



Firepower Threat Defense リモート アクセス VPN

- [Firepower Threat Defense リモート アクセス VPN について \(1 ページ\)](#)
- [Firepower Threat Defense リモート アクセス VPN の機能 \(4 ページ\)](#)
- [Firepower Threat Defense リモート アクセス VPN に関するガイドラインと制限事項 \(5 ページ\)](#)
- [Firepower Threat Defense のリモート アクセス VPN の管理 \(7 ページ\)](#)
- [Firepower Threat Defense のリモート アクセス VPN ポリシーの編集 \(9 ページ\)](#)

Firepower Threat Defense リモート アクセス VPN について

Firepower Threat Defense は、リモート アクセス SSL と IPsec IKEv2 VPN をサポートするセキュアなゲートウェイ機能を提供します。完全なトンネルクライアントである AnyConnect Secure Mobility Client[`AnyConnectSecureMobilityClient`] は、セキュリティゲートウェイへのセキュアな SSL および IKEv2 IPsec 接続をリモート ユーザに提供します。これはエンドポイントデバイスでサポートされている唯一のクライアントで、Firepower Threat Defense デバイスへのリモート VPN 接続が可能です。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 IKEv2 IPsec 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、この 2 つのタイプのリモート 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。

AnyConnect クライアント プロファイルエディタ

AnyConnect クライアント プロファイルは、クライアントが操作と外観を設定するために使用する XML ファイルに保存された設定パラメータのグループです。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、Windows 用の 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。

AnyConnect Secure Mobility Client[AnyConnectSecureMobilityClient]展開

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 v4.x](#)』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 IKEv2 IPsec 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。

ログイン後、セキュア ゲートウェイは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]運用

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。次に、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。

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 証明書ベースの認証](#)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一切提供されません。

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



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

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

VPN 接続を介して一度認証されると、リモート ユーザは VPN の ID を引き受けます。この VPN ID は、Firepower Threat Defense セキュア ゲートウェイ上のアイデンティティ ポリシーによって、そのリモート ユーザに属するネットワーク トラフィックを認識してフィルタリングするために使用されます。

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

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](#)を参照してください。

Firepower Threat Defense リモート アクセス VPN の機能

- 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。
- IPv4 および IPv6。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 Firepower Threat Defense 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。

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 または LDAP/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。
- 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 RA VPN イベント。
- Firepower Threat Defense 統合 CLI により利用可能なトンネル統計。

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

AnyConnect

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、AnyConnect クライアントの展開に使用されるだけで、エンティティ自体としてはサポートされていません。

Firepower Threat Defense 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。
- すべてのポストチャ派生機能 (HostScan、エンドポイント ポストチャ アセスメント、および ISE) と、クライアント ポストチャに基づくダイナミック アクセス ポリシー。
- AnyConnect のカスタマイズとローカリゼーションのサポート。Firepower Threat Defense 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、Firepower Threat Defense 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 Firepower Threat Defense 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

- セカンダリ認証または二重認証
- SAML 2.0 を使用する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
- RADIUS CoA
- VPN ロード バランシングはサポートされません。

設定 (Configuration)

- 新しい RA VPN ポリシーは、ウィザードの指示に従うことによるのみ追加できます。新しいポリシーを作成するにはウィザード全体を通して処理する必要があり、完了する前に取り消すと、ポリシーが保存されません。
- 2人のユーザが同時に RA 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 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。
- 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一切提供されません。

リモート アクセス VPN ポリシーを追加する前の前提条件

- ウィザードを使用してリモート アクセス VPN を設定している間は、VPN セッションを認証するために使用されるインライン AAA サーバを作成できません。したがって、リモート アクセス VPN 構成ウィザードを使用する前に事前設定する必要があります。LDAP/AD AAA サーバの作成の詳細については、[レلمの作成](#) を参照してください。RADIUS AAA サーバグループの作成については、[RADIUS サーバグループ](#) を参照してください。
- 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 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 デバイスで使わ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。

認証、認可、アカウントिंग

- 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。RADIUS 認証と LDAP/AD 認証がサポートされています。
- LDAP/AD の認可とアカウントングは、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 設定では、RADIUS サーバグループのみを承認サーバまたはアカウント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、FQDN またはホスト名を持つ CA サーバを解決できません。IP アドレスが使用されている場合にのみ解決できます。

DNS 設定 CLI コマンドで FlexConfig オブジェクトを使用して FlexConfig ポリシーを作成することにより、DNS を設定できます。詳細については、[FlexConfig ポリシーの設定](#)および[FlexConfig オブジェクトの設定](#)を参照してください。FlexConfig オブジェクトで使用する DNS コマンドの詳細については、次を参照してください。<http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/basic.html#wp1080248>

Firepower Threat Defense のリモート アクセス VPN の管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
エクスポート制御機能が有効になっている、スマート ライセンス アカウントに関連付けられている AnyConnect ライセンスのいずれか： <ul style="list-style-type: none"> • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex 	該当なし	Firepower Threat Defense	任意 (Any)	管理者 (Administrator)

手順

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

リストに表示されるポリシーは VPN 構成ウィザードを使用して作成されていて、多くの場合すでに編集されています。失効ステータスは、ターゲット デバイスにリモート アクセス VPN

ポリシーの旧バージョンがあることを示します。ポリシー設定を更新するには、最新のリモート アクセス VPN ポリシーを導入します。

ステップ 2 次のアクションのいずれかを選択します。

-  **追加**：基本的なポリシー設定を順を追って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。

(注) 新しい RA VPN ポリシーは、ウィザードの指示に従うことによつてのみ追加できます。新しいポリシーを作成するにはウィザード全体を通して処理する必要があります。完了する前に取り消すと、ポリシーが保存されません。

RA VPN ウィザードを実行する前に、次の構成タスクが必要です。

- ヘッドエンドとして機能する各 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する必要があります。
- RADIUS サーバグループオブジェクトと、この RA VPN ポリシーで使用されている AD または LDAP レルムを設定する必要があります。

(注) リモートアクセス VPN ソリューションが動作するには、AAA 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する必要があります。設定とトラブルシューティングの詳細については、[AAA サーバ接続 \(20 ページ\)](#) を参照してください。

ウィザードが完了すると、このポリシー一覧ページに戻ります。基本的な RA VPN ポリシー設定を完了するために、VPN ユーザのアクセス制御を設定し、NAT 免除を有効にします (必要な場合)。次に、構成を展開し、VPN 接続を確立します。

-  **編集**：既存のリモートアクセス VPN ポリシーを変更します。編集アイコンまたは VPN ポリシーの行をクリックして、編集するポリシーを開きます。詳細については、[Firepower Threat Defense のリモート アクセス VPN ポリシーの編集 \(9 ページ\)](#) を参照してください。

(注) 2 人のユーザが同時に RA 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。

-  **削除**：リモートアクセス VPN 構成を削除します。

次のタスク

設定変更を展開します。[設定変更の展開](#)を参照してください。



(注) 一部の VPN 設定は、展開時にのみ検証されます。展開が成功したことを確認してください。

Firepower Threat Defense のリモート アクセス VPN ポリシーの編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
エクスポート制御機能が有効になっている、スマート ライセンス アカウントに関連付けられている AnyConnect ライセンスのいずれか： <ul style="list-style-type: none"> • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex 	該当なし	Firepower Threat Defense	任意 (Any)	管理者 (Administrator)

手順

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

リストに表示されるポリシーは VPN 構成ウィザードを使用して作成されていて、多くの場合すでに編集されています。失効ステータスは、ターゲット デバイスにリモート アクセス VPN ポリシーの旧バージョンがあることを示します。ポリシー設定を更新するには、最新のリモート アクセス VPN ポリシーを導入します。

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。

リモート アクセス ポリシーの主な構成要素が表示されます。

ステップ 3 [接続プロファイル (Connection Profile)] を追加または編集するには、[Firepower Threat Defense リモート アクセス VPN 接続プロファイルの追加と編集 \(10 ページ\)](#) を参照してください。

ステップ 4 [アクセスインターフェイス (Access Interfaces)] を追加または編集するには、[Firepower Threat Defense 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 \(23 ページ\)](#) を参照してください。

ステップ 5 [詳細設定 (Advanced)] タブを選択し、リモート アクセス VPN 設定を次のように完了します。

- a) [AnyConnect クライアント イメージ (AnyConnect Client Images)] を設定するには、[Cisco AnyConnect セキュア モビリティ クライアント イメージについて Firepower Threat Defense \(26 ページ\)](#) を参照してください。

- b) [アドレス割り当てポリシー (Address Assignment Policy)] を設定するには、[Firepower Threat Defense リモート アクセス VPN アドレス割り当てポリシーについて \(28 ページ\)](#) を参照してください。
- c) この接続プロファイルの [証明書マップ (Certificate Maps)] を設定するには、[証明書マップの設定 \(29 ページ\)](#) を参照してください。
- d) ナビゲーション ウィンドウから [グループ ポリシー (Group Policies)] を選択すると、この接続プロファイルを使ってリモートユーザに割り当てることのできるグループポリシーをさらに追加できます。これらは、プロファイル作成時に指定されたデフォルトグループポリシーに追加されます。[グループ ポリシーの設定 \(30 ページ\)](#) を参照してください。
- e) [IPsec] オプションを編集するには、[Firepower Threat Defense IPsec 設定の編集 \(31 ページ\)](#) を参照してください。

Firepower Threat Defense リモート アクセス VPN 接続プロファイルの追加と編集

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。



(注) デフォルト接続プロファイルを削除することはできません。

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
エクスポート制御機能が有効になっている、スマート ライセンス アカウントに関連付けられている AnyConnect ライセンスのいずれか： <ul style="list-style-type: none"> • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex 	該当なし	Firepower Threat Defense	任意 (Any)	管理者 (Administrator)

手順

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

リストに表示されるポリシーは VPN 構成ウィザードを使用して作成されていて、多くの場合すでに編集されています。失効ステータスは、ターゲット デバイスにリモート アクセス VPN ポリシーの旧バージョンがあることを示します。ポリシー設定を更新するには、最新のリモート アクセス VPN ポリシーを導入します。

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。

リモート アクセス ポリシーの主な構成要素が表示されます。

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。詳細については、次を参照してください。 [Firepower Threat Defense リモート アクセス VPN 接続プロファイル オプション \(11 ページ\)](#)

関連トピック

[Firepower Threat Defense リモート アクセス VPN 接続プロファイル オプション \(11 ページ\)](#)

[Firepower Threat Defense リモート アクセス VPN 接続プロファイル](#)

[Firepower Threat Defense 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 \(23 ページ\)](#)

[Firepower Threat Defense リモート アクセス VPN の \[IPsec/IKEv2 パラメータ \(IPsec/IKEv2 Parameters\) \] ページ \(37 ページ\)](#)

[エイリアスについて \(22 ページ\)](#)

[クライアントアドレスの割り当てについて \(12 ページ\)](#)

Firepower Threat Defense リモート アクセス VPN 接続プロファイル オプション

[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、[接続プロファイル (Connection Profile)] タブでリストされている接続プロファイルを選択して編集します。

フィールド

[接続プロファイル (Connection Profile)] ページには、リモート アクセス VPN ポリシー下で作成されたプロファイルが一覧表示されます。この表には、クライアントのアドレス割り当て、グループポリシー、および AAA オプションに関する情報が一覧表示されます。

接続プロファイルを追加するには、[追加 (Add)] アイコンを選択し、[接続プロファイルの追加 (Add Connection Profile)] ウィンドウで次を指定します。

- [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。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。接続プロファイルの詳細については、[を参照してください](#)。
[Firepower Threat Defense リモート アクセス VPN 接続プロファイルの追加と編集 \(10 ページ\)](#)
- [グループポリシー (Group Policy)]: VPN 接続の確立時にクライアントに適用されるユーザ指向の属性の集合です。ユーザ グループの共通属性は、グループ ポリシーによって設定されます。グループ ポリシーの詳細については、[グループ ポリシーの設定 \(30 ページ\)](#) を参照してください。



(注) 新しいグループ ポリシーを追加 (+) することも、既存のポリシーを編集 (✎) することもできます。

関連トピック

[Firepower Threat Defense リモート アクセス VPN 接続プロファイル](#)

[Firepower Threat Defense リモート アクセス VPN 接続プロファイルの追加と編集 \(10 ページ\)](#)

[Firepower Threat Defense のリモート アクセス VPN ポリシーの編集 \(9 ページ\)](#)

[グループ ポリシーの設定 \(30 ページ\)](#)

[リモート アクセス VPN の AAA の設定 \(14 ページ\)](#)

[クライアントアドレスの割り当てについて \(12 ページ\)](#)

[エイリアスについて \(22 ページ\)](#)

クライアントアドレスの割り当てについて

クライアントアドレスの割り当て

リモート アクセス VPN ユーザ用の IP アドレスを提供する手段です。

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ることができます。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。

[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 にすでに作成されているプールから 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。

- [アドレスプール (Address Pools)] : 選択したプールから名前と IP アドレス範囲を指定します。リストからプールを選択するには、[追加 (Add)] アイコンを選択します。選択したアドレスプールを編集するには、[編集 (Edit)] アイコンを選択します。アドレスプールを削除するには、その行で [削除 (Delete)] アイコンを選択します。



(注) 複数の Firepower Threat Defense デバイス間でリモート アクセス VPN の設定を共有する場合は、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。

新しい IPv4 アドレスまたは 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。

- [DHCP サーバ (DHCP Servers)] : 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。

[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。



(注) DHCP サーバアドレスは、IPv4 アドレスでのみ設定可能です。

関連トピック

[エイリアスについて](#) (22 ページ)

[リモート アクセス VPN の AAA の設定](#) (14 ページ)

[Firepower Threat Defense リモート アクセス VPN 接続プロファイル オプション](#) (11 ページ)

[Firepower Threat Defense IPsec 設定の編集](#) (31 ページ)

[Firepower Threat Defense リモート アクセス VPN アドレス割り当てポリシーについて](#) (28 ページ)

リモート アクセス VPN の AAA の設定

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（アカウントティング）を確認できます。AAA サーバの例としては、RADIUS、LDAP/AD、TACACS+、Kerberos 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トティング 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。



(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。DNS 設定 CLI コマンドで FlexConfig オブジェクトを使用して FlexConfig ポリシーを作成することにより、DNS を設定します。詳細については、[FlexConfig ポリシーの設定](#)および[FlexConfig オブジェクトの設定](#)を参照してください。

- [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、ユーザの識別を行う方法です。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)] を [RADIUS] として選択した場合、デフォルトで、承認サーバは同じ値になります。ドロップダウンリストから [アカウントティング サーバ (Accounting Server)] を選択します。[認証サーバ (Authentication Server)] ドロップダウンリストから [AD] および [LDAP] を選択する場合は、手動でそれぞれ [承認サーバ (Authorization Server)] と [アカウントティング サーバ (Accounting Server)] を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)] : 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)] : 両方のタイプの認証が行われます。[AAAのみ (AAA Only)] および [クライアント証明書のみ (Client Certificate Only)] の説明を参照してください。

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。認証だけで使用することも、認可およびアカウント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されている LDAP または AD レルムまたは RADIUS サーバ グループを入力または選択します。

- [承認サーバ (Authorization Server)] : 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。

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 の認可の仕組みについて詳しくは、後述の「**権限および属性のポリシー実施の概要**」を参照してください。

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、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必要があります。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。

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) 取得された 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。

- [アカウントティングサーバ (Accounting Server)] : 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 オブジェクトを入力または選択します。

アカウントリングは、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 アカウントリ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。アカウントリング情報には、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じたバイト数、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。アカウントリングは、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。

- [ユーザ名からレルムを削除 (Strip Realm from username)] : AAA サーバにユーザ名を渡す前に、ユーザ名からレルムを削除するかどうか。たとえば、このオプションを選択して、*domainusername* 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)] : AAA サーバにユーザ名を渡す前に、ユーザ名からグループを削除するかどうか。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。

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すると、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。

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。

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。

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、認証前にユーザー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。Firepower Threat Defense デバイスに接続するすべてのユーザーは、最初にこのグループに所属します。このグループでは、AAA サーバから返されるユーザー属性、またはユーザーに割り当てられたグループポリシーにはない属性が定義されています。



- (注) Firepower Threat Defense デバイスは、ASA とは異なり、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、ユーザー属性または 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最終的にユーザーセッションに使用されます。

RADIUS 承認

前述のとおり、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 接続にユーザー承認属性（ユーザー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。

次のリンクには、ASA 用にサポートされているすべての RADIUS 承認属性が一覧表示されています。これは、リモート アクセス VPN 承認用の Firepower Threat Defense デバイスにも適用する必要があります。 <http://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/aaa-radius.html#ID-2113-000003a>



- (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。一般的に使用される RADIUS サーバで RADIUS 承認を構成するには、このリンクを参照してください。

https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/ref_extserver.html#24640

Firepower Threat Defense デバイスでサポートされている RADIUS 属性

次に、Firepower Threat Defense デバイスから RADIUS サーバに送信されるアップストリーム属性番号を示します。

- 146：トンネルグループ名または接続プロファイル名。
- 150：クライアントタイプ（適用可能な値：2 = AnyConnect クライアント SSL VPN、6 = AnyConnect クライアント IPsec VPN（IKEv2））。
- 151：セッションタイプ（適用可能な値：1 = AnyConnect クライアント SSL VPN、2 = AnyConnect クライアント IPsec VPN（IKEv2））。

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。上記 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。

Firepower Threat Defense デバイスで正式にサポートされているダウンストリーム RADIUS 属性番号は、次のものだけです。

- [グループ ポリシー (Group-Policy)] (属性番号=25) : リモート アクセス VPN セッション用のグループ ポリシーを設定します。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 :

- [アクセス時間 (Access-hours)] (属性番号 = 1)
- [バナー (Banner)] (属性番号 = 15、36)
- [IP アドレス プール (IP Address Pools)] (属性番号 = 217)

IP アドレス プール名は RADIUS サーバ上で構成されており、RADIUS 承認時に使用するデバイスに同じ名前前の IP アドレス プールを構成し、展開する必要があります。IP アドレス プールを使用するには、リモート アクセス VPN ポリシーで接続プロファイルを作成し、その中に IP アドレス プールを設定して、IP アドレス プールを Firepower Threat Defense デバイスに展開できるようにします。IP アドレス プールを接続プロファイルに関連付けることなくデバイスに展開する方法はありません。



(注) ASA とは異なり、IP アドレス プールはグループ ポリシーで構成することはできず、Firepower Threat Defense デバイスの接続プロファイルでのみ構成できます。

- [同時ログイン (Simultaneous-logins)] (属性番号 = 2)
- [VLAN] (属性番号 = 140)
- [ダウンロード可能な ACL (Downloadable ACLs)] : Cisco-AV-Pair 構成でサポートされません。ダウンロード可能な ACL の Cisco-AV-Pair 構成の詳細については、リンクを参照してください。 https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/ref_extserver.html#50902

ACL コンテンツは、承認中に RADIUS サーバからもダウンロードされ、デバイス上で事前設定する必要はありません。

- [フィルタ ACL (Filter ACLs)] (属性番号 = 86、87)



- (注) 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。フィルタ ACL を使用するには、リモート アクセス VPN 設定でグループ ポリシーを設定し、[VPN フィルタ (VPN Filter)] フィールドでフィルタ ACL を使用して、フィルタ ACL をデバイスに展開できるようにします。実際にはグループポリシーを使用しない可能性があっても、フィルタ ACL を展開するように設定する必要があります。グループポリシーに関連付けることなく、デバイスにフィルタ ACL を直接展開することはできません。

AAA サーバ接続

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。これらのアクティビティに対して 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)])。

- ユーザ識別処理の場合、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 認証の場合、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で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。ルーティングの決定を確認するには、**show route management-only** および **show route** コマンドを使用します。

- 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。また、何らかの理由で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は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。



(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で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。ルーティングの決定を確認するには、**show route management-only** および **show route** コマンドを使用します。



- (注) FQDN またはホスト名を使用して AAA サーバ名、名前付き URL、および CA サーバを使用するには、各デバイスで DNS を設定する必要があります。DNS を設定しない場合、システムは単に IP アドレスを設定して使用します。DNS 設定 CLI コマンドで FlexConfig オブジェクトを使用して FlexConfig ポリシーを作成することにより、DNS を設定できます。詳細については、[FlexConfig ポリシーの設定](#) および [FlexConfig オブジェクトの設定](#) を参照してください。FlexConfig オブジェクトで使用する DNS コマンドの詳細については、次を参照してください。 <http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/basic.html#wp1080248>

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** および **traceroute system** : 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** および **traceroute destination** : 診断インターフェイスおよびデータ 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** および **test aaa-server authorization** : AAA サーバで認証および承認をテストします。
- **clear aaa-server statistics groupname** または **clear aaa-server statistics protocol protocol** : グループまたはプロトコルごとに AAA サーバの統計情報をクリアします。
- **aaa-server** 失敗した AAA サーバをアクティブ化するには **groupname active host hostname**、または AAA サーバを不合格にするには **aaa-server groupname fail host hostname**。
- デバッグ コマンド : **debug ldap level**、**debug aaa authentication**、**debug aaa authorization**、および **debug aaa accounting**。

エイリアスについて

エイリアス

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。



(注) エイリアス URL とエイリアス名は、リモート アクセス VPN ポリシーのすべての接続プロファイルで一意である必要があります。

[エイリアス名 (Alias Name)] と [エイリアス URL (Alias URL)] を追加するには、個別のペインで [追加 (Add)] アイコンを選択し、[エイリアス名 (Alias Name)] および [エイリアス URL (Alias URL)] をそれぞれ指定します。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。エイリアス URL を追加するには、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。

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。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)] を選択します。[保存 (Save)] をクリックして、変更内容を保存します。

Firepower Threat Defense 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

アクセス インターフェイス

[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、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す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。アクセス インターフェイスの追加の詳細については、[アクセス インターフェイスの追加 \(24 ページ\)](#)を参照してください。

アクセス インターフェイスを編集するには、その行の [編集 (Edit)] アイコンを選択します。アクセス インターフェイスを削除するには、その行の [削除 (Delete)] アイコンを選択します。

アクセス設定

- [ユーザがログインする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 will 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。このオプションは、**IPsec-IKEv2 VPN** で選択する必要があります。

[SSL 設定 (SSL Settings)] では、次の情報を使用します。

- [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)] : SSL グローバル アイデンティティ証明書を指定します。ドロップダウン リストからオプションを選択します。インターフェイス固有のアイデンティティ証明書が提供されていない場合、**SSL グローバル アイデンティティ証明書**がすべての関連インターフェイスに使用されます。

[IPsec-IKEv2 設定 (IPsec-IKEv2 Settings)] では、次の情報を使用します。

- [IKEv2 アイデンティティ証明書 (IKEv2 Identity Certificate)] : IKEv2 アイデンティティ証明書を指定します。

関連トピック

[Firepower Threat Defense リモート アクセス VPN の \[IPsec/IKEv2 パラメータ \(IPsec/IKEv2 Parameters\)\] ページ \(37 ページ\)](#)

[SSL 設定について](#)

[アクセスインターフェイスの追加 \(24 ページ\)](#)

[エイリアスについて \(22 ページ\)](#)

アクセスインターフェイスの追加

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
エクスポート制御機能が有効になっている、スマートライセンスアカウントに関連付けられている AnyConnect ライセンスのいずれか： <ul style="list-style-type: none"> • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex 	該当なし	Firepower Threat Defense	任意 (Any)	管理者 (Administrator)

手順

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

リストに表示されるポリシーは VPN 構成ウィザードを使用して作成されていて、多くの場合すでに編集されています。失効ステータスは、ターゲット デバイスにリモート アクセス VPN ポリシーの旧バージョンがあることを示します。ポリシー設定を更新するには、最新のリモート アクセス VPN ポリシーを導入します。

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。

リモート アクセス ポリシーの主な構成要素が表示されます。

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 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。ドロップダウンリストから値を選択します。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。

アクセス インターフェイスに **プロトコル** オブジェクトを関連付けます。

b) [IKEv2 の有効化 (Enable 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。

c) [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。

ステップ 5 [Datagram Transport Layer Security の有効化 (Enable Datagram Transport Layer Security)] を選択します。

これを選択すると、インターフェイスで Datagram Transport Layer Security が有効になり、AnyConnect VPN クライアントは 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。

ステップ 6 [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)] を選択します。

a) 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、**SSL グローバル アイデンティティ証明書** がデフォルトで使用されます。

ステップ7 [OK] をクリックして変更を保存します。

リモート アクセス VPN の詳細オプション

Cisco AnyConnect セキュア モビリティ クライアント イメージについて Firepower Threat Defense

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リビジョンを検査し、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します。

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。

AnyConnect クライアント イメージ ファイルをダウンロードするには、<https://software.cisco.com/download/navigator.html?mdfid=283000185> をご覧ください。

関連トピック

[Firepower Management Center への Cisco AnyConnect Mobility クライアント イメージの追加 \(27 ページ\)](#)

[Firepower Threat Defense リモート アクセス VPN 接続プロファイル](#)

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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
エクスポート制御機能が有効になっている、スマート ライセンス アカウントに関連付けられている AnyConnect ライセンスのいずれか： <ul style="list-style-type: none"> • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex 	該当なし	Firepower Threat Defense	任意 (Any)	管理者 (Administrator)

手順

- ステップ 1 [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。
- 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。

または、[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、[Firepower Threat Defense 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について Firepower Threat Defense \(26 ページ\)](#) を参照してください。

特定のオペレーティング システムで追加のクライアント イメージが利用可能な場合に、特定のクライアント イメージを表示するには、[並べ替えボタンを表示 (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。

関連トピック

[Cisco AnyConnect セキュア モビリティ クライアント イメージについて Firepower Threat Defense \(26 ページ\)](#)

[Firepower Threat Defense リモート アクセス VPN 接続プロファイル](#)

Firepower Threat Defense リモート アクセス VPN アドレス割り当てポリシーについて

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 ポリシーを使用して、リモート アクセス VPN クライアントへの IP アドレスを見つけることができます。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

[クライアントアドレスの割り当てについて](#) (12 ページ)

[リモート アクセス VPN の AAA の設定](#) (14 ページ)

[Firepower Threat Defense リモート アクセス VPN 接続プロファイル](#)

証明書マップの設定

証明書から接続プロファイルへのマップは、セキュアゲートウェイでの証明書認証に使用されます。

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。ルール、または証明書マップは、[Firepower Threat Defense 証明書のマップ オブジェクトについて](#)で定義されます。

手順

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

リストに表示されるポリシーは VPN 構成ウィザードを使用して作成されていて、多くの場合すでに編集されています。失効ステータスは、ターゲット デバイスにリモート アクセス VPN ポリシーの旧バージョンがあることを示します。ポリシー設定を更新するには、最新のリモート アクセス VPN ポリシーを導入します。

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。

リモート アクセス ポリシーの主な構成要素が表示されます。

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)] を選択します。

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、クライアントをマッピングする接続プロファイル (トンネルグループ) を決定します。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。

- 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に求められます。

ステップ 5 このポリシーの [接続プロファイル マッピングの証明書 (Certificate to Connection Profile Mapping)] を追加します。

- [追加 (Add)] をクリックします。
- [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。
- 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される [接続プロファイル (Connection Profile)] を指定します。
- [保存 (Save)] をクリックします。

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

スマート ライセンス	従来ライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	該当なし	Firepower Threat Defense	任意 (Any)	Admin

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) Firepower Threat Defense 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。

手順

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

リストに表示されるポリシーは VPN 構成ウィザードを使用して作成されていて、多くの場合すでに編集されています。失効ステータスは、ターゲット デバイスにリモート アクセス VPN ポリシーの旧バージョンがあることを示します。ポリシー設定を更新するには、最新のリモート アクセス VPN ポリシーを導入します。

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。

リモート アクセス ポリシーの主な構成要素が表示されます。

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、RA VPN ポリシー作成時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 必要に応じて [選択済みグループ ポリシー (Selected Group Policy)] ウィンドウを設定したら、[OK] をクリックします。

関連トピック

[グループ ポリシー オブジェクトの設定](#)

Firepower Threat Defense IPsec 設定の編集

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
エクスポート制御機能が有効になっている、スマート ライセンス アカウントに関連付けられている AnyConnect ライセンスのいずれか： <ul style="list-style-type: none"> • AnyConnect VPN Only • AnyConnect Plus • AnyConnect Apex 	該当なし	Firepower Threat Defense	任意 (Any)	管理者 (Administrator)

手順

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

リストに表示されるポリシーは VPN 構成ウィザードを使用して作成されていて、多くの場合すでに編集されています。失効ステータスは、ターゲット デバイスにリモート アクセス VPN ポリシーの旧バージョンがあることを示します。ポリシー設定を更新するには、最新のリモート アクセス VPN ポリシーを導入します。

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。

(注) 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、[Firepower Threat Defense 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 \(23 ページ\)](#) を参照してください。

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、[暗号マップ オプション \(33 ページ\)](#) 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、[Firepower Threat Defense 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 \(23 ページ\)](#) 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、[Firepower Threat Defense リモート アクセス VPN IKE ポリシー ページ \(36 ページ\)](#) を参照してください。新規 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。Firepower Threat Defense では、AnyConnect IKEv2 クライアントのみがサポートされます。サードパーティの標準 IKEv2 クライアントはサポートされません。
- 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、[Firepower Threat Defense リモート アクセス VPN の \[IPsec/IKEv2 パラメータ \(IPsec/IKEv2 Parameters\)\] ページ \(37 ページ\)](#) 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。

ステップ 6 [展開 (Deploy)] をクリックして、Firepower Threat Defense デバイスに設定の変更を展開します。

関連トピック

[Firepower Threat Defense のリモート アクセス VPN ポリシーの編集](#) (9 ページ)

[Firepower Threat Defense 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](#) (23 ページ)

リモート アクセス VPN の [暗号マップ (Crypto Maps)] ページ

このページを使用して、IPsec-IKEv2 プロトコルが有効になっているインターフェイス グループを表示します。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、[Firepower Threat Defense 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](#) (23 ページ) を参照してください。

テーブルの行を選択し、[編集 (Edit)] アイコンをクリックして、暗号マップのオプションを編集します。詳細については、[暗号マップ オプション](#) (33 ページ) を参照してください。

インターフェイス グループ (Interface Group)

IKEv2 プロトコルが有効なインターフェイス グループ。

IKEv2 IPsec プロポーザル (IKEv2 IPsec Proposals)

トランスフォームセットは、トンネル内のトラフィックの確立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。

リバース ルート インジェクション (Reverse Route Injection)

リバース ルート インジェクション (RRI) により、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。

関連トピック

[暗号マップ オプション](#) (33 ページ)

[Firepower Threat Defense IPsec 設定の編集](#) (31 ページ)

暗号マップ オプション

ナビゲーションパス

[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。ナビゲーション ウィンドウで、[IPsec] > [暗号マップ (Crypto Maps)] を開きます。

インターフェイス グループ (Interface Group)

IKEv2 プロトコルが有効なインターフェイス グループ。



(注) [Firepower Threat Defense 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](#) (23 ページ) タブを使用して、選択した VPN 設定に関連付けられているインターフェイス グループを追加または削除することができます。

IKEv2 IPsec プロポーザル (IKEv2 IPsec Proposals)

[編集 (Edit)] をクリックして、選択した IKEv2 方式のプロポーザルを指定します。[IKEv2 IPsec プロポーザル (IKEv2 IPsec Proposal)] ダイアログボックスで、使用可能なトランスフォームセットから選択するか、新しい IKEv2 IPsec プロポーザルを作成します。新しい IKEv2 IPsec プロポーザルの作成方法の詳細については、[IKEv2 IPsec プロポーザル オブジェクトの設定](#)を参照してください。

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)

リバース ルート インジェクション (RRI) により、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。

クライアントサービスの有効化 (Enable Client Services)

IKEv2 を有効にした場合だけ使用できます。

この接続に対して、Firepower Threat Defense デバイスのクライアント サービス サーバを有効にするかどうかを選択します。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と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、IKEv2 IPsec 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。

Perfect Forward Secrecy の有効化 (Enable Perfect Forward Secrecy)

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) を使用するかどうかを指定します。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 (Modulus Group)

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。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)。

ライフタイム継続時間 (秒数)

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。

ライフタイムのサイズ (KB)

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。

ESPv3 設定 (ESPv3 Settings)

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) ビットセットを持つ大きなパケットを IPsec サブシステムがどのように処理するかを定義します。

ポリシー

- 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、ペイロードサイズ、およびタイムアウト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。

関連トピック

[Firepower Threat Defense IPsec 設定の編集](#) (31 ページ)

リモート アクセス VPN における Firepower Threat Defense IKE ポリシーについて

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) Firepower Threat Defense 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。

Firepower Threat Defense リモート アクセス VPN IKE ポリシー ページ

IKE ポリシー

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 における Firepower Threat Defense IKE ポリシーについて \(36 ページ\)](#) を参照してください。



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

使用可能な IKEv2 ポリシーから選択するか、新しい IKEv2 ポリシーを追加するには [追加 (Add)] ボタンをクリックします。新しい IKEv2 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。

[名前 (Name)]

IKEv2 ポリシーの名前。

整合性

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

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。IKEv1 では、整合性アルゴリズムと PRF アルゴリズムを分けることができません。ただし、IKEv2 では、これらのエレメントに対して異なるアルゴリズムを指定できます。

DH グループ

暗号化に使用する Diffie-Hellman グループです。

関連トピック

[Firepower Threat Defense IPsec 設定の編集 \(31 ページ\)](#)

Firepower Threat Defense リモート アクセス VPN の [IPsec/IKEv2 パラメータ (IPsec/IKEv2 Parameters)] ページ

IKEv2 セッションの設定

ピアに送信するアイデンティティ

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、デバイスを再起動できません。

オンにすると、すべてのアクティブなセッションが自動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。

IKEv2 セキュリティ アソシエーション IKEv (SA) の設定

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。以下のオプションを選択します：

- カスタム (Custom)
- 常に (Always)
- なし (Never)

着信クッキーチャレンジのしきい値 (Threshold to Challenge Incoming Cookies)

許可されるネゴシエーション中の SA の総数の割合。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。デフォルトは 50% です。

許可されるネゴシエーション中の SA の数 (Number of SAs Allowed in Negotiation)

一時点でネゴシエーション中にできる SA の最大数を制限します。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。

IPsec 設定

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) が可能であることを確認します。

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。

NAT 設定

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選択します。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。

インターバル (Interval)

NAT キープアライブ インターバルを 10 ~ 3600 秒に設定します。デフォルトは 20 秒です。

関連トピック

[Firepower Threat Defense IPsec 設定の編集 \(31 ページ\)](#)

