから既存のリモートアクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 [追加（Add）] アイコンをクリックし、[接続プロファイルの追加（Add Connection Profile）] ウィンドウで次の項目を指定します。

a) [接続プロファイル（Connection Profile）]：リモート ユーザが VPN 接続のために使用する名前を指定します。接続プロファイルにはリモートユーザによる VPN デバイスへの接続方法を定義する一連のパラメータが含まれます。

b) [クライアントアドレスの割り当て（Client Address Assignment）]：リモート クライアントの IP アドレスは、ローカルの IP アドレス プール、DHCP サーバ、および AAA サーバから割り当てられます。

c) [AAA]：セキュア VPN ゲートウェイとして機能する管理対象デバイスが、どのユーザに（認証）、何を許可し（承認）、そのユーザが何を実行したか（アカウンティング）を判断できるようにAAAサーバを設定します。

d) [エイリアス（Aliases）]：接続プロファイルの代替名または URL を指定します。リモート アクセス VPN 管理者は、エイリアス名とエイリアス URL を有効または無効にできます。VPN ユーザは、AnyConnect VPN クライアントを使用して Firepower Threat Defense デバイスのリモート アクセス VPN に接続する場合にエイリアス名を使用できます。

ステップ 4 **[保存（Save）]** をクリックします。

関連トピック

接続プロファイルの設定 （21 ページ）

VPN クライアントの IP アドレスの設定

クライアント アドレスの割り当ては、リモート アクセス VPN ユーザ用の IP アドレスを割り当てる手段です。

リモート VPN クライアントの IP アドレスは、ローカルの IP アドレス プール、DHCP サーバ、および AAA サーバから割り当てように設定できます。最初に AAA サーバが割り当てられ、その後で他のものが割り当てられます。[詳細（Advanced）] タブで [クライアント アドレスの割り当て（Client Address Assignment）] ポリシーを設定して、割り当て基準を定義します。この接続プロファイルに関連付けられているグループ ポリシーやシステムのデフォルト グループ ポリシーである [DfltGrpPolicy] で定義された IP プールが存在しない場合、この接続プロファイルで定義されている IP プールのみが使用されます。

[IPv4 アドレス プール（IPv4 Address Pools）]：SSL VPN クライアントは、Firepower Threat Defense デバイスに接続したときに新しい IP アドレスを受け取ります。アドレス プールでは、

リモート クライアントが受け取ることのできるアドレス範囲が定義されます。既存の IP アドレス プールを選択します。IPv4 および IPv6 アドレスそれぞれに最大 6 つのプールを追加できます。

（注） Firepower Management Center の既存の IP プールから IP アドレスを使用するか、または [追加（Add）] オプションを使用して新しいプールを作成できます。また、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アドレスプール（Address Pools）] パスを使用して、Firepower Management Center に IP プールを作成することもできます。詳細については、アドレス プールを参照してください。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。
既存のリモート アクセス ポリシーがリストされます。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 更新する接続プロファイルを選択し、対応する [編集（Edit）] アイコンをクリックして、[クライアントアドレスの割り当て（Client Address Assignment）] タブを選択します。

ステップ 4 [アドレスプール（Address Pools）] で次の項目を選択します。

a) [追加（Add）] アイコンをクリックして IP アドレスを追加し、[IPv4] または [IPv6] を選択して対応するアドレス プールを追加します。利用可能なプールから IP アドレス プールを選択し、[追加（Add）] をクリックします。

（注） 複数の Firepower Threat Defense デバイス間でリモート アクセス VPN ポリシーを共有する場合は、すべてのデバイスが同じアドレス プールを共有することに留意してください。ただし、デバイスレベルのオブジェクト オーバーライドを使用して、グローバル定義をデバイスごとの一意なアドレス プールに置き換える場合を除きます。NAT を使用していないデバイスでアドレスが重複しないようにするには、一意なアドレス プールが必要です。

b) 新しい IPv4 または IPv6 アドレス プールを追加するには、[アドレスプール（Address Pools）] ウィンドウで [追加（Add）] アイコンを選択します。IPv4 プールを選択する場合は、開始と終了の IP アドレスを提供します。新しい IPv6 アドレス プールを含めることを選択する場合は、1 ～ 16384 の範囲の [アドレス数（Number of Addresses）] を入力します。オブジェクトが多数のデバイス間で共有される場合は、IP アドレスの競合を回避するために、[オーバーライドを許可（Allow Overrides）] オプションを選択します。詳細については、アドレス プールを参照してください。

c) [OK] をクリックします。

ステップ 5 [DHCPサーバ（DHCP Servers）] で次の項目を選択します。

（注） DHCP サーバ アドレスは、IPv4 アドレスでのみ設定可能です。

a) 名前と DHCP（Dynamic Host Configuration Protocol）のサーバ アドレスをネットワーク オブジェクトとして指定します。オブジェクト リストからサーバを選択するには、[追加（Add）] アイコンを選択します。DHCP サーバを削除するには、その行で [削除（Delete）] アイコンを選択します。

b) [新しいネットワーク オブジェクト（New Network Objects）] ウィンドウで [追加（Add）] アイコンを選択し、新しいネットワーク オブジェクトを追加します。新しいオブジェクト名、説明、ネットワークを入力し、必要に応じて [オーバーライドを許可（Allow Overrides）] オプションを選択します。詳細については、ネットワーク オブジェクトの作成およびオブジェクトのオーバーライドの許可を参照してください。

c) [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックします。

関連トピック

接続プロファイルの設定 （21 ページ）

リモートアクセス VPN の AAA 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。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 AAA 設定が更新されるように接続プロファイルを選択し、対応する [編集（Edit）] アイコンをクリックしてから、[AAA] タブをクリックします。

ステップ 4 [認証（Authentication）] で次の項目を選択します。

- [認証方式（Authentication Method）]：ユーザに対してネットワークとネットワーク サービスへのアクセスを許可する前に、ユーザの識別方法を決定します。有効なユーザ クレデンシャル（通常は、ユーザ名とパスワード）を要求することで、アクセスが制御されます。また、クライアントからの証明書

も含まれます。サポートされている認証方式は、[AAA のみ（AAA only）]、[クライアント証明書のみ（Client Certificate only）]、および [AAA とクライアント証明書（AAA + Client Certificate）] です。

[認証方式（Authentication Method）] の選択に応じて、次のようになります。

- [AAA のみ（AAA only）] : [認証サーバ（Authentication Server）] に [RADIUS] を選択した場合、デフォルトで許可サーバは同じ値になります。ドロップダウン リストから [アカウンティング サーバ（Accounting Server）] を選択します。認証サーバ ドロップダウン リストから [AD] と [LDAP] を選択した場合は常に、[認証サーバ（Authorization Server）] と [アカウンティング サーバ（Accounting Server）] をそれぞれ手動で選択する必要があります。
- [クライアント証明書のみ（Client Certificate Only）] : 各ユーザはクライアント証明書を使用して認証されます。クライアント証明書は、VPN クライアント エンドポイントで設定する必要があります。デフォルトでは、ユーザ名はクライアント証明書フィールド CN および OU から派生します。クライアント証明書の他のフィールドにユーザ名が指定されている場合は、[プライマリ（Primary）] と [セカンダリ（Secondary）] フィールドを使用して適切なフィールドをマップします。

  クライアント証明書のユーザ名が含まれる [マップ固有フィールド（Map Specific Field）] オプションを選択すると、[プライマリ（Primary）] および [セカンダリ（Secondary）] フィールドに [CN（一般名）（CN (Common Name)）] と [OU（組織ユニット）（OU (Organisational Unit)）] のデフォルト値がそれぞれ表示されます。[DN全体をユーザ名として使用（Use entire DN as username）] オプションを選択した場合、ユーザ ID が自動的に取得されます。識別名（DN）は、個々のフィールドから構成される一意の識別子であり、ユーザを接続プロファイルと照合するときに識別子として使用できます。DN ルールは、拡張証明書認証に使用されます。

  [固有のフィールドをマップ（Map specific field）] オプションに関連する [プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、次の共通の値が含まれています。

  - C（国）
  - CN（一般名）
  - DNQ（DN 修飾子）
  - EA（電子メール アドレス）
  - GENQ（世代識別子）
  - GN（姓名の名）
  - I（イニシャル）
  - L（地名）
  - N（名前）
  - O（組織）
  - OU（組織ユニット）
  - SER（シリアル番号）
  - SN（姓名の姓）

- SP（都道府県）
- T（タイトル）
- UID（ユーザ ID）
- UPN（ユーザ プリンシパル名）

- [クライアント証明書とAAA（Client Certificate & AAA）]：各ユーザはクライアント証明書とAAAサーバの両方を使用して認証されます。

  どの認証方式を選択する場合にも、[ユーザが承認データベースに存在するときにのみ接続を許可（Allow connection only if user exists in authorization database）] を選択または選択解除します。

- [認証サーバ（Authentication Server）]：認証とは、ユーザに対してネットワークとネットワーク サービスへのアクセスを許可する前に、ユーザの識別を行う方法です。認証には、有効なユーザ クレデンシャル、証明書、またはその両方が必要です。認証は、単独で使用することも、認可およびアカウンティングとともに使用することもできます。

  以前にリモート アクセス VPN ユーザを認証するように設定した LDAP または AD レルムか RADIUS サーバ グループを指定します。

- [セカンダリ認証を使用（Use secondary authentication）]：VPN セッションのセキュリティを強化するため、プライマリ認証の他にセカンダリ認証を設定します。セカンダリ認証は、[AAA のみ（AAA only）] と [クライアント証明書と AAA（Client Certificate & AAA）] の認証方式にのみ適用されます。

  セカンダリ認証はオプションの機能であり、2 つのセットのユーザ名とパスワードを AnyConnect ログイン画面に入力するにはVPNユーザが必要です。認証サーバまたはクライアント証明書からセカンダリ ユーザ名を事前入力するように設定することもできます。リモート アクセス VPN 認証は、プライマリとセカンダリの両方の認証が成功した場合にのみ許可されます。いずれの認証サーバに到達できない場合、1 つの認証が失敗すると、VPN 認証が拒否されます。

  セカンダリ認証の設定前に、2つ目のユーザ名とパスワードのセカンダリ認証のサーバグループ（AAA サーバ）を設定する必要があります。たとえば、プライマリ認証サーバをLDAPまたはActive Directoryレルムに、セカンダリ認証を RADIUS サーバに設定できます。

  （注） デフォルトでは、セカンダリ認証は必要ありません。

  [認証サーバ（Authentication Server）]：VPN ユーザのセカンダリ ユーザ名とパスワードを提供するセカンダリ認証サーバ。

  [セカンダリ認証のユーザ名（Username for secondary authentication）] で次の項目を選択します。

  - [プロンプト（Prompt）]：VPN ゲートウェイへのログイン中にユーザ名とパスワードを入力するようユーザに要求します。
  - [プライマリ認証ユーザ名を使用（Use primary authentication username）]：プライマリとセカンダリの両方の認証にプライマリ認証サーバからユーザ名が取得されます。パスワードは 2 つ入力する必要があります。

- [クライアント証明書からのユーザ名をマップ（Map username from client certificate）]：クライアント証明書からセカンダリ ユーザ名が事前に入力されます。
  - クライアント証明書のユーザ名を含む [固有のフィールドをマップ（Map specific field）] オプションを選択する場合。[プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、デフォルト値の [CN（共通名）（CN (Common Name)）] と [組織ユニット（OU）（OU (Organisational Unit)）] がそれぞれ表示されます。[DN（識別名）全体をユーザ名として使用（Use entire DN (Distinguished Name) as username）] オプションを選択した場合はユーザ ID が自動的に取得されます。

    プライマリとセカンダリのフィールドのマッピングの詳細については、「**認証方式**」の説明を参照してください。
  - [ユーザ ログイン ウィンドウに証明書からユーザ名を事前に入力（Prefill username from certificate on user login window）]：ユーザが AnyConnect VPN クライアント経由で接続したときにクライアント証明書からセカンダリ ユーザ名を事前に入力します。
    - [ログイン ウィンドウでユーザ名を非表示にする（Hide username in login window）]：セカンダリ ユーザ名はクライアント証明書から事前に入力されますがユーザには表示されず、ユーザが事前に入力されたユーザ名を変更しないようにします。

- [VPN セッションのセカンダリ ユーザ名を使用（Use secondary username for VPN session）]：VPN セッション中のユーザ アクティビティのレポートにセカンダリ ユーザ名を使用します。

ステップ 5 [認可（Authorization）] で次の項目を選択します。

- [認可（Authorization Server）]：認証の完了後、認可によって、認証済みの各ユーザが使用できるサービスおよびコマンドが制御されます。認可は、ユーザが実行を認可されていることを示す属性のセット、実際の機能、および制限事項をアセンブルすることによって機能します。認可を使用しない場合は、認証が単独で、認証済みのすべてのユーザに対して同じアクセス権を提供します。認可には、認証が必要です。RADIUS サーバのみが承認サービスでサポートされます。リモート アクセス VPN 認可の仕組みについては、権限および属性のポリシー実施の概要 （6 ページ）を参照してください。

  リモート アクセス VPN ユーザを承認するように事前設定された RADIUS サーバ グループ オブジェクトを入力または選択します。

  RADIUS サーバが接続プロファイルのユーザ承認用に構成されている場合、リモート アクセス VPN システムの管理者は、ユーザまたはユーザ グループに複数の承認属性を構成できます。RADIUS サーバに構成される承認属性は、ユーザまたはユーザ グループに固有にできます。ユーザが認証されると、これらの特定の承認属性が Firepower Threat Defense デバイスにプッシュされます。

  （注） 許可サーバから所得した AAA サーバ属性は、グループ ポリシーまたは接続プロファイルで事前に設定されていた可能性がある属性値を上書きします。

- 必要な場合は、[ユーザが承認データベースに存在するときにのみ接続を許可（Allow connection only if user exists in authorization database）] をオンにします。

  有効にすると、システムは正常に接続するために、クライアントのユーザ名が承認データベース内に存在することを確認します。ユーザ名が承認データベース内に存在しない場合、接続が拒否されます。

ステップ 6 [アカウンティング（Accounting）] で次の項目を選択します。

- [アカウンティングサーバ（Accounting Server）]：アカウンティングは、ユーザがアクセスしているサービス、およびユーザが消費しているネットワーク リソース量を追跡するために使用されます。AAAアカウンティングがアクティブになると、ネットワーク アクセス サーバはユーザ アクティビティを RADIUS サーバに報告します。アカウンティング情報には、セッションの開始時刻と停止時刻、ユーザ名、セッションごとのデバイスを通過したバイト数、使用されたサービス、および各セッションの時間が含まれています。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。アカウンティングは、単独で使用するか、認証および認可とともに使用することができます。

  リモート アクセス VPN セッションを構成するために使用される RADIUS サーバ グループ オブジェクトを指定します。

ステップ 7 [詳細設定（Advanced Settings）] で次の項目を選択します。

- [ユーザ名からレルムを削除（Strip Realm from username）]：ユーザ名を AAA サーバに渡す前に、ユーザ名からレルムを削除するには選択します。たとえば、このオプションを選択して、*domain\username* を指定した場合、ユーザ名からドメインが削除され、認証用の AAA サーバに送信されます。デフォルトでは、このオプションはオフになっています。
- [ユーザ名からグループを削除（Strip Group from username）]：ユーザ名を AAA サーバに渡す前に、ユーザ名からグループを削除するには選択します。デフォルトでは、このオプションはオフになっています。

  （注） レルムとは管理ドメインのことです。これらのオプションを有効にすると、ユーザ名だけに基づいて認証できます。これらのオプションを任意に組み合わせて有効にできます。ただし、サーバが区切り文字を解析できない場合は、両方のチェックボックスをオンにする必要があります。
- [パスワード管理（Password Management）]：リモート アクセス VPN ユーザのパスワードを管理できるようにします。パスワードが期限切れになる前に通知するか、パスワードが期限切れになる日に通知するかを選択します。

ステップ 8 **[保存（Save）]** をクリックします。

の RADIUS サーバ属性 Firepower Threat Defense

Firepower Threat Defense デバイスは、リモート アクセス VPN ポリシーで認証および/または承認のために設定された外部 RADIUS サーバから、VPN 接続にユーザ承認属性（ユーザの権利または権限とも呼ばれる）を適用することをサポートしています。

（注） Firepower Threat Defense デバイスはベンダー ID 3076 の属性をサポートしています。

次のユーザ認可属性が Firepower Threat Defense デバイスから RADIUS サーバに送信されます。

- RADIUS 属性 146 および 150 は、認証および認可の要求の場合に Firepower Threat Defense デバイスから RADIUS サーバに送信されます。
- 3 つの属性（146、150、151）はすべて、アカウンティングの開始、暫定更新、および停止要求のために、Firepower Threat Defense デバイスから RADIUS サーバに送信されます。

表 *1 : Firepower Threat Defense* から *RADIU* サーバに送信される *RADIUS* 属性

属性	Attribute Number	構文、タイプ	シングルまたはマルチ値	説明または値
接続プロファイル名またはトンネル グループ名。	146	文字列	シングル	1 ～ 253 文字
クライアント タイプ（Client Type）	150	整数	シングル	2 = AnyConnect クライアント SSL VPN、6 = AnyConnect クライアント IPsec VPN（IKEv2）
セッション タイプ	151	整数	シングル	1 = AnyConnect クライアント SSL VPN、2 = AnyConnect クライアント IPsec VPN（IKEv2）

表 *2 :* 送信される *RADIUS* 属性 *Firepower Threat Defense*

属性	Attribute Number	構文、タイプ	シングルまたはマルチ値	説明または値
Access-List-Inbound	86	文字列	シングル	アクセス リスト属性の両方が、FTDデバイスで設定されている ACL の名前を使用します。スマート CLI 拡張アクセス リストのオブジェクト タイプを使用して、これらの ACL を作成します（**[デバイス（Device）] > [詳細設定（Advanced Configuration）] > [スマートCLI（Smart CLI）] > [オブジェクト（Object）]** を選択します）。 これらの ACL は、着信（FTD デバイスに入るトラフィック）または発信（FTDデバイスから出るトラフィック）方向のトラフィックフローを制御します。
Access-List-Outbound	87	文字列	シングル	
Address-Pools	217	文字列	シングル	FTDデバイスで定義されたネットワークオブジェクトの名前。RA VPN へのクライアント接続のアドレスプールとして使用されるサブネットを識別します。[Objects] ページでネットワークオブジェクトを定義します。
Banner1	15	文字列	シングル	ユーザがログインするときに表示されるバナー。

属性	Attribute Number	構文、タイプ	シングルまたはマルチ値	説明または値
Banner2	36	文字列	シングル	ユーザがログインするときに表示されるバナーの 2 番目の部分。Banner2 は Banner1 に付加されます。
ダウンロード可能 ACL（Downloadable ACLs）	Cisco-AV-Pair	merge-dacl {before-avpair | after-avpair}		Cisco-AV-Pair 構成でサポートされます。
Filter ACLs	86、87	文字列	シングル	フィルタ ACL は、RADIUS サーバで ACL 名で参照されます。ACL 設定が Firepower Threat Defense デバイス上にすでに存在していて、RADIUS 承認時に使用できるようにする必要があります。 86 = アクセスリスト-インバウンド 87 = アクセスリスト-アウトバウンド
Group-Policy	25	文字列	シングル	接続に使用されるグループポリシー。RA VPN の [Group Policy] ページでグループポリシーを作成する必要があります。次の形式のいずれかを使用できます。 • グループ ポリシー名 • OU=グループ ポリシー名 • OU=グループ ポリシー名;
Simultaneous-Logins	2	整数	シングル	ユーザが確立を許可されている個別の同時接続の数（0 ～ 2147483647）。
VLAN	140	整数	シングル	ユーザの接続を制限する VLAN（0 ～ 4094）。FTD デバイスのサブインターフェイスでも、この VLAN を設定する必要があります。

接続プロファイルのエイリアスの作成または更新

エイリアスには、特定の接続プロファイルの代替名または URL が含まれます。リモート アクセス VPN 管理者は、エイリアス名とエイリアス URL を有効または無効にできます。VPN ユーザは、Firepower Threat Defense デバイスに接続するときにエイリアス名を選択できます。このデバイスに設定されているすべての接続のエイリアス名の表示をオンまたはオフにできます。また、リモート アクセス VPN 接続の開始時にエンドポイントが選択できるエイリアス URL のリストを設定することもできます。ユーザがエイリアス URL を使用して接続すると、システムはエイリアス URL と一致する接続プロファイルを使用して自動的にそのユーザをログに記録します。

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 使用可能な VPN ポリシーのリストから、設定を変更するポリシーを選択します。

ステップ 3 接続プロファイルを選択し、対応する編集アイコンをクリックします。

ステップ 4 [エイリアス（Aliases）] タブをクリックします。

ステップ 5 エイリアス名を追加するには、次の手順を実行します。

a) [エイリアス名（Alias Names）] の [追加（Add）] をクリックします。
b) [エイリアス名（Alias Name）] を指定します。
c) エイリアスを有効にするには、各ウィンドウで [有効（Enabled）] チェックボックスをオンにします。
d) [OK] をクリックします。

ステップ 6 エイリアス URL を追加するには、次の手順を実行します。

a) [エイリアスURL（Alias URL）] の [追加（Add）] をクリックします。
b) リストから [エイリアスURL（Alias URL）] を選択するか、新しい URL オブジェクトを作成します。詳細については、URL オブジェクトの作成を参照してください。
c) エイリアスを有効にするには、各ウィンドウで [有効（Enabled）] チェックボックスをオンにします。
d) [OK] をクリックします。

- エイリアス名またはエイリアス URL を編集するには、[編集（Edit）] アイコンをクリックします。
- エイリアス名またはエイリアス URL を削除するには、その行で [削除（Delete）] アイコンをクリックします。

ステップ 7 **[保存（Save）]** をクリックします。

関連トピック

接続プロファイルの設定 （21 ページ）

リモートアクセス VPN のアクセス インターフェイスの設定

[アクセス インターフェイス（Access Interface）] テーブルには、デバイス インターフェイスを含むインターフェイス グループとセキュリティ ゾーンが示されています。これらは、リモート アクセス SSL または IPsec IKEv2 VPN 接続用に設定されています。このテーブルには、各インターフェイス グループまたはセキュリティ ゾーン、インターフェイスで使用されるインターフェイス トラストポイント、および Datagram Transport Layer Security（DTLS）が有効かどうかが表示されます。

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。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 リストから既存のリモートアクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 [アクセスインターフェイス（Access Interface）] タブをクリックします。

ステップ 4 アクセスインターフェイスを追加するには、[追加（Add）] アイコンを選択し、[アクセスインターフェイスの追加（Add Access Interface）] ウィンドウで以下に対する値を指定します。

a) [アクセスインターフェイス（Access Interface）]：インターフェイスが属するインターフェイス グループまたはセキュリティ ゾーンを選択します。

インターフェイス グループまたはセキュリティ ゾーンは、ルーテッド タイプでなければなりません。他のインターフェイス タイプは、リモート アクセス VPN 接続ではサポートされていません。

b) 次のオプションを選択して、アクセスインターフェイスに [プロトコル（Protocol）] オブジェクトを関連付けます。

- [IPSet-IKEv2の有効化（Enable IPSet-IKEv2）]：**IKEv2** 設定を有効にするには、このオプションを選択します。
- [SSL の有効化（Enable SSL）]：**SSL** 設定を有効にするには、このオプションを選択します。
  - [Datagram Transport Layer Security の有効化（Enable Datagram Transport Layer Security）] を選択します。

    選択すると、インターフェイスで Datagram Transport Layer Security（DTLS）がイネーブルになり、AnyConnect VPN Client は 2 つの同時トンネル（SSL トンネルと DTLS トンネル）を使用して SSL VPN 接続を確立できます。

DTLS を有効にすると、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

- [インターフェイス固有のアイデンティティ証明書を設定する（Configure Interface Specific Identity Certificate）] チェックボックスをオンにして、ドロップダウン リストから [インターフェイスアイデンティティ証明書（Interface Identity Certificate）] を選択します。

  [インターフェイスアイデンティティ証明書（Interface Identity Certificate）] を選択しないと、[トラストポイント（Trustpoint）] がデフォルトで使用されます。

  [インターフェイスアイデンティティ証明書（Interface Identity Certificate）] または [トラストポイント（Trustpoint）] を選択しないと、[SSLグローバルアイデンティティ証明書（SSL Global Identity Certificate）] がデフォルトで使用されます。

c) [OK] をクリックして変更を保存します。

ステップ 5 [アクセス設定（Access Settings）] で次の項目を選択します。

- [ユーザがログイン中に接続プロファイルを選択することを許可する（Allow Users to select connection profile while logging in）]：複数の接続プロファイルがある場合、このオプションを選択すると、ユーザはログイン時に正しい接続プロファイルを選択できます。このオプションを **IPsec-IKEv2** VPN に選択する必要があります。

ステップ 6 [SSL設定（SSL Settings）] で次のオプションを使用します。

- [Web アクセス ポート番号（Web Access Port Number）]：VPN セッションで使用するポート。デフォルト ポートは 443 です。
- [DTLS ポート番号（DTLS Port Number）]：DTLS 接続に使用する UDP ポート。デフォルト ポートは 443 です。
- [SSLグローバルアイデンティティ証明書（SSL Global Identity Certificate）]：[インターフェイス固有のアイデンティティ証明書（Interface Specific Identity Certificate）] が提供されていない場合、選択した [SSLグローバルアイデンティティ証明書（SSL Global Identity Certificate）] がすべての関連インターフェイスに使用されます。

ステップ 7 [IPsec-IKEv2設定（IPsec-IKEv2 Settings）] の場合、リストから [IKEv2アイデンティティ証明書（IKEv2 Identity Certificate）] を選択するか、アイデンティティ証明書を追加します。

ステップ 8 [VPNトラフィックのアクセスコントロール（Access Control for VPN Traffic）] セクションで、アクセス コントロール ポリシーをバイパスする場合に次のオプションを選択します。

- [復号されたトラフィック（sysopt permit-vpn）に対するバイパス アクセス コントロール ポリシー（Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)）]：デフォルトでは、復号されたトラフィックは、アクセス コントロール ポリシーのインスペクションの対象になります。復号されたトラフィック オプションに対してバイパス アクセス コントロール ポリシーを有効にすると、ACL インスペクションがバイパスされますが、AAA サーバからダウンロードされた VPN フィルタ ACL と認証 ACL は、VPN トラフィックに引き続き適用されます。

（注） このオプションを選択した場合は、Firepower Threat Defense デバイスのアクセス コントロール ポリシーの更新 （16 ページ） で指定したリモート アクセス VPN のアクセス コントロール ポリシーを更新する必要はありません。

ステップ 9 [保存（Save）] をクリックしてアクセス インターフェイスの変更を保存します。

関連トピック

インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン

リモート アクセス VPN の高度なオプションの設定

Cisco AnyConnect セキュア モビリティ クライアント イメージ

Cisco AnyConnect セキュア モビリティ クライアント イメージ

Cisco AnyConnect セキュア モビリティ クライアントは Firepower Threat Defense デバイスへのセキュアな SSL 接続または IPsec（IKEv2）接続を提供し、これにより、リモート ユーザによる企業リソースへのフル VPN プロファイリングが可能となります。インストール済みのクライアントがない場合、リモート ユーザは、クライアントレス VPN 接続を受け入れるように設定されたインターフェイスの IP アドレスをブラウザに入力し、AnyConnect クライアントをダウンロードしてインストールすることができます。Firepower Threat Defense デバイスは、リモート コンピュータのオペレーティング システムに適合するクライアントをダウンロードします。ダウンロード後に、クライアントがインストールされてセキュアな接続が確立されます。すでにクライアントがインストールされている場合は、ユーザの認証時に Firepower Threat Defense デバイスがクライアントのバージョンを検査し、必要に応じてクライアントをアップグレードします。

リモート アクセス VPN 管理者は、新規または追加の AnyConnect クライアント イメージを VPN ポリシーに関連付けます。管理者は、サポート対象外または期限切れで不要になったクライアント パッケージの関連付けを解除できます。

Firepower Management Center は、ファイル パッケージ名を使用してオペレーティング システムの種類を判別します。ユーザがオペレーティング システム情報を示さずにファイルの名前を変更した場合は、有効なオペレーティング システム タイプをリスト ボックスから選択する必要があります。

シスコのソフトウェア ダウンロード センターを参照して AnyConnect クライアント イメージ ファイルをダウンロードします。

関連トピック

への Cisco AnyConnect Mobility クライアント イメージの追加 Firepower Management Center （35 ページ）

への Cisco AnyConnect Mobility クライアント イメージの追加 Firepower Management Center

[AnyConnectファイル（AnyConnect File）] オブジェクトを使用して、Cisco AnyConnect Mobility クライアント イメージを Firepower Management Center にアップロードすることもできます。詳細については、FTD ファイル オブジェクトを参照してください。クライアント イメージの詳細については、Cisco AnyConnect セキュア モビリティ クライアント イメージ （34 ページ）を参照してください。

特定のクライアント イメージを表示するには、[再注文ボタンの表示（Show re-order buttons）] リンクをクリックします。

（注） すでにインストールされている Cisco AnyConnect クライアント イメージを削除するには、その行の [削除（Delete）] アイコンをクリックします。

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。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

ステップ 1 Firepower Management Center Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）]、リストされている RA VPN ポリシーを選択および編集し、[詳細設定（Advanced）] タブを選択します。 を選択します

ステップ 2 [AnyConnect イメージ（AnyConnect Images）] ダイアログの [使用可能な AnyConnect イメージ（Available AnyConnect Images）] 部分で [追加（Add）] アイコンをクリックします。

ステップ 3 使用可能な AnyConnect イメージの [名前（Name）]、[ファイル名（File Name）]、および [説明（Description）] を入力します。

ステップ 4 [参照（Browse）] をクリックして、アップロードするクライアント イメージを選択する場所に移動します。

ステップ 5 [保存（Save）] をクリックしてイメージを Firepower Management Center にアップロードします。
クライアント イメージを Firepower Management Center にアップロードすると、オペレーティング システムに Firepower Management Center にアップロードされたイメージのプラットフォーム情報が表示されます。

関連トピック

Cisco AnyConnect セキュア モビリティ クライアント イメージ （34 ページ）

リモート アクセス VPN クライアントに対する AnyConnect イメージの更新

シスコのソフトウェア ダウンロード センターで新しい AnyConnect クライアント更新を入手できる場合は、そのパッケージを手動でダウンロードしてリモート アクセス VPN ポリシーに追加します。それにより、オペレーティング システムに応じて VPN クライアント システム上で新しい AnyConnect パッケージがアップグレードされます。

始める前に

この項の手順は、Firepower Threat Defense VPN ゲートウェイに接続しているリモート アクセス VPN クライアントに新しい AnyConnect クライアント イメージを更新するのに役立ちます。AnyConnect のイメージを更新する前に、次の設定が完了していることを確認します。

- シスコのソフトウェア ダウンロード センターから最新の AnyConnect イメージ ファイルをダウンロードします。
- Firepower Management Center の Web インターフェイスで、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [AnyConnect ファイル（AnyConnect File）] に移動し、新しいAnyConnect クライアント イメージ ファイルを追加します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リストから既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 [詳細（Advanced）] > [AnyConnect クライアント イメージ（AnyConnect Client Image）] >[追加（Add）] をクリックします。

ステップ 4 [利用可能なAnyConnectイメージ（Available AnyConnect Images）] からクライアント イメージ ファイルを選択し、[追加（Add）] をクリックします。

必要な AnyConnect クライアント イメージが表示されていない場合は、[追加（Add）] アイコンをクリックして参照し、イメージをアップロードします。

ステップ 5 リモート アクセス VPN ポリシーを保存します。
リモート アクセス VPN ポリシーの変更が展開されると、リモート アクセス VPN ゲートウェイとして設定されている Firepower Threat Defense デバイスで新しい AnyConnect クライアント イメージが更新されます。新しい VPN ユーザが VPN ゲートウェイに接続すると、クライアント イメージのオペレーティング システムに応じて、新しい AnyConnect クライアント イメージがダウンロードされます。既存の VPN ユーザの場合、AnyConnect クライアント イメージは次の VPN セッションで更新されます。

関連トピック

リモート アクセス VPN 接続プロファイル オプション

リモート アクセス VPN のアドレス割り当てポリシー

Firepower Threat Defense デバイスは、IPv4 または IPv6 ポリシーを使用して、リモート アクセス VPN クライアントに IP アドレスを割り当てることができます。複数のアドレス割り当て方式を設定すると、Firepower Threat Defense デバイスは IP アドレスが見つかるまで各オプションを試行します。

IPv4 または IPv6 ポリシー

IPv4 または IPv6 ポリシーを使用すると、リモート アクセス VPN クライアントへの IP アドレスに対応できます。まず、IPv4 ポリシーを試してから、次に IPv6 ポリシーを試す必要があります。

- [承認サーバを使用（Use Authorization Server）]：ユーザごとに外部承認サーバからアドレスを取得します。IP アドレスが設定された承認サーバを使用している場合は、この方式を使用することをお勧めします。アドレス割り当ては、RADIUS ベースの承認サーバでのみサポートされています。AD/LDAP ではサポートされていません。この方法は、IPv4 と IPv6 の両方の割り当てポリシーで使用できます。
- [DHCP を使用（Use DHCP）]：接続プロファイルに設定された DHCP サーバから IP アドレスを取得します。グループ ポリシーで DHCP ネットワーク範囲を設定することによって、DHCP サーバが使用できる IP アドレスの範囲を定義することもできます。DHCP を使用する場合は、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [ネットワーク（Network）] ペインでサーバを設定します。この方法は IPv4 の割り当てポリシーに使用できます。
- [内部アドレス プールを使用（Use an internal address pool）]：内部的に設定されたアドレス プールは、最も設定が簡単なアドレス プール割り当て方式です。この方式を使用する場合は、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [アドレス プール（Address Pools）] ペインで IP アドレス プールを作成し、接続プロファイルで同じものを選択します。この方法は、IPv4 と IPv6 の両方の割り当てポリシーで使用できます。
- [IP アドレスが解放された後時間が経ってから IP アドレスを再利用する（Reuse an IP address so many minutes after it is released）]：IP アドレスがアドレス プールに戻った後、IP アドレスの再使用を遅らせます。遅延時間を設けることにより、IP アドレスがすぐに再割り当てされることによって発生する問題がファイアウォールで生じないようにできます。デフォルトでは、遅延はゼロに設定されています。つまり、Firepower Threat Defense デバイスは IP アドレスの再使用の際に遅延を課しません。遅延時間を延長する場合は、IP アドレスを再割り当てするまでの時間を 0 ～ 480 の範囲で指定します。この設定要素は、IPv4 割り当てポリシーで使用できます。

関連トピック

接続プロファイルの設定 （21 ページ）
リモート アクセス VPN 認証 （4 ページ）

証明書マップの設定

証明書マップを使用して、証明書フィールドの内容に基づいて接続プロファイルとユーザ証明書をマッチングするルールを定義できます。証明書マップは、セキュア ゲートウェイでの証明書認証に使用されます。

ルール、または証明書マップは、FTD 証明書のマップ オブジェクトについてで定義されます。

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 **[詳細（Advanced）]** > **[証明書マップ（Certificate Maps）]** をクリックします。

ステップ 4 [証明書グループ照合の全般設定（General Settings for Certificate Group Matching）] ペインで次のオプションを選択します。

優先順位に基づいて選択されます。つまり、最初の選択候補で一致するものが見つからなかった場合、オプション リストの次の候補がマッチングされます。ルールが満たされると、マッピングが実行されます。ルールが満たされない場合、デフォルトの接続プロファイル（下に表示されている）がこの接続に使用されます。次のいずれか、またはすべてのオプションを選択して、認証を確立し、クライアントにマッピングする必要のある接続プロファイル（トンネル グループ）を決定します。

- **グループ URL と証明書マップが異なる接続プロファイルと一致する場合、グループ URL を使用します**
- [設定されているルールを使用して証明書を接続プロファイルと照合（Use the configured rules to match a certificate to a Connection Profile）]：接続プロファイル マップで定義されているルールを使用するには、これを有効にします。

（注） 証明書マッピングを設定することは、証明書に基づく認証を意味します。設定されている認証方法に関係なく、リモート ユーザはクライアント証明書を提供するよう求められます。

ステップ 5 [証明書から接続プロファイルへのマップ（Certificate to Connection Profile Map）] セクションで、[マッピングの追加（Add Mapping）] をクリックし、このポリシーの証明書から接続プロファイルへのマッピングを作成します。

a) [証明書マップ（Certificate Map）] オブジェクトを選択するか、作成します。
b) 証明書マップ オブジェクトのルールが満たされた場合に使用する必要のある [接続プロファイル（Connection Profile）] を選択します。
c) [OK] をクリックして、マッピングを作成します。

ステップ 6 **[保存（Save）]** をクリックします。

グループ ポリシーの設定

グループ ポリシーはグループ ポリシー オブジェクト内に保存される属性と値の一連のペアで、リモート アクセス VPN のエクスペリエンスを定義します。たとえば、グループ ポリシー オブジェクトで、アドレス、プロトコル、接続設定などの一般的な属性を設定します。

ユーザに適用されるグループ ポリシーはVPN トンネルが確立される際に決定されます。RADIUS 承認サーバがグループ ポリシーを割り当てるか、または現在の接続プロファイルから取得されます。

（注） FTD ではグループ ポリシー属性の継承はありません。ユーザについては、グループ ポリシー オブジェクトが全体として使用されます。ログイン時に AAA サーバで特定されたグループ ポリシー オブジェクトが使用されるか、またはこれが指定されていない場合は、VPN 接続に対して設定されたデフォルトのグループ ポリシーが使用されます。指定されたデフォルトのグループ ポリシーはデフォルト値に設定できますが、これは、接続プロファイルに割り当てられ、他のグループ ポリシーがユーザに対して特定されていない場合にのみ使用されます。

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
いずれか（Any）	該当なし	FTD	いずれか（Any）	Admin

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 **[詳細（Advanced）]** > **[グループ ポリシー（Group Policies）]** をクリックします。

ステップ 4 このリモート アクセス VPN ポリシーに関連付けるグループ ポリシーをさらに選択します。これらは、リモート アクセス VPN ポリシー作成中に割り当てられたデフォルトのグループ ポリシーを凌駕するものです。[追加（Add）] をクリックします。

[更新（Refresh）] と [検索（Search）] ユーティリティを使用して、グループ ポリシーを検索します。必要に応じて、新しいグループ ポリシー オブジェクトを追加します。

ステップ 5 利用可能なグループ ポリシーから [グループポリシー（group policies）] を選択し、[追加（Add）] をクリックして選択します。

ステップ 6 [OK] をクリックして、グループ ポリシーの選択を完了します。

関連トピック

グループ ポリシー オブジェクトの設定

リモート アクセス VPN の IPsec の設定

IPsec 設定は、リモート アクセス VPN ポリシーを設定する際に、VPN プロトコルとして IPsec を選択した場合にのみ適用可能です。そうでない場合は、[アクセス インターフェイスの編集（Edit Access Interface）] ダイアログボックスを使用して、IKEv2 を有効にすることができます。詳細については、リモートアクセス VPN のアクセス インターフェイスの設定 （31 ページ）を参照してください。

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。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 使用可能な VPN ポリシーのリストから、設定を変更するポリシーを選択します。

ステップ 3 [Advanced] タブをクリックします。
IPsec 設定のリストは、画面左側のナビゲーション ウィンドウに表示されます。

ステップ 4 ナビゲーション ウィンドウを使用して、次の IPsec オプションを編集します。

a) 暗号マップ（Crypto Maps）：[暗号マップ（Crypto Maps）]ページには、IKEv2 プロトコルが有効になっているインターフェイス グループがリストされます。暗号マップは、IKEv2 プロトコルが有効になっているインターフェイス用に自動生成されます。暗号マップを編集するには、リモート アクセス VPN 暗号マップの設定 （41 ページ）を参照してください。[アクセス インターフェイス（Access Interface）] タブで、選択した VPN ポリシーにインターフェイス グループを追加または削除できます。詳細については、リモートアクセス VPN のアクセス インターフェイスの設定 （31 ページ）を参照してください。

b) IKE ポリシー（IKE Policy）：[IKE ポリシー（IKE Policy）] ページには、AnyConnect エンドポイントが IPsec プロトコルを使用して接続している場合、選択した VPN ポリシーに適用可能なすべての IKE ポリシー オブジェクトがリストされます。詳細については、リモート アクセス VPN での IKE ポリシー

（44 ページ）を参照してください。新しい IKE ポリシーを追加するには、IKEv2 ポリシー オブジェクトの設定を参照してください。FTD がサポートしているのは AnyConnect IKEv2 のみです。サードパーティ標準の IKEv2 クライアントはサポートされていません。

c) [IPsec/IKEv2 パラメータ（IPsec/IKEv2 Parameters）]：[IPsec/IKEv2 パラメータ（IPsec/IKEv2 Parameters）] ページでは、IKEv2 セッション設定、IKEv2 セキュリティ アソシエーション設定、IPsec 設定、および NAT 透過設定を変更できます。詳細については、リモート アクセス VPN の [IPsec/IKEv2パラメータ（IPsec/IKEv2 Parameters）] の設定 （45 ページ）を参照してください。

ステップ 5 **[保存（Save）]** をクリックします。

リモート アクセス VPN 暗号マップの設定

暗号マップは、IPsec-IKEv2 プロトコルが有効になっているインターフェイス用に自動生成されます。[アクセス インターフェイス（Access Interface）] タブで、選択した VPN ポリシーにインターフェイス グループを追加または削除できます。詳細については、リモートアクセス VPN のアクセス インターフェイスの設定 （31 ページ）を参照してください。

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。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]** を選択します。

ステップ 2 使用可能な VPN ポリシーのリストから、設定を変更するポリシーを選択します。

ステップ 3 [詳細設定（Advanced）] > [暗号マップ（Crypto Maps）] をクリックし、テーブルの行を選択して、[編集（Edit）] アイコンをクリックし、暗号マップ オプションを編集します。

ステップ 4 [IKEv2 IPsecプロポーザル（IKEv2 IPsec Proposals）] を選択し、トランスフォーム セットを選択して、トンネル内のトラフィックの保護に使用される認証アルゴリズムおよび暗号化アルゴリズムを指定します。

ステップ 5 [リバースルートインジェクションを有効にする（Enable Reverse Route Injection）] を選択し、スタティック ルートは、リモート トンネル エンドポイントで保護されているネットワークとホストのルーティング プロセスに自動的に挿入されます。

ステップ 6 [クライアントサービスの有効化（Enable Client Services）] を選択し、ポート番号を指定します。

クライアント サービス サーバは、HTTPS（SSL）アクセスを提供します。これにより、AnyConnect ダウンロードは、ソフトウェア アップグレード、プロファイル、ローカリゼーションおよびカスタマイゼーション ファイル、CSD、SCEP、および AnyConnect クライアントが必要とするその他のファイル ダウンロードを受信できます。このオプションを選択した場合は、クライアント サービスのポート番号を指定します。クライアント サービス サーバを有効にしない場合、ユーザは、AnyConnect クライアントが必要する可能性があるこれらのファイルをダウンロードできません。

（注） 同じデバイスで実行する SSL VPN に対して同じポートを使用できます。SSL VPN を設定した場合でも、IPsec-IKEv2 クライアントで SSL を介してファイルをダウンロードするには、このオプションを選択する必要があります。

ステップ 7 [Perfect Forward Secrecyの有効化（Enable Perfect Forward Secrecy）] を選択し、[係数グループ（Modulus Group）] を選択します。

暗号化された交換ごとに一意のセッション キーを生成および使用するために、Perfect Forward Secrecy（PFS）を使用します。固有のセッション キーを使用することで、後続の復号から交換が保護されます。また、交換全体が記録されていて、攻撃者がエンドポイント デバイスで使用されている事前共有キーや秘密キーを入手している場合であっても保護されます。このオプションを選択する場合は、[係数グループ（Modulus Group）] リストで、PFS セッション キーの生成時に使用する Diffie-Hellman キー導出アルゴリズムも選択します。

係数グループは、2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループです。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。リモート アクセス VPN 設定を許可する係数グループを選択します。

- [1]：Diffie-Hellman グループ 1（768 ビット係数）。
- [2]：Diffie-Hellman グループ 2（1024 ビット係数）。
- [5]：Diffie-Hellman グループ 5（1536 ビット係数。128 ビット キーの保護に推奨されるが、グループ 14 の方がより強力）。AES 暗号化を使用する場合は、このグループ（またはそれ以上）を使用します。
- [14]：Diffie-Hellman グループ 14（2048 ビット係数。128 ビット キーの保護に推奨される）。
- [19]：Diffie-Hellman グループ 19（256 ビットの楕円曲線フィールド サイズ）。
- [20]：Diffie-Hellman グループ 20（384 ビットの楕円曲線フィールド サイズ）。
- [21]：Diffie-Hellman グループ 21（521 ビットの楕円曲線フィールド サイズ）。
- [24]：Diffie-Hellman グループ 24（2048 ビット係数および 256 ビット素数位数サブグループ）。

ステップ 8 [ライフタイム継続時間（秒数）（Lifetime Duration (seconds)）] を指定します。

セキュリティ アソシエーション（SA）のライフタイム（秒数）。このライフタイムを超えると、SA の期限が切れ、2つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。

120 ～ 2147483647 秒の値を指定できます。デフォルトは 28800 秒です。

ステップ 9 [ライフタイムのサイズ（KB）（Lifetime Size (kbytes)）] を指定します。

特定のセキュリティ アソシエーションが期限切れになる前にそのセキュリティ アソシエーションを使用して IPsec ピア間を通過できるトラフィック量（KB 単位）。

10 ～ 2147483647 KB の値を指定できます。デフォルトは 4,608,000 KB です。無限のデータを指定することはできません。

ステップ 10 次の [ESPv3設定（ESPv3 Settings）] を選択します。

- [着信ICMPのエラーメッセージを検証（Validate incoming ICMP error messages）]：IPsec トンネルを介して受信され、プライベート ネットワーク上の内部ホストが宛先の ICMP エラー メッセージを検証するかどうかを選択します。
- [「フラグメント禁止」ポリシーを有効にする（Enable 'Do Not Fragment' Policy）]：IP ヘッダーに Do-Not-Fragment（DF）ビット セットを使用する大量のパケットを IPsec サブシステムがどのように処理するかを定義し、[ポリシー（Policy）] リストからいずれかの項目を選択します。
  - コピー（Copy）：DF ビットを保持します。
  - クリア（Clear）：DF ビットを無視します。
  - 設定（Set）：DF ビットを設定して使用します。
- [トラフィックフロー機密保持（TFC）パケットを有効にする（Enable Traffic Flow Confidentiality (TFC) Packets）]：トンネルを通過するトラフィック プロファイルをマスクするダミーの TFC パケットを有効にします。[バースト（Burst）]、[ペイロード サイズ（Payload Size）]、および [タイムアウト（Timeout）] パラメータを使用して、指定した SA で不定期にランダムな長さのパケットを生成します。
  - バースト（Burst）：1 ～ 16 バイトの値を指定します。
  - ペイロード サイズ（Payload Size）：64 ～ 1024 バイトの値を指定します。
  - タイムアウト（Timeout）：10 ～ 60 秒の値を指定します。

ステップ 11 [OK] をクリックします。

関連トピック

インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン

リモート アクセス VPN での IKE ポリシー

Internet Key Exchange（IKE、インターネット キー エクスチェンジ）は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA、セキュリティ アソシエーション）の自動的な確立に使用されるキー管理プロトコルです。IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE によって IPsec などの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKE プロポーザルは、2 つのピア間のネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。

（注） FTD は、リモート アクセス VPN では IKEv2 のみサポートします。

IKEv1 とは異なり、IKEv2 プロポーザルでは、1 つのポリシーで複数のアルゴリズムおよびモジュラス グループを選択できます。フェーズ 1 のネゴシエーションでピアを選択するため、作成する IKE プロポーザルの数を 1 つにすることは可能ですが、複数の異なる IKE プロポーザルを作成して、最も望ましいオプションを高い優先順位に設定することも検討してください。IKEv2 では、ポリシー オブジェクトが認証方式を指定しないため、その他のポリシーで認証要件を定義する必要があります。

リモート アクセス IPsec VPN を設定する際には IKE ポリシーが必要です。

リモート アクセス *VPN IKE* ポリシーの設定

IKE ポリシー テーブルには、IPsec プロトコルを使用して AnyConnect のエンドポイントを接続するとき、選択した VPN 設定に利用可能なすべての IKE ポリシー オブジェクトを記述します。詳細については、リモート アクセス VPN での IKE ポリシー （44 ページ）を参照してください。

（注） FTD では、リモート アクセス VPN の IKEv2 のみに対応しています。

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 使用可能な VPN ポリシーのリストから、設定を変更するポリシーを選択します。

ステップ 3 [詳細設定（Advanced）] > [IKEポリシー（IKE Policy）] をクリックします。

ステップ 4 [追加（Add）] ボタンをクリックして、利用可能な IKEv2 ポリシーから選択するか、新しい IKEv2 ポリシーを追加して、次の項目を指定します。

- [Name（名前）]：IKEv2 ポリシーの名前。
- [説明（Description）]：IKEv2 ポリシーの任意の説明

- [優先度（Priority）]：このプライオリティ値によって、共通のセキュリティ アソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE ポリシーの順序が決定します。
- [ライフタイム（Lifetime）]：セキュリティ アソシエーション（SA）のライフタイム（秒数）。
- [整合性（Integrity）]：IKEv2 ポリシーで使用されるハッシュ アルゴリズムの整合性アルゴリズム部分です。
- [暗号化（Encryption）]：フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 SA の確立に使用される暗号化アルゴリズムです。
- [PRFハッシュ（PRF Hash）]：IKE ポリシーに使用されるハッシュ アルゴリズムの疑似乱数関数（PRF）部分です。IKEv2 では、これらの要素に異なるアルゴリズムを指定できます。
- [DHグループ（DH Group）]：暗号化に使用する Diffie-Hellman グループです。

ステップ 5 **[保存（Save）]** をクリックします。

関連トピック

リモート アクセス VPN のアクセス インターフェイス オプション

リモート アクセス VPN の [IPsec/IKEv2パラメータ（IPsec/IKEv2 Parameters）] の設定

ステップ 1 **[Devices]** > **[VPN]** > **[Remote Access]**を選択します。

ステップ 2 使用可能な VPN ポリシーのリストから、設定を変更するポリシーを選択します。

ステップ 3 [詳細設定（Advanced）] > [IPsec] > [IPsec/IKEv2パラメータ（IPsec/IKEv2 Parameters）] をクリックします。

ステップ 4 [IKEv2セッション設定（IKEv2 Session Settings）] で次の項目を選択します。

- [ピアに送信されるID（Identity Sent to Peers）]：IKE ネゴシエーションでピアが自身の識別に使用する ID を選択します。
  - [自動（Auto）]：接続タイプごとの IKE ネゴシエーションを決定します。事前共有キー用の IP アドレス、証明書認証のための Cert DN（非対応）。
  - [IPアドレス（IP address）]：ISAKMP 識別情報を交換するホストの IP アドレスを使用します。
  - ホスト名（Hostname）：ISAKMP 識別情報を交換するホストの完全修飾ドメイン名（FQDN）を使用します。この名前は、ホスト名とドメイン名で構成されます。
- [トンネルの切断時の通知を有効にする（Enable Notification on Tunnel Disconnect）]：管理者は、SA で受信された着信パケットがその SA のトラフィック セレクタと一致しない場合のピアへの IKE 通知の送信を有効または無効にすることができます。デフォルトでは、[この通知を送信する（Sending this notification）] は無効になっています。
- [すべてのセッションが終了するまでデバイスの再起動を許可しない（Do not allow device reboot until all sessions are terminated）]：オンにすると、すべてのアクティブなセッションが自主的に終了してからシステムが再起動されます。デフォルトでは、無効になっています。

ステップ 5 [IKEv2セキュリティアソシエーションIKEv（SA）の設定（IKEv2 Security Association (SA) Settings）] で次の項目を選択します。

- [クッキーチャレンジ（Cookie Challenge）]：SA 開始パケットに応答してピア デバイスにクッキー チャレンジを送信するかどうかを選択します。阻止サービス妨害（DoS）攻撃に役立つことがあります。デフォルトでは、使用可能な SA の 50% がネゴシエーション中である場合にクッキー チャレンジを使用します。次のオプションのいずれか 1 つを選択します。
  - [カスタム（Custom）]：[着信クッキーチャレンジのしきい値（Threshold to Challenge Incoming Cookies）] を指定します。これは許可されるネゴシエーション中の SA の総数の割合です。この設定を指定すると、以降の SA ネゴシエーションに対してクッキーチャレンジがトリガーされます。範囲は 0 ～ 100 % です。デフォルト値は 50 % です。
  - [常時（Always）]：ピア デバイスにクッキー チャレンジを常に送信します。
  - [不可（Never）]：ピア デバイスにクッキー チャレンジを送信しません。
-
- [許可されるネゴシエーション中のSAの数（Number of SAs Allowed in Negotiation）]：一時点でのネゴシエーション中 SA の総数を制限します。クッキー チャレンジと共に使用する場合は、有効なクロス チェックが実行されるようにするため、クッキー チャレンジのしきい値をこの制限値よりも低くしてください。デフォルトは 100 % です。
- [許可されるSAの最大数（Maximum number of SAs Allowed）]：許可される IKEv2 接続の数を制限します。

ステップ 6 [IPsec設定（IPsec Settings）] で次の項目を選択します。

- [暗号化の前にフラグメンテーションを有効にする（Enable Fragmentation Before Encryption）]：このオプションは、IP フラグメンテーションをサポートしていない NAT デバイス間をトラフィックが通過できるようにします。このオプションを使用しても、IP フラグメンテーションをサポートしていない NAT デバイスの動作が妨げられることはありません。
- [パスの最大伝送ユニットのエージング（Path Maximum Transmission Unit Aging）]：PMTU（パスの最大伝送ユニット）のエージング（SA（セキュリティ アソシエーション）のリセット PMTU までのインターバル）が可能であるかを確認します。
- [値のリセット間隔（Value Reset Interval）]：SA（セキュリティ アソシエーション）の PMTU 値が元の値にリセットされるまでの時間（分）を入力します。有効範囲は 10 ～ 30 分です。デフォルトは無制限です。

ステップ 7 [NAT設定（NAT Settings）] で次の項目を選択します。

- [キープアライブメッセージトラバーサル（Keepalive Messages Traversal）]：NAT キープアライブ メッセージ トラバーサルを有効にするかどうかを設定します。VPN 接続ハブとスポークとの間にデバイス（中間デバイス）が配置されている場合、キープアライブ メッセージを転送するために NAT トラバーサル キープアライブを使用します。このデバイスでは、IPsec フローで NAT を実行します。このオプションを選択する場合は、セッションがアクティブであることを示すためにスポークと中間デバイス

間でキープアライブ信号が送信される間隔（秒）を設定します。値は10～3600秒となります。デフォルトは20秒です。

- [間隔（Interval）]：NATキープアライブ間隔を10～3600秒に設定します。デフォルトは20秒です。

ステップ8 **[保存（Save）]** をクリックします。

RADIUS ダイナミック認証

Firepower Threat Defenseは、RADIUSサーバを使用して、ダイナミック アクセス コントロール リスト（ACL）またはユーザごとのACL名を使用するVPNリモートアクセスおよびファイアウォール カットスルー プロキシ セッションのユーザ許可を実行できます。ダイナミック認証またはRADIUS認可変更（RADIUS CoA）のダイナミックACLを実装するには、RADIUSサーバをサポートするように設定する必要があります。ユーザが認証を試みる場合、RADIUSサーバによってダウンロード可能ACL、またはACL名がFirepower Threat Defenseに送信されます。特定のサービスへのアクセスはACLによって許可されるか拒否されるかのいずれかです。Firepower Threat Defenseは認証セッションの期限が切れるとACLを削除します。

関連トピック

RADIUS サーバ グループ
インターフェイス オブジェクト：インターフェイスグループとセキュリティ ゾーン
RADIUS ダイナミック認証の設定 （48 ページ）
の RADIUS サーバ属性 Firepower Threat Defense （28 ページ）

RADIUS ダイナミック認証の設定

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。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

始める前に：

- RADIUS サーバで参照されている場合、セキュリティ ゾーンやインターフェイス グループには 1 つのインターフェイスのみ設定できます。
- ダイナミック認証が有効になっている RADIUS サーバでダイナミック認証を機能させるためには、Firepower Threat Defense 6.3 以降が必要です。
- Firepower Threat Defense 6.2.3 以前のバージョンでは、RADIUS サーバでのインターフェイスの選択はサポートされていません。展開中、インターフェイス オプションは無視されます。

表 *3*：手順

	操作内容	詳細
ステップ 1	Firepower Management Center Web インターフェイスにログインします。	
ステップ 2	ダイナミック認証を使用して、RADIUS サーバ オブジェクトを設定します。	RADIUS サーバ グループのオプション

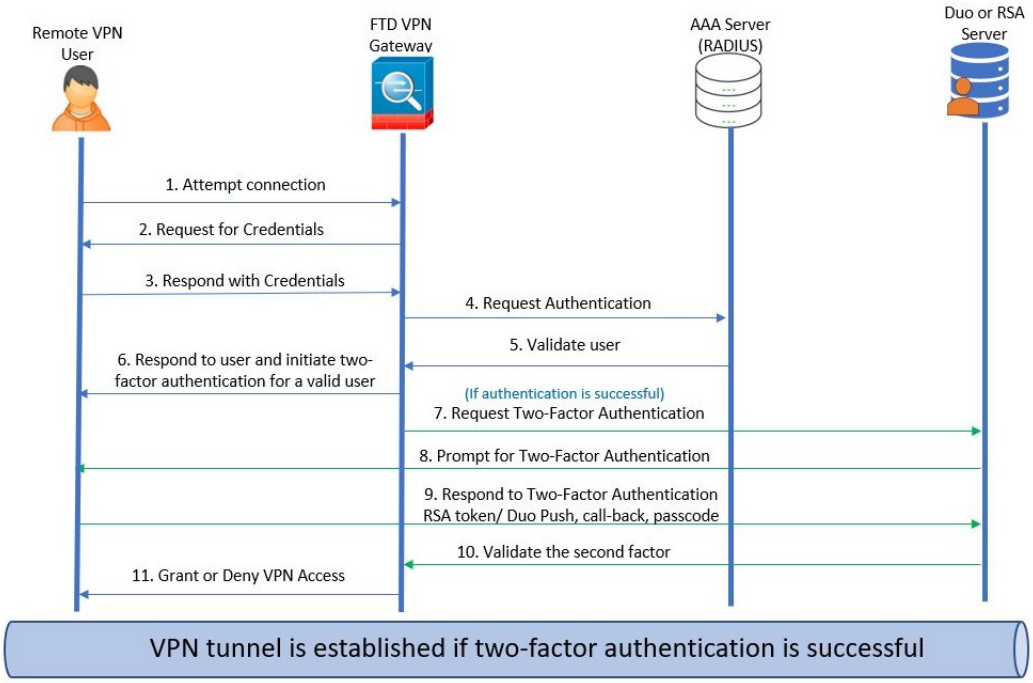
	操作内容	詳細
ステップ 3	認可変更（CoA）が有効になっているインターフェイスを介してISEサーバへのルートを設定し、ルーティングまたは特定のインターフェイスを介して Firepower Threat Defense から RADIUS サーバへの接続を確立します。	RADIUS サーバ グループのオプション ユーザ制御用 ISE/ISE-PIC の設定
ステップ 4	リモートアクセス VPN ポリシーを設定し、ダイナミック認証を使用して作成した RADIUS サーバ グループ オブジェクトを選択します。	新しいリモートアクセス VPN ポリシーの作成 （13 ページ）
ステップ 5	DNS サーバの詳細とドメインルックアップ インターフェイスを [プラットフォーム設定（Platform Settings）] を使用して設定します。	DNS の設定 （18 ページ） DNS サーバ グループ オブジェクト
ステップ 6	VNP ネットワーク経由で DNS サーバに到達可能な場合は、リモート アクセス VPN トンネルを介して DNS トラフィックを許可するためのスプリットトンネルをグループ ポリシーに設定します。	グループ ポリシー オブジェクトの設定
ステップ 7	設定変更を展開します。	設定変更の展開

Two-Factor Authentication

リモート アクセス VPN に対して二要素認証を設定することができます。二要素認証を使用する場合、ユーザはユーザ名とスタティック パスワードに加えて、RSA トークンやパスコードなどの追加項目を指定する必要があります。二要素認証が 2 番目の認証ソースを使用することと異なるのは、1 つの認証ソースで 2 つの要素が設定され、RSA サーバとの関係がプライマリ認証ソースに関連付けられている点です。

Firepower Threat Defense 2 番目の要素のためにモバイルにプッシュされる RSA トークンと Duo パスコードを、二要素認証プロセスの最初の要素としての RADIUS サーバまたは AD サーバとの組み合わせをサポートします。

図 *2:* 二要素認証



RSA 二要素認証の設定

このタスクの概要：

RADIUS サーバまたは AD サーバを RSA サーバの認証エージェントとして設定し、サーバをリモートアクセス VPN のプライマリ認証ソースとして Firepower Management Center で使用することができます。

この方法を使用する場合、ユーザは RADIUS または AD サーバで設定されているユーザ名を使用して認証し、パスワードと 1 回限りの一時的な RSA トークンを連結し、パスワードとトークンをカンマで区切る必要があります（*password,token*）。

この設定では、認証サービスを提供するために（Cisco ISE で供給されるような）個別の RADIUS サーバを使用することが一般的です。2 番目の RADIUS サーバを認証サーバとして設定し、必要に応じてアカウンティング サーバとしても設定します。

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。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

始める前に：

Firepower Threat Defense に RADIUS 二要素認証を設定する前に、次の設定が完了していることを確認します。

RSA サーバ上で以下の操作を実行します。

- RADIUS または Active Directory サーバを認証エージェントとして設定します。
- 設定（*sdconf.rec*）ファイルを生成してダウンロードします。
- トークン プロファイルを作成してトークンをユーザに割り当て、トークンをユーザに配布します。トークンをダウンロードして、リモート アクセス VPN クライアント システムにインストールします。

詳細については、RSA SecureID スイートのドキュメントを参照してください。

ISE サーバ上で以下の操作を実行します。

- RSA サーバで生成した設定（*sdconf.rec*）ファイルをインポートします。
- 外部アイデンティティ ソースとして RSA サーバを追加して、共有秘密を指定します。

表 4: 手順

	操作内容	詳細
ステップ 1	Firepower Management Center Web インターフェイスにログインします。	
ステップ 2	RADIUS サーバ グループを作成します。	RADIUS サーバ グループのオプション
ステップ 3	RADIUS または AD サーバをホストとして指定して、新しい RADIUS サーバ グループ内に RADIUS サーバ オブジェクトを作成します。タイムアウトの時間は 60 秒以上に設定します。	RADIUS サーバ オプション （注） RADIUS または AD サーバは、RSA サーバで認証エージェントとして設定されているサーバと同じである必要があります。 二要素認証の場合は、AnyConnect クライアントプロファイル XML ファイルでもタイムアウトが 60 秒以上に更新されていることを確認してください。
ステップ 4	ウィザードを使用して新しいリモートアクセス VPN ポリシーを設定するか、既存のリモートアクセス VPN ポリシーを編集します。	新しいリモートアクセス VPN ポリシーの作成 （13 ページ）
ステップ 5	認証サーバとして RADIUS を選択し、新しく作成した RADIUS サーバ グループを認証サーバとして選択します。	リモートアクセス VPN の AAA 設定 （24 ページ）
ステップ 7	設定変更を展開します。	設定変更の展開

Duo 二要素認証の設定

このタスクの概要：

Duo RADIUS サーバはプライマリ認証ソースとして設定できます。この方法では、Duo RADIUS 認証プロキシを使用します。（LDAPS 経由での Duo クラウド サービスとの直接接続は使用できません）。

Duo の設定に関する詳細手順については、https://duo.com/docs/cisco-firepower を参照してください。

その後、最初の認証要素として別の RADIUS サーバ（または AD サーバ）を使用し、2 番目の要素として Duo クラウド サービスを使用するため、プロキシ サーバ宛の認証要求を転送するように Duo を設定します。

このアプローチを使用する場合、Duo クラウドまたは web サーバと、関連付けられている RADIUS サーバの両方で設定されたユーザ名を使用してユーザを認証する必要があります。ユーザは、RADIUS サーバに設定されたパスワードと、その後に次のいずれかの Duo コードを入力する必要があります。

- **Duo-passcode**。*my-password*12345 など。
- **push**。たとえば、*my-password*,**push** など。push は、ユーザによるインストールと登録が完了している Duo モバイル アプリに認証をプッシュ送信するように Duo に指示する場合に使用します。
- **sms**。たとえば、*my-password*,**sms** など。**sms** は、ユーザのモバイルデバイスにパスコードの新しいバッチと SMS メッセージを送信するように Duo に指示する場合に使用します。**sms** を使用すると、ユーザの認証試行が失敗します。ユーザは再認証し、2 番目の要素として新しいパスコードを入力する必要があります。

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。 • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex	該当なし	FTD	いずれか（Any）	Admin

始める前に：

Firepower Threat Defense で Duo 認証プロキシを使用する RADIUS 二要素認証を設定する前に、次の設定が完了していることを確認します。

- リモート アクセス VPN ユーザに対して実行中のプライマリ認証（RADIUS または AD）を設定してから、Duo の展開を開始します。
- ネットワーク内の Windows または Linux マシンに Duo プロキシ サービスをインストールして、Duo と Firepower Threat Defense リモート アクセス VPN を統合します。また、この Duo プロキシ サーバは RADIUS サーバとしても機能します。

  次の場所から最新の Duo 認証プロキシをダウンロードしてインストールします。

  - **Windows**：https://dl.duosecurity.com/duoauthproxy-latest.exe
  - **Linux**：https://dl.duosecurity.com/duoauthproxy-latest-src.tgz
  - https://duo.com/docs/checksums#duo-authentication-proxy でチェックサムを確認します。

- Duo 認証ファイル `authproxy.cfg` を設定します。https://duo.com/docs/authproxy_reference ページの指示に従って、認証設定を構成します。

  `authproxy.cfg` 設定ファイルには、RADIUS または ISE サーバの詳細、Firepower Threat Defense デバイス、Duo プロキシ サーバの詳細、統合鍵、秘密鍵、API ホストの詳細を含める必要があります。

- `authproxy.cfg` ファイルに正しい API ホスト情報が含まれていることを確認します。
- [Duoセキュリティ設定（Duo Security Server）] > [Duo管理者パネル（Duo Admin Panel）] > [アプリケーション（Applications）] > [CISCO RADIUS VPN] で、新しくインストールされた Duo プロキシ サーバのセカンダリ認証ファクタなど、その他の必要な設定を指定します。

表 *5:* 手順

	操作内容	詳細
ステップ 1	Firepower Management Center Web インターフェイスにログインします。	
ステップ 2	RADIUS サーバ グループを作成します。	RADIUS サーバ グループのオプション
ステップ 3	RADIUS サーバをホストとして指定して、新しい RADIUS サーバ グループ内に RADIUS サーバ オブジェクトを作成します。タイムアウトの時間は 60 秒以上に設定します。	RADIUS サーバ オプション （注） RADIUS サーバは、RSA サーバで認証エージェントとして設定されているサーバと同じである必要があります。 二要素認証の場合は、AnyConnect クライアントプロファイル XML ファイルでもタイムアウトが 60 秒以上に更新されていることを確認してください。

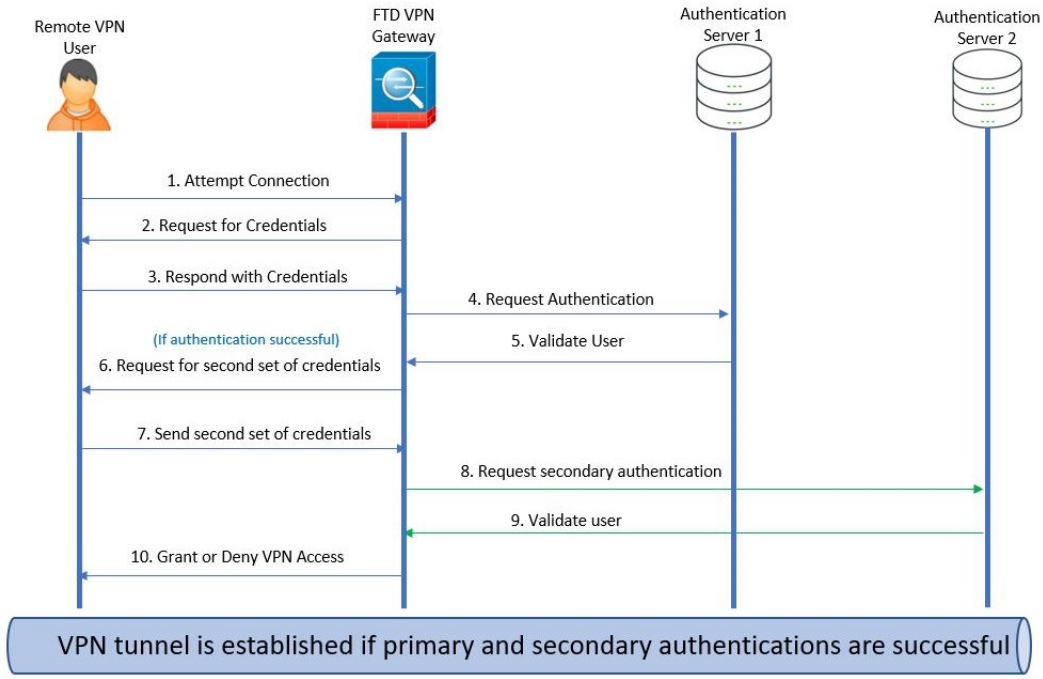
	操作内容	詳細
ステップ 4	ウィザードを使用して新しいリモートアクセス VPN ポリシーを設定するか、既存のリモートアクセス VPN ポリシーを編集します。	新しいリモートアクセス VPN ポリシーの作成（13 ページ）
ステップ 5	認証サーバとして RADIUS を選択し、Duo プロキシ サーバを指定して作成した RADIUS サーバ グループを認証サーバとして選択します。	リモートアクセス VPN の AAA 設定（24 ページ）
ステップ 7	設定変更を展開します。	設定変更の展開

Secondary Authentication

Firepower Threat Defense のセカンダリ認証または二重認証は、2 つの異なる認証サーバを使用して、リモート アクセス VPN 接続にさらにもう 1 つのセキュリティのレイヤを追加します。セカンダリ認証が有効になっている場合、AnyConnect VPN のユーザは VPN ゲートウェイにログインするために 2 組のクレデンシャルを提供する必要があります。

Firepower Threat Defense リモート アクセス VPN は、AAA のみのセカンダリ認証と、クライアント証明書認証方式および AAA 認証方式をサポートします。

図 *3:* リモート アクセス *VPN* セカンダリ認証または二重認証



関連トピック

リモートアクセス VPN のセカンダリ認証の設定 （56 ページ）

リモートアクセス VPN のセカンダリ認証の設定

クライアント証明書と認証サーバの両方を使用するようにリモート アクセス VPN 認証が設定されている場合、VPN クライアント認証はクライアント証明書の検証と AAA サーバの両方を使用して実行されます。

始める前に

- 2 つの認証（AAA）サーバの設定：プライマリおよびセカンダリ認証サーバ、必要な ID 証明書。認証サーバには、RADIUS サーバ、AD または LDAP レルムを使用できます。
- リモート アクセス VPN 設定が機能するように AAA サーバに Firepower Threat Defense デバイスからアクセスできることを確認します。AAA サーバへの接続を確実にするために、ルーティングを設定します（[デバイス（Devices）]>[デバイス管理（Device Management）]>[デバイスの編集（Edit Device）]>[ルーティング（Routing）]）。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）]>[VPN]>[リモート アクセス（Remote Access）] を選択します。

ステップ 2 リスト内の既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。または、[追加（Add）] をクリックして新しいリモート アクセス VPN ポリシーを作成します。

ステップ 3 新しいリモート アクセス VPN ポリシーには、接続プロファイルの設定時に認証を設定します。既存の設定の場合は、クライアント プロファイルが含まれている接続プロファイルを選択し、[編集（Edit）] をクリックします。

ステップ 4 [AAA] タブで、[認証方式（Authentication Method）]、[AAA]、[クライアント証明書とAAA（Client Certificate & AAA）] を選択します。

- [認証方式（Authentication Method）] の選択に応じて、次のようになります。

  [クライアント証明書とAAA（Client Certificate & AAA）]：クライアント証明書と AAA サーバの両方を使用して認証されます。

  - [AAA]：[認証サーバ（Authentication Server）] に [RADIUS] を選択した場合、デフォルトで許可サーバは同じ値になります。ドロップダウン リストから [アカウンティング サーバ（Accounting Server）] を選択します。認証サーバ ドロップダウン リストから [AD] と [LDAP] を選択した場合は常に、[認証サーバ（Authorization Server）] と [アカウンティング サーバ（Accounting Server）] をそれぞれ手動で選択する必要があります。
  - どの認証方式を選択する場合にも、[ユーザが承認データベースに存在するときにのみ接続を許可（Allow connection only if user exists in authorization database）] を選択または選択解除します。

- [セカンダリ認証を使用（Use secondary authentication）]：VPN セッションのセキュリティを強化するため、プライマリ認証の他にセカンダリ認証を設定します。セカンダリ認証は、[AAA のみ（AAA only）] と [クライアント証明書と AAA（Client Certificate & AAA）] の認証方式にのみ適用されます。

  セカンダリ認証はオプションの機能であり、2 つのセットのユーザ名とパスワードを AnyConnect ログイン画面に入力するにはVPNユーザが必要です。認証サーバまたはクライアント証明書からセカンダリ ユーザ名を事前入力するように設定することもできます。リモート アクセス VPN 認証は、プライマリとセカンダリの両方の認証が成功した場合にのみ許可されます。いずれの認証サーバに到達できない場合、1 つの認証が失敗すると、VPN 認証が拒否されます。

  セカンダリ認証の設定前に、2つ目のユーザ名とパスワードのセカンダリ認証のサーバ グループ（AAA サーバ）を設定する必要があります。たとえば、プライマリ認証サーバをLDAPまたはActive Directoryレルムに、セカンダリ認証を RADIUS サーバに設定できます。

  （注） デフォルトでは、セカンダリ認証は必要ありません。

  [認証サーバ（Authentication Server）]：VPN ユーザのセカンダリ ユーザ名とパスワードを提供するセカンダリ認証サーバ。

  [セカンダリ認証のユーザ名（Username for secondary authentication）] で次の項目を選択します。

  - [プロンプト（Prompt）]：VPN ゲートウェイへのログイン中にユーザ名とパスワードを入力するようユーザに要求します。
  - [プライマリ認証ユーザ名を使用（Use primary authentication username）]：プライマリとセカンダリの両方の認証にプライマリ認証サーバからユーザ名が取得されます。パスワードは 2 つ入力する必要があります。
  - [クライアント証明書からのユーザ名をマップ（Map username from client certificate）]：クライアント証明書からセカンダリ ユーザ名が事前に入力されます。

- クライアント証明書のユーザ名を含む [固有のフィールドをマップ（Map specific field）] オプションを選択する場合。[プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、デフォルト値の [CN（共通名）（CN (Common Name)）] と [組織ユニット（OU）（OU (Organisational Unit)）] がそれぞれ表示されます。[DN（識別名）全体をユーザ名として使用（Use entire DN (Distinguished Name) as username）] オプションを選択した場合はユーザ ID が自動的に取得されます。

  プライマリとセカンダリのフィールドのマッピングの詳細については、「**認証方式**」の説明を参照してください。

- [ユーザ ログイン ウィンドウに証明書からユーザ名を事前に入力（Prefill username from certificate on user login window）]：ユーザが AnyConnect VPN クライアント経由で接続したときにクライアント証明書からセカンダリ ユーザ名を事前に入力します。

  - [ログイン ウィンドウでユーザ名を非表示にする（Hide username in login window）]：セカンダリ ユーザ名はクライアント証明書から事前に入力されますがユーザには表示されず、ユーザが事前に入力されたユーザ名を変更しないようにします。

- [VPN セッションのセカンダリ ユーザ名を使用（Use secondary username for VPN session）]：VPN セッション中のユーザ アクティビティのレポートにセカンダリ ユーザ名を使用します。

詳細については、「リモートアクセス VPN の AAA 設定 （24 ページ）」を参照してください。

関連トピック

接続プロファイルの設定 （21 ページ）

リモート アクセス VPN の AAA の設定のカスタマイズ

ここでは、リモート アクセス VPN の AAA プリファレンスのカスタマイズについて説明します。詳細については、「リモートアクセス VPN の AAA 設定 （24 ページ）」を参照してください。

クライアント証明書を使用した VPN ユーザの認証

ウィザードを使用するか、またはポリシーを後で編集することによって新しいリモートアクセス VPN ポリシーを作成するときに、クライアント証明書を使用してリモート アクセス VPN 認証を設定できます。

始める前に

VPN ゲートウェイとして機能する各 Firepower Threat Defense デバイスにアイデンティティ証明書を取得するために使用する証明書登録オブジェクトを設定します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リスト内の既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。または、[追加（Add）] をクリックして新しいリモート アクセス VPN ポリシーを作成します。

ステップ 3 新しいリモート アクセス VPN ポリシーには、接続プロファイルの設定時に認証を設定します。既存の設定の場合は、クライアント プロファイルが含まれている接続プロファイルを選択し、[編集（Edit）] をクリックします。

ステップ 4 [AAA] タブで、[認証方式（Authentication Method）]、[クライアント証明書のみ（Client Certificate Only）] を選択します。

この認証方式では、ユーザはクライアント証明書を使用して認証されます。VPN クライアント エンドポイントで設定する必要があります。デフォルトでは、ユーザ名はクライアント証明書フィールド CN および OU からそれぞれ派生します。クライアント証明書の他のフィールドにユーザ名が指定されている場合は、[プライマリ（Primary）] と [セカンダリ（Secondary）] フィールドを使用して適切なフィールドをマップします。

クライアント証明書のユーザ名を含む [固有のフィールドをマップ（Map specific field）] オプションを選択する場合。[プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、デフォルト値の [CN（共通名）（CN (Common Name)）] と [組織ユニット（OU）（OU (Organisational Unit)）] がそれぞれ表示されます。[DN全体をユーザ名として使用（Use entire DN as username）] オプションを選択した場合、ユーザ ID が自動的に取得されます。識別名（DN）は、個々のフィールドから構成される一意の識別子であり、ユーザを接続プロファイルと照合するときに識別子として使用できます。DN ルールは、拡張証明書認証に使用されます。

- [固有のフィールドをマップ（Map specific field）] オプションに関連する [プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、次の共通の値が含まれています。
  - C（国）
  - CN（一般名）
  - DNQ（DN 修飾子
  - EA（電子メール アドレス）
  - GENQ（世代識別子）
  - GN（姓名の名）
  - I（イニシャル）
  - L（地名）
  - N（名前）
  - O（組織）
  - OU（組織ユニット）
  - SER（シリアル番号）

- SN（姓名の姓）
- SP（都道府県）
- T（タイトル）
- UID（ユーザ ID）
- UPN（ユーザ プリンシパル名）

- どの認証方式を選択する場合にも、[ユーザが承認データベースに存在するときにのみ接続を許可（Allow connection only if user exists in authorization database）] を選択または選択解除します。

詳細については、「リモートアクセス VPN の AAA 設定 （24 ページ）」を参照してください。

関連トピック

接続プロファイルの設定 （21 ページ）
証明書の登録オブジェクトの追加

クライアント証明書と AAA サーバ経由でのリモート アクセス VPN のログインの設定

クライアント証明書と認証サーバの両方を使用するようにリモート アクセス VPN 認証が設定されている場合、VPN クライアント認証はクライアント証明書の検証と AAA サーバの両方を使用して実行されます。

始める前に

- VPN ゲートウェイとして機能する各 Firepower Threat Defense デバイスのアイデンティティ証明書を取得するために使用される証明書登録オブジェクトを設定します。
- RADIUS サーバ グループ オブジェクトと、このリモート アクセス VPN ポリシーで使用されている AD または LDAP レルムを設定します。
- リモート アクセス VPN 設定が機能するように AAA サーバに Firepower Threat Defense デバイスからアクセスできることを確認します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リスト内の既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。または、[追加（Add）] をクリックして新しいリモート アクセス VPN ポリシーを作成します。

ステップ 3 新しいリモート アクセス VPN ポリシーには、接続プロファイルの設定時に認証を設定します。既存の設定の場合は、クライアント プロファイルが含まれている接続プロファイルを選択し、[編集（Edit）] をクリックします。

ステップ 4 [AAA] タブで、[認証方式（Authentication Method）]、[クライアント証明書と AAA（Client Certificate & AAA）] を選択します。

- [認証方式（Authentication Method）] の選択に応じて、次のようになります。

  [クライアント認証と AAA（Client Certificate & AAA）]：両方のタイプの認証が実行されます。

  - [AAA]：[認証サーバ（Authentication Server）] に [RADIUS] を選択した場合、デフォルトで許可サーバは同じ値になります。ドロップダウン リストから [アカウンティング サーバ（Accounting Server）] を選択します。認証サーバ ドロップダウン リストから [AD] と [LDAP] を選択した場合は常に、[認証サーバ（Authorization Server）] と [アカウンティング サーバ（Accounting Server）] をそれぞれ手動で選択する必要があります。

  - [クライアント証明書（Client Certificate）]：ユーザはクライアント証明書を使用して認証されます。クライアント証明書は、VPN クライアント エンドポイントで設定する必要があります。デフォルトでは、ユーザ名はクライアント証明書フィールド CN および OU からそれぞれ派生します。クライアント証明書の他のフィールドにユーザ名が指定されている場合は、[プライマリ（Primary）] と [セカンダリ（Secondary）] フィールドを使用して適切なフィールドをマップします。

    クライアント証明書のユーザ名を含む [固有のフィールドをマップ（Map specific field）] オプションを選択する場合。[プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、デフォルト値の [CN（共通名）（CN (Common Name)）] と [組織ユニット（OU）（OU (Organisational Unit)）] がそれぞれ表示されます。[DN全体をユーザ名として使用（Use entire DN as username）] オプションを選択した場合、ユーザ ID が自動的に取得されます。識別名（DN）は、個々のフィールドから構成される一意の識別子であり、ユーザを接続プロファイルと照合するときに識別子として使用できます。DN ルールは、拡張証明書認証に使用されます。

    [固有のフィールドをマップ（Map specific field）] オプションに関連する [プライマリ（Primary）] フィールドと [セカンダリ（Secondary）] フィールドには、次の共通の値が含まれています。

    - C（国）
    - CN（一般名）
    - DNQ（DN 修飾子
    - EA（電子メール アドレス）
    - GENQ（世代識別子）
    - GN（姓名の名）
    - I（イニシャル）
    - L（地名）
    - N（名前）
    - O（組織）
    - OU（組織ユニット）
    - SER（シリアル番号）

- SN（姓名の姓）
- SP（都道府県）
- T（タイトル）
- UID（ユーザ ID）
- UPN（ユーザ プリンシパル名）

- どの認証方式を選択する場合にも、[ユーザが承認データベースに存在するときにのみ接続を許可（Allow connection only if user exists in authorization database）] を選択または選択解除します。

詳細については、「リモートアクセス VPN の AAA 設定 （24 ページ）」を参照してください。

関連トピック

接続プロファイルの設定 （21 ページ）
証明書の登録オブジェクトの追加

VPN セッションでのパスワード変更の管理

パスワードの管理では、リモート アクセス VPN 管理者がリモート アクセス VPN ユーザのパスワード期限切れの通知を設定できます。パスワード管理は、 AAA のみとクライアント証明書と AAA の認証設定の AAA 設定で使用できます。詳細については、リモートアクセス VPN の AAA 設定 （24 ページ）を参照してください。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リストから既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 AAA の設定が含まれている接続プロファイルを選択し、[編集（Edit）] をクリックします。

ステップ 4 [AAA] > [詳細設定（Advanced Settings）] > [パスワード管理（Password Management）] を選択します。

ステップ 5 [パスワード管理の有効化（Enable Password Management）] を選択し、次のいずれかを選択します。

- [Notify User（ユーザ通知）] : パスワードの有効期限が切れる前にユーザに通知します。ボックスに日数を指定します。
- [パスワードの有効期限の日にユーザに通知（Notify user on the day password expires）] : パスワードが期限切れになる当日にユーザに通知します。

ステップ 6 **[保存（Save）]** をクリックします。

関連トピック

接続プロファイルの設定 （21 ページ）

承認を得るための LDAP または Active Directory の設定

認証に LDAP サーバまたは Active Directory（AD）サーバを使用してリモート アクセス VPN を設定する場合は、FlexConfig オブジェクトを使用して属性マップを設定する必要があります。これは、Firepower Management Center の Web インターフェイス上では属性マップが直接サポートされていないためです。

始める前に

LDAP または AD のレルム オブジェクトが作成されていることを確認します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 認証サーバとして、LDAP または AD レルム オブジェクトを含むリモート アクセス VPN ポリシーを作成します。または、既存のリモート アクセス VPN の設定を編集し、LDAP または AD レルムを認証サーバとして選択します。

ステップ 3 [オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [FlexConfig] > [FlexConfig オブジェクト（FlexConfig Object）] を選択します。

ステップ 4 FlexConfig ポリシーを作成し、次の 2 つの FlexConfig オブジェクトを作成して追加セクションに割り当てます。

FlexConfig ポリシーの設定を参照してください。

a) [展開タイプ（Deployment type）] を [1 回（Once）]、[タイプ（Type）] を [後ろに付加（Append）] にして、LDAP 属性マップの FlexConfig オブジェクトを作成します。

オブジェクトの本文には、次を入力します。

```
lda attribute-map <LDAP_Map_for_VPN_Access>
          map-name  memberOf Group-Policy
          map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=cisco,DC=com
LabAdminAccessGroupPolicy
         map-value memberOf CN=cisco-Eng,CN=Users,OU=stbu,DC=cisco,DC=com VPNAccessGroupPolicy
```

b) [展開タイプ（Deployment type）] を [毎回（Everytime）]、[タイプ（Type）] を [後ろに付加（Append）] にして、LDAP 属性マップを LDAP AAA サーバに関連付ける FlexConfig オブジェクト属性を作成します。

（注） このマッピングは、LDAP 属性マップの割り当てが Firepower Management Center によって拒否されるため、その割り当てを元に戻すために必要です。

オブジェクトの本文領域に次を入力します。

```
aaa-server <LDAP/AD_Realm_name> host <AD Server IP>
          ldap-attribute-map <LDAP_Map_for_VPN_Access>
          exit
```

リモート アクセス VPN ポリシーの設定に追加した接続プロファイルの AAA サーバの設定に使用した LDAP レルム名と同じ *AAA* サーバを使用します。

詳細については、FlexConfig テキスト オブジェクトの設定を参照してください。

a) **[保存（Save）]** をクリックします。

FlexConfig ポリシー内での FlexConfig オブジェクトの順序が、LDAP 属性マップの FlexConfig オブジェクトの後に AAA サーバ オブジェクトが続いていることを確認します。

これは、LDAP 属性マップを設定し、それを Firepower Threat Defense デバイス上の LDAP サーバ設定と関連付けます。

関連トピック

FlexConfig オブジェクトの設定

RADIUS サーバへのアカウンティング レコードの送信

リモート アクセス VPN のアカウンティング レコードは、ユーザがアクセスしたサービスやユーザが使用したネットワーク リソースの量を VPN 管理者が追跡するのに役立ちます。アカウンティング情報には、ユーザセッションの開始時刻と停止時刻、ユーザ名、セッションごとのデバイスを通過したバイト数、使用されたサービス、および各セッションの時間が含まれています。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。

アカウンティングは、単独で使用するか、認証および認可とともに使用することができます。AAA アカウンティングをアクティブ化すると、ネットワーク アクセス サーバは設定されたアカウンティング サーバにユーザ アクティビティをレポートします。RADIUS サーバはアカウンティング サーバとして設定できます。そのため、ユーザ アクティビティ情報のすべてが Firepower Management Center から RADIUS サーバに送信されます。

（注） リモート アクセス VPN AAA の設定では、認証、許可、およびアカウンティング用に同じ RADIUS サーバまたは個別の RADIUS サーバを使用できます。

始める前に

認証要求またはアカウンティング レコードが送信される RADIUS サーバで RADIUS グループ オブジェクトを設定します。RADIUS サーバ グループのオプションを参照してください。

RADIUS サーバが Firepower Threat Defense デバイスから到達可能であることを確認します。[デバイス（Devices）] > [デバイス管理（Device Management）] > [デバイスの編集（Edit Device）] > [ルーティング（Routing）] で Firepower Management Center のルーティングを設定し、RADIUS へのサーバへの接続を確保します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リスト内の既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。または、新しいリモート アクセス VPN ポリシーを作成します。

ステップ 3 AAA の設定が含まれている接続プロファイルを選択し、[編集（Edit）] > [AAA] をクリックします。

ステップ 4 **アカウンティング サーバ**として RADIUS サーバを選択します。

ステップ 5 **[保存（Save）]** をクリックします。

関連トピック

接続プロファイルの設定 （21 ページ）
リモートアクセス VPN の AAA 設定 （24 ページ）

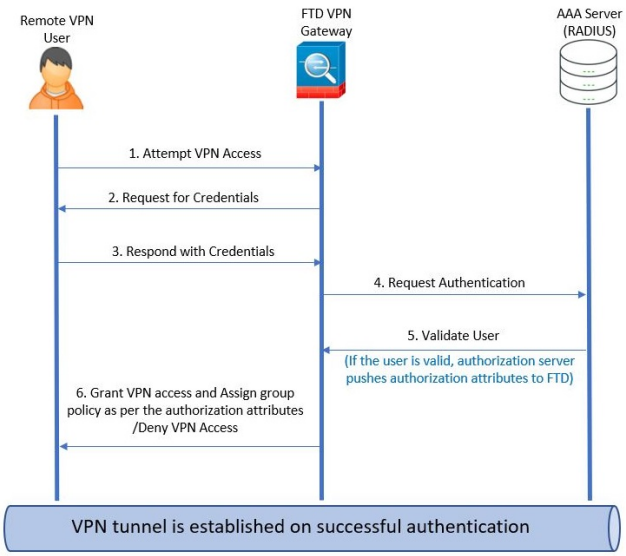
認証サーバへのグループ ポリシーの選択の委任

ユーザに適用されるグループ ポリシーは VPN トンネルが確立される際に決定されます。ウィザードを使用してリモートアクセス VPN ポリシーを作成するときに接続プロファイルのグループポリシーを選択するか、または後で接続プロファイルの接続ポリシーを更新することができます。ただし、グループポリシーを割り当てるように AAA（RADIUS）サーバを設定するか、または現在の接続プロファイルから取得されます。Firepower Threat Defense デバイスが設定プロファイルに設定されている属性と競合する外部 AAA サーバから属性を受信した場合は、AAA サーバからの属性が常に優先されます。

IETF RADIUS サーバ属性 25 を送信してユーザ/ユーザ グループの許可プロファイルを設定し、対応するグループ ポリシー名にマップするように、ISE または RADIUS サーバを構成します。ユーザまたはユーザ グループに特定のグループ ポリシーを設定すると、ダウンロード可能な ACL をプッシュし、バナーを設定し、VLAN を制限し、セッションに SGT を適用する高度なオプションを設定できます。これらの属性は、VPN 接続が確立した時点でそのグループに含まれているすべてのユーザに適用されます。

詳細については、『Cisco Identity Services Engine Administrator Guide』の「Configure Standard Authorization Policies」」の項およびの RADIUS サーバ属性 Firepower Threat Defense （28 ページ）を参照してください。

図 *4 : AAA* サーバによるリモート アクセス *VPN* グループ ポリシーの選択



関連トピック

グループ ポリシー オブジェクトの設定
接続プロファイルの設定 （21 ページ）

許可サーバによるグループポリシーまたはその他の属性の選択のオーバーライド

リモートアクセス VPN ユーザが VPN に接続すると、接続プロファイル内に設定されているグループ ポリシーとその他の属性がそのユーザに割り当てられます。ただし、リモート アクセス VPN システムの管理者は、ユーザまたはユーザ グループの許可プロファイルを設定するように ISE または RADIUS サーバを設定することによって、グループ ポリシーとその他の属性の選択を認証サーバに委任できます。ユーザが認証されると、これらの特定の承認属性が Firepower Threat Defense デバイスにプッシュされます。

始める前に

許可サーバとして RADIUS を使用したリモート アクセス VPN ポリシーが設定されていることを確認します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リストから既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 まだ設定されていない場合は、許可サーバとして RADIUS または ISE を選択します。

ステップ 4 [詳細（Advanced）] > [グループ ポリシー（Group Policies）] を選択し、必要なグループ ポリシーを追加します。グループ ポリシー オブジェクトの詳細については、グループ ポリシー オブジェクトの設定を参照してください。

1 つのグループ ポリシーのみを 1 つの接続プロファイルにマップすることができますが、1 つのリモート アクセス VPN ポリシーには複数のグループ ポリシーを作成できます。これらのグループ ポリシーは、ISE または RADIUS サーバで参照でき、許可サーバの許可属性を割り当てることによって接続プロファイル内に設定されているグループ ポリシーをオーバーライドするように設定できます。

ステップ 5 ターゲットの Firepower Threat Defense デバイス上に設定を展開します。

ステップ 6 許可サーバで、IP アドレスとダウンロード可能な ACL の RADIUS 属性を持つ許可プロファイルを作成します。

リモート アクセスで選択した許可サーバにグループ ポリシーを設定すると、そのグループ ポリシーは、ユーザが認証された後にリモート アクセス VPN ユーザの接続プロファイルに設定されているグループ ポリシーをオーバーライドします。

関連トピック

グループ ポリシー オブジェクトの設定

ユーザ グループへの VPN アクセスの拒否

VPN を使用可能な認証済みのユーザまたはユーザ グループが不要な場合は、VPN アクセスを拒否するグループ ポリシーを設定できます。リモート アクセス VPN ポリシー内にグループ ポリシーを作成し、許可を行うため、ISE または RADIUS サーバの設定でそれを参照します。

始める前に

リモートアクセス ポリシー ウィザードを使用してリモートアクセス VPN が設定されており、リモート アクセス VPN ポリシーに認証の設定が行われていることを確認します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リストから既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 [詳細（Advanced）] > [グループ ポリシー（Group Policies）] をクリックします。

ステップ 4 グループ ポリシーを選択して [編集（Edit）] アイコンをクリックするか、または新しいグループ ポリシーを追加します。

ステップ 5 [詳細（Advanced）] > [セッション設定（Session Settings）] を選択し、[ユーザごとの同時ログイン（Simultaneous Login Per User）] を 0（ゼロ）に設定します。
これにより、ユーザまたはユーザ グループは VPN への接続を完全に停止します。

ステップ 6 [保存（Save）] をクリックしてグループ ポリシーを保存した後、リモート アクセス VPN 設定を保存します。

ステップ 7 IETF RADIUS サーバ 属性 25 を送信し、対応するグループ ポリシー名にマップするようにユーザ/ユーザ グループの許可プロファイルを設定して、ISE または RADIUS サーバ サーバを設定します。

ステップ 8 リモート アクセス VPN ポリシーでは、ISE または RADIUS サーバを承認サーバとして構成できます。

ステップ 9 リモート アクセス VPN ポリシーを保存および展開します。

関連トピック

接続プロファイルの設定 （21 ページ）

ユーザ グループに対する接続プロファイルの選択の制限

1 つの接続プロファイルをユーザまたはユーザ グループに適用する場合、接続プロファイルを無効にすることで、AnyConnect VPN クライアントを使用して接続するときに選択するユーザのグループ エイリアスまたは URL のリストが表示されないようにすることができます。

たとえば、モバイルユーザ、会社支給のラップトップのユーザ、個人のラップトップのユーザなど、異なる VPN ユーザ グループに組織が特定の設定を使用する場合は、それらの各ユーザ グループに固有の接続プロファイルを設定し、ユーザが VPN に接続したときに適切に接続プロファイルを適用することができます。

デフォルトでは、AnyConnect クライアントは Firepower Management Center に設定されており、Firepower Threat Defense に展開されている接続プロファイル（接続プロファイル名別、エイリアス別、またはエイリアス URL 別）のリストを表示します。カスタム接続プロファイルが設定されていない場合、AnyConnect は *DefaultWEBVPNGroup* 接続プロファイルを表示します。次の手順を使用して、1 つの接続プロファイルをユーザ グループに適用します。

始める前に

- Firepower Management Center の Web インターフェイスで、リモート アクセス VPN ポリシー ウィザードを使用し、[認証方式（Authentication Method）] を [クライアント証明書のみ（Client Certificate Only）] または [クライアント証明書と AAA（Client Certificate + AAA）] に設定してリモート アクセス VPN を設定します。証明書からユーザ名のフィールドを選択します。
- 認証のための ISE または RADIUSの サーバを設定し、グループ ポリシーを認証サーバに関連付けます。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リストから既存のリモート アクセス ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 [アクセス インターフェイス（Access Interfaces）] タブを選択し、[ログイン時にユーザによる接続プロファイルの選択を許可（Allow users to select the connection profile while logging in）] を無効にします。

ステップ 4 [詳細（Advanced）]> [証明書マップ（Certificate Maps）] をクリックします。

ステップ 5 [設定したルールを使用して証明書を接続プロファイルと照合する（Use the configured rules to match a certificate to a Connection Profile）] をオンにします。

ステップ 6 [証明書マップ名（Certificate Map Name）] を選択するか、または [追加（Add）] アイコンをクリックして証明書ルールを追加します。

ステップ 7 [接続プロファイル（Connection Profile）] を選択し、[OK] をクリックします。
この設定では、ユーザが AnyConnect クライアントから接続すると、そのユーザにはマップされた接続プロファイルが提供され、VPN を使用するように認証されます。

関連トピック

グループ ポリシー オブジェクトの設定
接続プロファイルの設定 （21 ページ）

リモート アクセス VPN クライアントでの AnyConnect クライアント プロファイルの更新

AnyConnect クライアント プロファイルは、AnyConnect の一部として VPN クライアント システムに展開される管理者定義のエンドユーザ要件および認証ポリシーを含む XML ファイルで

す。これでエンドユーザが事前設定されたネットワーク プロファイルを使用できるようになります。

独立した設定ツールである GUI ベースの AnyConnect プロファイル エディタを使用して AnyConnect クライアント プロファイルを作成します。スタンドアロン プロファイル エディタを使用して、新しい AnyConnect プロファイルを作成したり、既存の AnyConnect プロファイルを変更したりできます。プロファイル エディタはシスコのソフトウェア ダウンロード センターからダウンロードできます。

詳細については、『Cisco AnyConnect Secure Mobility Client Administrator Guide』の該当するリリースの「AnyConnect プロファイル エディタ」の章を参照してください。

始める前に

- リモート アクセス ポリシー ウィザードを使用してリモート アクセス VPN が設定されており、設定が Firepower Threat Defense デバイスに展開されていることを確認します。新しいリモート アクセス VPN ポリシーの作成 （13 ページ）を参照してください。
- Firepower Management Center の Web インターフェイスで、[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [AnyConnect ファイル（AnyConnect File）] に移動し、新しいAnyConnect クライアント イメージ を追加します。

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 リストから既存のリモート アクセス VPN ポリシーを選択し、対応する [編集（Edit）] アイコンをクリックします。

ステップ 3 クライアント プロファイルに含まれている編集すべき接続プロファイルを選択して [編集（Edit）] をクリックします。

ステップ 4 [グループ ポリシーの編集（Edit Group Policy）] > [AnyConnect] > [プロファイル（Profiles）] をクリックします。

ステップ 5 リストからクライアント プロファイルの XML ファイルを選択するか、または [追加（Add）] アイコンをクリックして新しいクライアント プロファイルを追加します。

ステップ 6 グループ ポリシーと接続プロファイルを保存し、その後にリモート アクセス VPN ポリシーを保存します。

ステップ 7 変更を展開します。
クライアント プロファイルに加えた変更は、リモート アクセス VPN ゲートウェイに接続したときに VPN クライアント上で更新されます。

関連トピック

グループ ポリシー オブジェクトの設定

リモート アクセス VPN の例

ユーザあたりの AnyConnect 帯域幅を制限する方法

ここでは、ユーザが Cisco AnyConnect VPN クライアントを使用して Firepower Threat Defense リモートアクセス VPN ゲートウェイに接続する場合に VPN ユーザに消費される最大帯域幅を制限する手順について説明します。Firepower Threat Defense で Quality of Service（QoS）ポリシーを使用して最大帯域幅を制限し、単一のユーザやグループまたは複数のユーザがリソース全体を引き継ぐことがないようにすることができます。この設定では、重要なトラフィックに優先順位を付け、帯域幅の占有を防止し、ネットワークを管理できます。トラフィックが最大レートを超えると、Firepower Threat Defenseは超過した分のトラフィックをドロップします。

	操作内容	詳細
ステップ 1	レルムを作成および設定します。	Active Directory レルムの作成および設定 （70 ページ）。
ステップ 2	新しく作成したレルムで利用可能なユーザまたはグループの QoS ポリシーおよび QoS ルールを作成します。	QoS ポリシーとルールの作成 （71 ページ）
ステップ 3	リモートアクセス VPN ポリシーを設定し、ユーザ認証用に新しく作成したレルムを選択します。	リモート アクセス VPN ポリシーの作成または更新 （72 ページ）
ステップ 4	リモートアクセス VPN ポリシーを展開します。	設定変更の展開

Active Directory レルムの作成および設定

ここでは、レルムを作成し、アクティビティをモニタする VPN ユーザおよびユーザ グループを指定する手順について説明します。

ステップ 1 Firepower Management Center web インターフェイスで、[システム（System）] > [統合（Integration）] > [レルム（Realms）] を選択します。

ステップ 2 [新規レルム（New Realm）] をクリックして、レルムの詳細を指定し、[OK] をクリックします。

ステップ 3 次のタブに必要な詳細を入力し、[保存（Save）] をクリックします。

- [ディレクトリ（Directory）] : 1 つのレルムに複数のディレクトリを指定できます。この場合、ユーザ制御用のユーザ クレデンシャルとグループ クレデンシャルを照合するために、そのレルムの [ディレ

クトリ（Directory）] タブ ページにリストされている順序で、各ドメイン コントローラがクエリされます。

レルム ディレクトリの設定を参照してください。

- [レルム設定（Realm Configuration）]：レルムの作成中に入力されたレルム設定を更新できます。
- [ユーザダッシュボード（User Download）]：ユーザとグループは、Firepower Management Center のダウンロードに含めることも、ダウンロードから除外することもできます。

レルムが作成され、[レルム（Realms）] タブに追加されます。

ステップ 4 [ステート（State）] を右にスライドし、レルムをユーザ コントロールで使用できるように有効にします。レルムの管理を参照してください

ステップ 5 ダウンロード アイコンをクリックし、ユーザおよびユーザ グループを Firepower Management Center にダウンロードします。ユーザとグループのダウンロードを参照してください

ステップ 6 **[保存（Save）]** をクリックします。

関連トピック

レルムの作成

QoS ポリシーとルールの作成

管理対象デバイスに展開する QoS ポリシーによりレート制限が決まります。ユーザまたはユーザ グループが消費できる VPN 帯域幅を制限するようにレルムを選択すると、QoS ポリシーを作成できます。各 QoS ポリシーは、複数のデバイスを対象にすることができます。各デバイスで同時に展開可能な QoS ポリシーは 1 つです。

。

ステップ 1 Firepower Management Center web インターフェイスで、[デバイス（Devices）] > [QoS] > [新しいポリシー（New Policy）] を選択します。

ステップ 2 [名前（Name）] を入力し、必要に応じて [説明（Description）] を入力します。

ステップ 3 （オプション）QoS ポリシーを展開する [使用可能なデバイス（Available Devices）] を選択し、[ポリシーに追加（Add to Policy）] をクリックするか、[選択されたデバイス（Selected Devices）] にドラッグ アンド ドロップします。

（注） リモート アクセス VPN ポリシーを展開する同じデバイスを選択します。ポリシーを展開する前に、デバイスを割り当てる必要があります。

ステップ 4 QoS ポリシーの [ルール（Rules）] タブで、[ルールの追加（Add Rule）] をクリックします。

ステップ 5 [名前（Name）]を入力します。

ステップ 6 ルール コンポーネントを設定します。

- [有効（Enabled）]：ルールを有効にするかどうかを指定します。

- [QoSの適用（Apply QoS On）]：レート制限するインターフェイス（[宛先インターフェイスオブジェクトのインターフェイス（Interfaces in Destination Interface Objects）] または [送信元インターフェイスオブジェクトのインターフェイス（Interfaces in Source Interface Objects）]）を選択します。選択するインターフェイスは、入力されたインターフェイス制約（任意ではなく）と一致する必要があります。
- [インターフェイスごとのトラフィック制限（Traffic Limit Per Interface）]：ダウンロード制限とアップロード制限を Mbits/sec 単位で入力します。[無制限（Unlimited）] のデフォルト値にすると、一致するトラフィックはその方向でレート制限されません。
- [ユーザ（Users）]：[ユーザ（Users）] で、新しい作成したレルムおよびユーザを選択し、VPN トラフィックを制限します。追加する条件に対応する他のタブをクリックします。[QoSの適用（Apply QoS On）] の選択内容に対応する、送信元インターフェイスまたは宛先インターフェイスの条件を設定する必要があります。
- [コメント（Comments）]：[コメント（Comments）] をクリックし、コメントを追加し、[OK] をクリックします。

ステップ 7 ルールを保存します。

ポリシー エディタで、ルールの位置を設定します。クリックしてドラッグするか、または右クリック メニューを使用してカットアンドペーストを実行します。ルールには 1 から番号が付けられます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールは、そのトラフィックを処理するルールです。適切なルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。

ステップ 8 [保存（Save）] をクリックして、ポリシーを保存します。

関連トピック

QoS ポリシーの作成
QoS ポリシーによるレートの制限

リモート アクセス VPN ポリシーの作成または更新

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 ウィザードを使用して新しいリモート アクセス VPN ポリシーを作成します。[認証サーバ（Authentication Server）] で新しく作成したレルムをするか、既存の VPN ポリシーを編集して、次の手順を実行します。

a) VPN ユーザに割り当てる接続プロファイルを選択し、[編集（Edit）] ボタンをクリックします。
b) [AAA] タブで、[認証方式（Authentication Method）]：[AAA] または [証明書と AAA（Certificate & AAA）] を選択します。
c) [認証サーバ（Authentication Server）] として必要なレルムを選択します。
d) 必要に応じて他の接続プロファイル オプションを更新し、接続プロファイルを保存します。

ステップ 3 リモート アクセス VPN ポリシーに必要な設定を完了し、[保存（Save）] をクリックします。

関連トピック

新しいリモート アクセス VPN 接続の設定 （12 ページ）
接続プロファイルの設定 （21 ページ）

ユーザ ID ベースのアクセス コントロール ルールに VPN アイデンティティを使用する方法

	操作内容	詳細
ステップ 1	レルムを作成および設定します。	Active Directory レルムの作成および設定 （70 ページ）。
ステップ 2	アイデンティティ ポリシーを作成し、アイデンティティ ルールを追加します。	アイデンティティ ポリシーおよびアイデンティティ ルールの作成 （74 ページ）。
ステップ 3：	アクセス コントロール ポリシーとアイデンティティ ポリシーを関連付けます。	アイデンティティポリシーとアクセスコントロール ポリシーの関連付け （75 ページ）
ステップ 4	リモートアクセス VPN ポリシーを設定し、ユーザ認証用に新しく作成したレルムを選択します。	リモート アクセス VPN ポリシーの作成または更新 （72 ページ）
ステップ 5	リモートアクセス VPN ポリシーを展開します。	設定変更の展開

Active Directory レルムの作成および設定

ここでは、レルムを作成し、アクティビティをモニタする VPN ユーザおよびユーザ グループを指定する手順について説明します。

ステップ 1 Firepower Management Center web インターフェイスで、[システム（System）] > [統合（Integration）] > [レルム（Realms）] を選択します。

ステップ 2 [新規レルム（New Realm）] をクリックして、レルムの詳細を指定し、[OK] をクリックします。

ステップ 3 次のタブに必要な詳細を入力し、[保存（Save）] をクリックします。

- [ディレクトリ（Directory）] : 1 つのレルムに複数のディレクトリを指定できます。この場合、ユーザ制御用のユーザ クレデンシャルとグループ クレデンシャルを照合するために、そのレルムの [ディレクトリ（Directory）] タブ ページにリストされている順序で、各ドメイン コントローラがクエリされます。

レルム ディレクトリの設定を参照してください。

- [レルム設定（Realm Configuration）]：レルムの作成中に入力されたレルム設定を更新できます。
- [ユーザダッシュボード（User Download）]：ユーザとグループは、Firepower Management Center のダウンロードに含めることも、ダウンロードから除外することもできます。

レルムが作成され、[レルム（Realms）] タブに追加されます。

ステップ 4 [ステート（State）] を右にスライドし、レルムをユーザ コントロールで使用できるように有効にします。レルムの管理を参照してください

ステップ 5 ダウンロード アイコンをクリックし、ユーザおよびユーザ グループを Firepower Management Center にダウンロードします。ユーザとグループのダウンロードを参照してください

ステップ 6 **[保存（Save）]** をクリックします。

関連トピック

レルムの作成

アイデンティティ ポリシーおよびアイデンティティ ルールの作成

アイデンティティ ポリシーには、トラフィックに関連付けられているレルムと認証方式に基づいて、ユーザ認証を実行するアイデンティティ ルールが含まれます。アイデンティティ ルールでは、トラフィックのセットを、レルムおよび認証方式（パッシブ認証、アクティブ認証、または認証なし）と関連付けます。アイデンティティ ルールで呼び出す前に、使用するレルムおよび認証方式を完全に設定しておく必要があります。

ステップ 1 Firepower Management Center web インターフェイスで、[ポリシー（Policies）] > [アクセスコントロール（Access Control）] > [アイデンティティ（Identity）] を選択し、[新しいポリシー（New Policy）] をクリックします。

ステップ 2 [名前（Name）] および [説明（Description）] を入力し、[保存（Save）] をクリックします。

ステップ 3 ポリシーにルールを追加するには、[ルールの追加（Add Rule）] をクリックし、[名前（Name）] を入力します。

ステップ 4 ルールを**有効**にするかどうかを指定します。

ステップ 5 既存のカテゴリにルールを追加するには、ルールを [挿入（Insert）] する場所を指定します。新しいカテゴリを追加するには、[カテゴリの追加（Add Category）] をクリックします。

ステップ 6 リストからルール [アクション（Action）] を選択し、リモート アクセス VPN で設定されているインターフェイスを送信元インターフェイスとして選択します。

ステップ 7 [レルムと設定（Realms & Settings）] タブをクリックし、[レルム（Realms）] リストからアイデンティティ ルール用に作成された新しいレルムを選択します。リモート アクセス VPN ポリシーでユーザ認証用に選択したものと同じレルムを選択していることを確認してください。

ステップ 8 選択したレルムでユーザの優先設定を構成し、その他の必要なルール オプションを選択します。

ステップ 9 [追加（Add）] をクリックして、アイデンティティ ポリシーを保存します。

関連トピック

アイデンティティ ポリシーの作成および管理

アイデンティティ ポリシーとアクセス コントロール ポリシーの関連付け

アイデンティティ ポリシーを、リモート アクセス VPN ポリシーが展開される Firepower Threat Defense デバイスに展開されているアクセス コントロール ポリシーに関連付ける必要があります。

ステップ 1 Firepower Management Center web インターフェイスで、[ポリシー（Policies）] > [アクセスコントロール（Access Control）] を選択し、[アクセスコントロール（Access Control）] をクリックします。

ステップ 2 必要なアクセス コントロール ポリシーを選択し、[編集（Edit）] アイコンをクリックします。

ステップ 3 アクセス コントロール ポリシー エディタで、[詳細（Advanced）] タブをクリックします。

ステップ 4 [アイデンティティポリシー設定（Identity Policy Settings）] 領域で編集アイコン（）をクリックします。

代わりに表示アイコン（）が表示される場合、設定は先祖ポリシーから継承され、設定を変更する権限がありません。 設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 5 ドロップダウン リストからアイデンティティ ポリシーを選択します。

編集アイコンをクリックすると、アイデンティティ ポリシーを編集できます。

ステップ 6 [OK] をクリックします。

ステップ 7 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

関連トピック

アイデンティティ ポリシーの作成および管理

リモート アクセス VPN ポリシーの作成または更新

ステップ 1 Firepower Management Center の Web インターフェイスで、[デバイス（Devices）] > [VPN] > [リモート アクセス（Remote Access）] を選択します。

ステップ 2 ウィザードを使用して新しいリモート アクセス VPN ポリシーを作成します。[認証サーバ（Authentication Server）] で新しく作成したレルムをするか、既存の VPN ポリシーを編集して、次の手順を実行します。

a) VPN ユーザに割り当てる接続プロファイルを選択し、[編集（Edit）] ボタンをクリックします。

b) [AAA] タブで、[認証方式（Authentication Method）] : [AAA] または [証明書と AAA（Certificate & AAA）] を選択します。

c) [認証サーバ（Authentication Server）] として必要なレルムを選択します。

d) 必要に応じて他の接続プロファイル オプションを更新し、接続プロファイルを保存します。

ステップ 3 リモート アクセス VPN ポリシーに必要な設定を完了し、[保存（Save）] をクリックします。

関連トピック

新しいリモート アクセス VPN 接続の設定 （12 ページ）
接続プロファイルの設定 （21 ページ）