リモート アクセス VPN

リモートアクセス仮想プライベートネットワーク（VPN）では、インターネットに接続されたコンピュータやその他のサポート対象デバイスを使用して、各ユーザーが離れた場所からネットワークに接続できます。これにより、モバイル ワーカーが各自のホーム ネットワークや公共の Wi-Fi ネットワークなどから接続できるようになります。

ここでは、ネットワークのリモート アクセス VPN を設定する方法について説明します。

リモート アクセス VPN の概要

Secure Firewall 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 Secure Client 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 ユーザーに提供します。クライアントが Firewall Threat Defense と SSL VPN 接続をネゴシエートする際、Transport Layer Security（TLS）または Datagram Transport Layer Security（DTLS）を使用して接続します。

Secure Client 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、Firewall 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 ユーザーは 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 Secure Client 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 Secure Client 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。

[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 を基本機能も含めて設定します。次に、必要に応じてポリシー構成を強化し、Firewall 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 の機能

次の表では、Secure Firewall Threat Defense のリモートアクセス VPN の機能について説明します。

表 *1* : リモートアクセス *VPN* の機能

	説明
Secure Firewall Threat Defense リモートアクセス VPN の機能	• Secure Client を使用した SSL および IPsec-IKEv2 リモートアクセス。 • Secure Firewall 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。 • Firewall Management Center と Firewall Device Manager の両方での構成サポート。デバイス固有のオーバーライド。 • Secure Firewall Management Center および Firewall 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 サーバーのサポート。 • 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。 • Cisco Secure Client バージョン 4.7 以降での DTLS v1.2 プロトコルのサポート。 • Secure Clientモジュールは、リモートアクセス VPN 接続用の追加のセキュリティサービスをサポートしています。 • VPN ロード バランシング。

	説明
AAA 機能	• 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ー認証。 • RADIUS サーバー、LDAP、または AD を使用する AAA ユーザー名とパスワードベースのリモート認証。 • RADIUS グループとユーザー承認属性、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 サーバー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。 • Secure Firewall Management Center の Web インターフェイスを使用した LDAP または AD 認可属性。 • SAML 2.0 を使用したシングルサインオンのサポート。 • 同じエンティティ ID に対して複数のアプリケーションを持つことができるが、ID 証明書は一意である、Microsoft Azure での複数の ID プロバイダートラストポイントのサポート。 • 地理位置情報に基づいてリモートアクセス VPN 接続を制限します。
VPN トンネリング機能	• 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。

	説明
リモートアクセス VPN モニタリングの機能	• 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 ユーザーを表示する新しい VPN ダッシュボード ウィジェット。 • ユーザー名や 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。 • Firewall Threat Defense 統合 CLI により利用可能なトンネル統計。

Secure Client のコンポーネント

Secure Client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 Secure Client イメージ および Secure Client 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。の「*Deploy AnyConnect*」の章Cisco Secure Client（AnyConnect を含む）管理者ガイド、リリース 5 [英語] の「*Deploy Cisco Secure Client*」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 ユーザーは、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 ユーザーは 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。

ユーザー 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ーを識別すると、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、Firewall 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。

Secure Client 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。

Secure Client プロファイル およびエディタ

Secure Client プロファイル は、構成パラメータのグループで、動作や表示の設定に VPN クライアントで使用される 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。

Secure Client 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、Secure Client 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、Firewall 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 サーバー認証

Secure Firewall 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。

リモートアクセス VPN ポリシーウィザードを使用しているときに、選択した証明書を対象の Firewall 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 ポリシー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 ポリシーの構成が完了し、展開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、証明書で説明しています。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 ユーザー認証はユーザー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、Secure Firewall Threat Defense または Secure Firewall 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 サーバーでは、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、ユーザーの身元（認証）、ユーザーが許可されていること（認可）、およびユーザーが行ったこと（アカウンティング）を確認できます。AAA サーバーの例としては、RADIUS、LDAP/AD、TACACS+、Kerberos などがあります。Firewall 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 サーバーが認証のためにサポートされています。

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。

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 サーバーグループを設定する必要があります。詳細については、LDAP レルムまたは Active Directory（AD）レルムおよびレルムディレクトリを作成するおよびRADIUS サーバーグループの追加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 サーバー名、名前付き URL、および FQDN またはホスト名を持つ CA サーバーを解決できません。解決できるのは IP アドレスのみです。

リモート ユーザー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 サーバー 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、Secure Firewall Threat Defense セキュア ゲートウェイと統合されます。

（注） ユーザーが認証ソースとして Active Directory を使用してリモートアクセス VPN で認証を受ける場合、ユーザーは自分のユーザー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 はこのユーザー名をログオン名、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 でユーザーの命名属性 [英語] を参照してください。

認証に RADIUS を使用する場合、ユーザー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 ユーザーには *VPN ID* が適用されます。この VPN ID は、そのリモート ユーザー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 Secure Firewall 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 ユーザー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制御ポリシーのセクションを参照してください。

関連トピック

リモートアクセス VPN の AAA 設定 （32 ページ）

権限および属性のポリシー実施の概要

Secure Firewall Threat Defense デバイスは、外部認証サーバーおよび/または承認 AAA サーバー（RADIUS）から、あるいは Firewall Threat Defense デバイス上のグループ ポリシーから、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 VPN 接続に適用することをサポートしています。Firewall 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 サーバーから属性を受信した場合は、AAA サーバーからの属性が常に優先されます。

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

1. **外部 AAA サーバー上のユーザー属性**：ユーザー認証や認可が成功すると、サーバー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 サーバーからユーザーの RADIUS CLASS 属性 IETF-Class-25（OU=group-policy）の値が返された場合は、Firewall Threat Defense デバイスはそのユーザー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、サーバー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。

（注） Firewall 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、ユーザー属性または AAA サーバーのグループ 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ー セッションに使用されます。

関連トピック

リモートアクセス VPN の AAA 設定 （32 ページ）

AAA サーバー接続の概要

LDAP、AD、および RADIUS AAA サーバーは、ユーザー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、Firewall Threat Defense デバイスから到達できる必要があります。AAA サーバーは、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。

- **ユーザー識別処理**：サーバー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。

  Firewall Threat Defense では、管理インターフェイスにはデータ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**：サーバーはデータインターフェイスまた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。

  管理インターフェイスを使用するには、送信元インターフェイスとして明示的に管理を選択する必要があります。他の管理専用インターフェイスは使用できません。

両方のアクティビティに同じ AAA サーバーを使用するには、管理インターフェイスを送信元インターフェイスとして指定することを推奨します。

さまざまなインターフェイスの詳細については、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、Firewall Threat Defense デバイスからの AAA サーバー接続をモニターおよびトラブルシューティングします。

- **show aaa-server** AAA サーバーの統計情報を表示します。
- **show network** と **show network-static-routes** は管理インターフェイスのデフォルトルートとスタティックルートを表示します。
- **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 サーバーへのパスを確認します。
- **ping interface** *ifname* と **traceroute** *destination* はデータインターフェイスを介して AAA サーバーへのパスを確認します。
- **test aaa-server authentication** と **test aaa-server authorization** は AAA サーバー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 サーバー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 サーバーをアクティブ化します。または、 **aaa-server** *groupname* **fail host** *hostname* で AAA サーバーを不合格にします。
- **debug ldap level**、**debug aaa authentication**、 **debug aaa authorization**、**debug aaa accounting**。

リモートアクセス VPN のライセンス要件

Threat Defense License

Firewall Threat Defense リモートアクセス VPN には、Strong Encryption、およびセキュアクライアントの次のライセンスのいずれかが必要です。

- Secure Client Advantage
- Secure Client Premier

- Secure Client VPN Only

リモートアクセス VPN の要件と前提条件

Model support

Firewall Threat Defense

Supported domains

Any

User roles

Admin

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 人のユーザーが同時にリモート 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 Secure Firewall Threat Defense デバイスを移動することはできません。
- ECMP を使用している場合、リモートアクセス VPN は SSL をサポートしません。IPsec-IKEv2 を使用することをお勧めします。
- 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 Firewall Threat Defense 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。
- DHCP を使用してクライアントに IP アドレスを提供しており、クライアントがアドレスを取得できない場合は、NAT ルールを確認します。RA VPN ネットワークに適用される NAT ルールには、ルート ルックアップ オプションが含まれている必要があります。ルートルックアップは、DHCP要求が適切なインターフェイスを介してDHCPサーバーに確実に送信されるようにするために役立つ場合があります。

- IKE ポート 500/4500 または SSL ポート 443 が使用されている場合や、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、Secure Client 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 ポリシーを設定する前に Firewall 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 Firewall 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。
- ECMP ゾーンインターフェイスは、IPsec が有効なリモートアクセス VPN で使用できます。
- ECMP ゾーンインターフェイスは、SSL が有効なリモートアクセス VPN では使用できません。セキュリティゾーンまたはインターフェイスグループに属するすべてのリモートアクセス VPN インターフェイスが 1 つ以上の ECMP ゾーンにも属している場合、リモートアクセス VPN（SSL が有効）構成の展開は失敗します。ただし、セキュリティゾーンまたはインターフェイスグループに属するリモートアクセス VPN インターフェイスの一部のみが 1 つ以上の ECMP ゾーンにも属している場合は、それらのインターフェイスを除外してリモートアクセス VPN 構成を展開できます。
- リモート アクセス VPN ポリシーの設定を変更した後は、Firewall 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、設定変更を展開するためのベストプラクティスを確認してください。
- RA VPN ヘッドエンドなどに対する **curl** などのコマンドの実行は直接サポートされていないため、望ましい結果が得られない可能性があります。たとえば、ヘッドエンドは HTTP HEAD リクエストに応答しません。
- Firewall Threat Defense は、サードパーティ製クライアントが Null ユーザーエージェントを送信した場合、リモートアクセス VPN セッションを受け入れません。
- FlexConfig を使用してブラウザプロキシを設定できます。
- 高可用性を備えたリモートブランチ展開（RBD）では、高可用性ペアを解除すると、スタンバイユニットの RBD WAN インターフェイスで、RA VPN ポリシーの割り当てと VPN 設定が削除されます。
- **[復号化されたトラフィックのBypass Access Controlポリシー（Bypass Access Control policy for decrypted traffic）]** が、Firewall Threat Defense で無効になっており、ISE が DACL を発行すると、トラフィックはまず ACP と照合されます。許可された場合、DACL チェックに進みます。拒否された場合、DACL 照合はバイパスされます。

同時 VPN セッションのキャパシティプランニング（Firewall Threat Defense Virtual モデル）

同時 VPN セッションの最大数は、インストールされている Firewall Threat Defense Virtual スマートライセンスの権限付与階層によって制御され、レートリミッタによって適用されます。ライセンスを取得した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。この限度は、システム パフォーマンスが許容できないレベルにまで低下することがないように設定されています。キャパシティプランニングの際は次の限度を考慮してください。

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
Firewall Threat Defense Virtual5	50
Firewall Threat Defense Virtual10	250
Firewall Threat Defense Virtual20	250
Firewall Threat Defense Virtual30	250
Firewall Threat Defense Virtual50	750
Firewall Threat Defense Virtual100	10,000

同時 VPN セッションのキャパシティプランニング（ハードウェアモデル）

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。この限度は、システム パフォーマンスが許容できないレベルにまで低下することがないように設定されています。キャパシティプランニングの際は次の限度を考慮してください。

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 1010	75
Firepower 1120	150
Firepower 1140	400
Firepower 2110	1,500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10,000
Secure Firewall 3110	3000
Secure Firewall 3120	6000
Secure Firewall 3130	15,000

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
Secure Firewall 3140	20,000
Firepower 4100、すべてのモデル	10,000
Firepower 9300 アプライアンス、すべてのモデル	20,000
ISA 3000	25

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、Firewall Threat Defense 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、「Cisco Secure Firewall ASA Series Syslog Messages」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、Firewall 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。

Devices > **Platform Settings**、**[編集（Edit）]**、**[SSL]** の順に選択します。

Devices > **VPN** > **Remote Access**、**[編集（Edit）]**、**[詳細（Advanced）]** ドロップダウンリスト、**[IPsec]** の順に選択します。

SSL 設定と IPsec の詳細については、SSL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 （72 ページ）を参照してください。

認証、認可、アカウンティング

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 サーバー名、名前付き URL、および FQDN またはホスト名を持つ CA サーバーを解決できません。解決できるのは IP アドレスのみです。

[プラットフォーム設定（Platform Settings）] を使用して DNS を設定できます。詳細については、DNSおよびDNS サーバ グループ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、Secure Firewall Threat Defense または Secure Firewall 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。

Secure Client のサポートされない機能

サポートされている唯一の VPN クライアントは Cisco Secure Client 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 Secure Client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。

（注） Firewall Threat Defense デバイスで複数の Secure Client パッケージを使用すると、メモリ使用量が増加し、デバイスのパフォーマンスに影響を与える可能性があります。メモリの枯渇による継続的なリブートを回避するために、ローエンドの Threat Defense デバイスで複数の Secure Client パッケージを使用しないことを推奨します。

Firewall Threat Defense セキュアゲートウェイに接続する場合、次の Secure Client 機能はサポートされていません。

- TACACS、Kerberos（KCD 認証および RSA SDI）、および SDI。

新規リモート アクセス VPN 接続の設定

ここでは、VPN ゲートウェイとして Secure Firewall Threat Defense デバイス、VPN クライアントとして Cisco Secure Client 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手順について説明します。

手順	操作内容	詳細
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 （10 ページ） リモート アクセス VPN を設定するための前提条件 （15 ページ）
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 （16 ページ）
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。	Secure Firewall Threat Defense デバイスのアクセスコントロール ポリシーの更新 （19 ページ）
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。	（任意）NAT 免除の設定 （20 ページ）
5	DNS を設定します。	DNS の設定 （22 ページ）

手順	操作内容	詳細
6	Secure Client プロファイルを追加します。	Secure Client プロファイル XML ファイルの追加（22 ページ）
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
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 （26 ページ）

リモート アクセス VPN を設定するための前提条件

- Secure Firewall Threat Defense デバイスを展開し、Secure Firewall 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 Firewall 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。
- 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。
- AAA サーバーが Firewall Threat Defense デバイスから到達可能であることを確認します。ルーティングを構成（**Devices** > **Device Management** 、 **[編集（Edit）]** アイコンをクリックします。左ペインから **[ルーティング（Routing）]** を選択します。）AAA サーバーへの接続を確保します。

  リモート アクセス VPN の二重認証の場合は、プライマリとセカンダリの両方の認証サーバーに Firewall Threat Defense デバイスからアクセスできることを確認します。
- Firewall Threat Defense のリモートアクセス VPN を有効にするため、Secure Client Advantage、Secure Client Premier、または Secure Client VPN Only のうちいずれかの Cisco Secure Client 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 Secure Client イメージ ファイルをダウンロードします。

  Secure Firewall Management Center Web インターフェイスで、**Objects** > **Object Management** > **VPN** > **Secure Client File** に移動し、新しい Secure Client イメージファイルを追加します。
- ユーザーが 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（Interface）を参照してください。
- Secure Client 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、Secure Client 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、既存の Secure Client プロファイルを変更したり、新規に作成したりできます。

新しいリモート アクセス VPN ポリシーの作成

リモートアクセス VPN ポリシーウィザードは、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。必要に応じて追加の属性を指定することでポリシー構成を強化して Secure Firewall Threat Defense のセキュア ゲートウェイ デバイスに展開できます。

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 （15 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。

手順

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

ステップ 2 [追加（Add）] をクリックして、リモートアクセス VPN ポリシーウィザードを使用して、基本的なポリシー構成で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とプロトコルを選択します。

ここで選択する Firewall Threat Defense デバイスは、VPN クライアントユーザーのリモートアクセス VPN ゲートウェイとして機能します。

新しいリモートアクセス VPN ポリシーを作成するときに Firewall Threat Defense デバイスを追加したり、後で変更したりできます。「リモートアクセス VPN ポリシーのターゲットデバイスの設定 （27 ページ）」を参照してください。

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。Firewall 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。

（注）
Firewall Threat Defense は、NULL 暗号化を使用する IPSec トンネルをサポートしていません。IPSec-IKEv2 を選択した場合は、IPSec IKEv2 プロポーザルに NULL 暗号化を選択しないでください。「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。

SSL 設定については、SSLを参照してください。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 [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、リモートユーザーが 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。Firewall 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 （29 ページ）を参照してください。

ステップ 6 [認証、認可、およびアカウンティング（Authentication, Authorization & Accounting）] の設定を指定します。

設定の詳細については、次を参照してください。

- AAA 設定： リモートアクセス VPN の AAA 設定 （32 ページ）
- LDAP 属性マップ： LDAP 属性マッピングの設定 （60 ページ）
- SAML 2.0 シングルサインオン認証： SAML シングルサインオン認証の設定 （121 ページ）

ステップ 7 [クライアントアドレスの割り当て（Client Address Assignment）] の設定を指定します。

クライアントの IP アドレスは、AAA サーバー、DHCP サーバー、および IP アドレスプールから割り当てることができます。複数のオプションを選択した場合、IP アドレスの割り当ては、AAA サーバー、DHCP サーバー、IP アドレスプールの順に行われます。AAA サーバーからのクライアント IP アドレス割り当ては、レルムおよび RADIUS 認証についてのみサポートされています。レルムまたは RADIUS サーバーがクライアント IP アドレスを提供するように設定されていることを確認してください。

ステップ 8 [グループポリシー（Group Policy）] の設定を指定します。

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 ユーザーに対してリモート 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、ユーザー認証プロファイル、IP アドレス、Secure Client 設定、VLAN マッピング、およびユーザーセッション設定などの属性を設定します。RADIUS 承認サーバーがグループ 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 （60 ページ）を参照してください。

ステップ 9 [次へ（Next）] をクリックします。

ステップ 10 VPN ユーザーがリモートアクセス VPN への接続に使用する **[Secure Clientイメージ（Secure Client Image）]** を選択します。

Secure Client は Secure Firewall 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、リモートユーザー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。Firewall 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 ユーザー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、Secure Client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。

クライアントプロファイルおよびクライアントモジュールの設定については、グループポリシーの Secure Clientオプションを参照してください。

ステップ 11 [次へ（Next）] をクリックします。

ステップ 12 [入力 VPN アクセスのネットワーク インターフェイス（Network Interface for Incoming VPN Access）] を設定します。

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。

（任意）必要に応じて、[メンバーインターフェイスの DTLS の有効化（Enable DTLS on member interfaces）] チェックボックスをオンにします。DTLS は SSL プロトコルにのみ適用できます。

ステップ 13 [デバイス証明書（Device Certificates）] を設定します。

デバイス証明書（アイデンティティ証明書とも呼ばれる）により、リモート アクセス クライアントへの VPN ゲートウェイが識別されます。VPN ゲートウェイの認証に使用する証明書を選択します。**[証明書を登録（Certificate Enrollment）]** ドロップダウンリストで証明書を選択するか、**[+]** をクリックして証明書を追加して、VPN ゲートウェイを認証します。

ステップ 14 **サービス アクセス コントロール**を設定します。

サービス アクセス オブジェクトを使用して、バージョン 7.7 以降の Firewall Threat Defense デバイス上で VPN へのリモート クライアント アクセスを制御できます。このオブジェクトは、VPN 認証の前に、クライアントに対して地理位置情報ベースのアクセス制御を提供します。デフォルトでは、RA VPN はアクセス制御されないため、リモートクライアントは、サービス アクセス オブジェクトで指定されていない限り、任意の地理位置から接続できます。詳細については、地理位置情報に基づくリモートユーザーの VPN アクセスの管理 （93 ページ）およびサービスアクセスオブジェクトの設定を参照してください。

ステップ 15 [VPN トラフィックのアクセス制御（Access Control for VPN Traffic）] を設定します。

デフォルトでは、VPN トンネルで復号されたトラフィックはすべて、アクセス コントロール ポリシーの対象となります。復号されたトラフィックをアクセス コントロール ポリシーからバイパスするには、[復号されたトラフィックでアクセス 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)）] チェックボックスをオンにします。このオプションではアクセス コントロール ポリシー検査はバイパスされますが、AAA サーバーからダウンロードされた VPN フィルタ ACL および認可 ACL は引き続き VPN トラフィックに適用されます。

（注）
このオプションを選択した場合は、Secure Firewall Threat Defense デバイスのアクセス コントロール ポリシーの更新 （19 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 16 [次へ（Next）] をクリックします。

ステップ 17 リモートアクセス VPN ポリシー構成の [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 18 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。

リモートアクセス VPN ポリシーウィザードを完了すると、ポリシーリストページが表示されます。後で、DNS 構成をセットアップし、VPN ユーザー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）、基本的なリモートアクセス VPN ポリシー構成を完了します。

次のタスク

リモートアクセス VPN ダッシュボード（**Overview** > **Dashboards** > **Remote Access VPN**）を使用して、デバイス上のアクティブなリモートアクセス VPN セッションからのリアルタイムデータをモニターします。ユーザーセッションに関連する問題をすばやく特定し、ネットワークとユーザーの問題を軽減できます。詳細については、リモートアクセス VPN ダッシュボード（140 ページ）を参照してください。

Secure Firewall 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 Secure Firewall 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。

すべての VPN 接続のオプションを有効または無効にします。このオプションを無効にする場合は、トラフィックがアクセス コントロール ポリシーまたはプレフィルタポリシーによって許可されていることを確認してください。

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 （52 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。

手順

ステップ 1 Secure Firewall Management Center Web インターフェイスで、[**Policies** > **Access Control heading** > **Access Control**] を選択します

ステップ 2 更新するアクセス コントロール ポリシーで [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。

（任意）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。

リモートアクセスまたはサイト間 VPN の静的アイデンティティ NAT を設定する場合は、ルートルックアップオプションを使用して NAT を設定する必要があります。ルートルックアップがない場合、Firewall Threat Defense は、ルーティング テーブルの内容に関係なく、NAT コマンドで指定されたインターフェイスからトラフィックを送信します。たとえば、Firewall Threat

Defense で DHCP スコープのトラフィックを誤ったインターフェイス経由で送信しないようにします。トラフィックがインターフェイスの IP アドレスに戻ることはありません。ルート ルックアップ オプションを使用すると、Firewall Threat Defense は、インターフェイスを介さずに、インターフェイスの IP アドレス上で直接トラフィックの送信および傍受が可能です。VPN クライアントから内部ネットワーク上のホストへのトラフィックの場合、ルート ルックアップ オプションがあっても正しい出力インターフェイス（内部）になるため、通常のトラフィック フローは影響を受けません。

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。

手順

ステップ 1 Secure Firewall Management Center の Web インターフェイスで、**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）] をクリックし、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 （52 ページ）を参照してください。

a) [変換（Translation）] をクリックし、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 を無効にすることもできます。その場合、アップストリーム ルータに適切なルートが確実に設定されていなくてはなりません。

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、Firewall 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 サーバー名、名前付き URL、FQDN またはホスト名を持つ CA サーバーを解決できません。IP アドレスのみを解決できます。

手順

ステップ 1 DNS サーバー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およびDNS サーバ グループ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 サーバー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。

Secure Client プロファイル XML ファイルの追加

Secure Client プロファイルは、構成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で使用される 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。

Secure Client プロファイル は、Secure Client ソフトウェアパッケージの一部として提供される GUI ベースの設定ツールである Secure Client プロファイル エディタを使用して作成できます。これは、Firewall Management Center の外部から実行する独立したプログラムです。Secure Client プロファイル エディタの詳細については、Cisco Secure Client（AnyConnect を含む）管理者ガイド [英語] を参照してください。

始める前に

Secure Firewall Threat Defense リモートアクセス VPN ポリシーの場合、VPN クライアントに Secure Client プロファイル を割り当てる必要があります。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。

Secure Client 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。

手順

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

ステップ 2 更新するリモートアクセス VPN ポリシーで [編集（Edit）] をクリックします。

ステップ 3 Secure Client プロファイルを追加する接続プロファイルで [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）] をクリックします。新しいグループポリシーを追加する場合は、[追加（Add）] をクリックします。

ステップ 5 **[Secure Client]** > **[プロファイル（Profile）]**を選択します。

ステップ 6 [クライアントプロファイル（Client Profile）] ドロップダウンリストからプロファイルを選択します。新しいクライアントプロファイルを追加する場合は、[追加（Add）]をクリックして、次の手順を実行します。

a) プロファイルの [名前（Name）] を指定します。

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

（注）
二要素認証の場合、Secure Client プロファイルのタイムアウト値は 60 秒以上に設定してください。

c) [保存（Save）] をクリックします。

ステップ 7 変更を保存します。

（任意）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 ユーザー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、スプリットトンネリングを設定します。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 （60 ページ）を参照してください。

手順

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

ステップ 2 スプリットトンネリングを設定するリモートアクセス VPN ポリシーで [編集（Edit）] をクリックします。

ステップ 3 必要な接続プロファイルで [編集（Edit）] をクリックします。

ステップ 4 [追加（Add）] 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）] をクリックします。

ステップ 5 [全般（General）] > [スプリットトンネリング（Split Tunneling）] を選択します。

ステップ 6 [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、[次に指定されたネットワークを除外（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。

デフォルト設定では、VPN トンネル経由のすべてのトラフィックが許可されます。

ステップ 7 [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 8 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）] ドロップダウンから [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 9 変更を保存します。

関連トピック

アクセスリスト

（任意）ダイナミック スプリット トンネリングの設定

ダイナミック スプリット トンネリングにより、DNS ドメイン名に基づいてスプリットトンネリングを微調整できます。リモートアクセス VPN トンネルに含める、または除外する必要があるドメインを設定できます。除外されたドメインはブロックされません。代わりに、これらのドメインへのトラフィックは VPN トンネルの外部に保持されます。たとえば、パブリックインターネット上の Cisco WebEx にトラフィックを送信することで、保護されたネットワーク内のサーバーへのトラフィック用に VPN トンネル内の帯域幅を解放できます。この機能の設定に関する詳細については、「FMC で管理する FTD 上の AnyConnect ダイナミック スプリット トンネルの設定」を参照してください。

始める前に

バージョン 7.0 以降では、Firewall Management Center と Firewall Threat Defense を使用してこの機能を設定できます。Firewall Management Center の古いバージョンを使用している場合は、「FMC を使用した Firepower Threat Defense 用に向けた、高度な AnyConnect VPN の展開」の指示に従って、FlexConfig を使用して設定できます。

手順

ステップ 1 ダイナミック スプリット トンネルを使用するようにグループポリシーを設定します。

a) **Devices** > **VPN** > **Remote Access**を選択します。
b) ダイナミック スプリット トンネリングを設定するリモートアクセス VPN ポリシーで [編集（Edit）] をクリックします。
c) 必要な接続プロファイルで [編集（Edit）] をクリックします。
d) [グループポリシーの編集（Edit Group Policy）] をクリックします。

ステップ 2 [グループポリシーの追加/編集（Add/Edit Group Policy）] ダイアログボックスで Secure Client カスタム属性を設定します。

a) [Secure Client] タブをクリックします。
b) [カスタム属性（Custom Attributes）] をクリックし、[+] をクリックします。
c) Secure Client [属性（Attribute）] ドロップダウンリストから [ダイナミック スプリット トンネリング（Dynamic Split Tunneling）] を選択します。
d) [+] をクリックして、新しいカスタム属性オブジェクトを作成します。
e) カスタム属性オブジェクトの名前を入力します。
f) [Include domains]：リモートアクセス VPN トンネルに含めるドメイン名を指定します。

   IP アドレスに基づいて除外されるドメインをトンネルに含めることができます。

g) [Exclude domains]：リモートアクセス VPN から除外するドメイン名を指定します。

   除外されるドメインはブロックされず、これらのドメインへのトラフィックは VPN トンネルの外部に保持されます。

h) [Save（保存）] をクリックします。
i) **[追加（Add）]** をクリックします。

ステップ 3 設定されたカスタム属性を確認し、[保存（Save）] をクリックしてグループポリシーを保存します。

ステップ 4 [保存（Save）] をクリックして接続プロファイルを保存します。

ステップ 5 [保存（Save）] をクリックして、リモートアクセス VPN ポリシーを保存します。

次のタスク

1. Firewall Threat Defense に設定を展開します。
2. Firewall Threat Defense および Secure Client で設定されたダイナミック スプリット トンネルの設定を確認します。詳細については、「ダイナミック スプリット トンネリング設定の確認 （26 ページ）」を参照してください。

ダイナミック スプリット トンネリング設定の確認

Firewall Threat Defense で以下を実行します。

ダイナミック スプリット トンネリング設定を確認するには、次のコマンドを使用します。

- **show running-config webvpn**
- **show running-config anyconnect-custom-data**
- **show running-config group-policy** <*group-policy-name*>

Secure Client で以下を実行します。

[統計（Statistics）]（  ）アイコンをクリックし、[VPN] > [統計（Statistics）] を選択します。[ダイナミックスプリットの除外/包含（Dynamic Split Exclusion/Inclusion）] カテゴリでドメインを確認できます。

設定の確認

手順

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 Firewall Threat Defense のリモートアクセス VPN ゲートウェイデバイスの 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ー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）
Secure Client をシステムにインストールすると、VPN への接続が自動的に確立されます。

Secure Client がインストールされていない場合は、VPN から Secure Client をダウンロードするよう要求されます。

ステップ 4 インストールされていない場合は Secure Client をダウンロードし、VPN に接続します。Secure Client が自動的にインストールされます。認証が成功したら、Secure Firewall Threat Defense リモートアクセス VPN ゲートウェイへの接続を確立します。リモートアクセス VPN は、VPN ポリシー設定に従って、該当するアイデンティティポリシーまたは QoS ポリシーを適用します。

既存のリモートアクセス VPN ポリシーのコピーの作成

既存のリモートアクセス VPN ポリシーをコピーして、接続プロファイルやアクセスインターフェイスなど、すべての設定を含む新しいリモートアクセス VPN を作成できます。その後、デバイスを新しいポリシーに割り当て、必要に応じて、割り当てられたデバイスに VPN を展開できます。

（注） リモートアクセス VPN の読み取り専用権限を持つユーザーは、VPN のコピーを作成できません。ドメインで読み取り専用権限を持つユーザーは、リモートアクセス VPN をコピーできます。

手順

ステップ 1 **Devices** > **VPN** > **Remote Access**を選択します。
ステップ 2 コピーするポリシーで [コピー（Copy）] をクリックします。
ステップ 3 新しいリモートアクセス VPN の [名前（Name）] を指定します。
ステップ 4 [OK] をクリックします。

次のタスク

デバイスを新しいポリシーに割り当てるには、リモートアクセス VPN ポリシーのターゲットデバイスの設定 （27 ページ）を参照してください。

リモートアクセス VPN ポリシーのターゲットデバイスの設定

リモートアクセス VPN ポリシーを作成したら、そのポリシーを Threat Defense デバイスに割り当てることができます。

手順

ステップ 1 **Devices** > **VPN** > **Remote Access**を選択します。
ステップ 2 編集するリモートアクセス VPN ポリシーの横にある **Edit** () をクリックします。
ステップ 3 [ポリシー割り当て（Policy Assignments）] をクリックします。

ステップ 4 次のいずれかを実行します。

- デバイス、ハイアベイラビリティペア、またはデバイスグループをポリシーに割り当てるには、[Available Devices）] リストで選択し、[Add] をクリックします。表示されているデバイスをドラッグアンドドロップして選択することもできます。
- デバイスの割り当てを削除するには、[選択されたデバイス（Selected Device）] リストのデバイス、高可用性ペア、またはデバイスグループの横にある **Delete** ( ) をクリックします。

ステップ 5 [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。

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。

ローカルレルムとリモートアクセス VPN ポリシーの関連付け

ローカルレルムをリモートアクセス VPN ポリシーに関連付けて、ローカルユーザー認証を有効にすることができます。

レルムの作成と管理については、レルムを管理するを参照してください。

リモートアクセス VPN のローカルユーザー認証の設定については、リモートアクセス VPN の AAA 設定 （32 ページ）を参照してください。

手順

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

ステップ 2 編集するリモートアクセス VPN ポリシーの横にある **Edit** ( ) をクリックします。

ステップ 3 [ローカルレルム（Local Realm）] の横にあるリンクをクリックします。

ステップ 4 リストから [ローカルレルムサーバー（Local Realm Server）] を選択するか、[追加（Add）] をクリックして新しいローカルレルムを追加します。

ステップ 5 [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。

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。

その他のリモートアクセス VPN の設定

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、Firewall 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。

別のグループの VPN ユーザーに異なる権限を付与する場合は、各ユーザーグループの特定の接続プロファイルを追加し、リモートアクセス VPN ポリシーで複数の接続プロファイルを維持できます。

手順

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（Connection Profile）] を選択し、[編集（Edit）] をクリックします。

ステップ 4 （オプション）新しい接続プロファイルを追加する場合は、[追加（Add）]をクリックします。

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 （29 ページ）

ステップ 6 （任意）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 の AAA 設定 （32 ページ）

ステップ 7 （任意）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 （51 ページ）

ステップ 8 変更を保存します。

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により、リモートアクセス VPN ユーザー用の IP アドレスを割り当てることができます。

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 サーバー、および AAA サーバーから割り当てることができます。最初に AAA サーバーが割り当てられ、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、Firewall 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。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） Firewall 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、**Objects** > **Object Management** > **Address Pools** パスを使用すると Firewall Management Center で 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。

手順

ステップ 1 **Devices** > **VPN** > **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 リモートアクセス VPN ポリシーを選択し、編集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、編集アイコンをクリックします。

ステップ 4 [クライアントアドレス割り当て（Client Address Assignment）] タブで、次の手順を実行します。

ステップ 5 [アドレスプール（Address Pools）] の横にある [+] をクリックします。

a) [アドレスプール（Address Pools）] の横にある [+] 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。[利用可能プール（Available Pools）] 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 Secure Firewall 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) [アドレスプール（Address Pools）] ウィンドウで [利用可能プール（Available Pools）] の横にある [+] をクリックして、新しい IPv4 または IPv6 アドレスプールを追加します。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。

IP アドレスプールを編集する場合は、メンテナンス期間中に次の手順を実行することを推奨します。

1. リモートアクセス VPN からデバイスの割り当てを解除します。
2. デバイスを選択して、[展開（Deploy）] をクリックします。

   この展開では、デバイスからすべてのリモートアクセス VPN 設定が削除され、リモートアクセス VPN セッションが終了します。セッションは再確立されません。
3. IP アドレスプールの横にある編集アイコンをクリックして編集し、必要に応じて Firewall Management Center で他のリモートアクセス VPN 設定を編集します。
4. 更新されたリモートアクセス VPN ポリシーにデバイスを割り当てます。
5. 設定をデバイスに展開します。

   リモートアクセス VPN クライアントは、メンテナンス期間の後、デバイスに接続できます。

ステップ 6 [DHCPサーバー（DHCP Servers）] の横にある [+] をクリックして、DHCP サーバーを追加します。

（注）
DHCP サーバー 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）のサーバー 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。[追加（Add）] をクリックして、オブジェクトリストからサーバーを選択します。DHCP サーバーを削除するには、[削除（Delete）] をクリックします。
b) 新しいネットワークオブジェクトを追加するには、[新しいオブジェクト（New Objects）] ページで [追加（Add）] をクリックします。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 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 （29 ページ）

リモートアクセス VPN の AAA 設定

始める前に

- 必要なマシンとユーザーの証明書がエンドポイントに展開されていることを確認してください。Firewall Threat Defense の詳細については、「Firewall Threat Defense 証明書を管理する」を参照してください。
- 必要な証明書を使用して Secure Client プロファイルを設定します。詳細については、『*Cisco Secure Client (including AnyConnect) Administrator Guide*』を参照してください。

手順

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、**[編集（Edit）]**、**[AAA]** の順に選択します。

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）]：ユーザー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、ユーザーの識別方法を決定します。有効なユーザー クレデンシャル（通常は、ユーザー名とパスワード）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）]：[認証サーバー（Authentication Server）] に [RADIUS] を選択した場合、デフォルトで許可サーバー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 サーバー（Accounting Server）] を選択します。[認証サーバー（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 [承認サーバー（Authorization Server）] と [アカウンティング サーバー（Accounting Server）] を選択する必要があります。
  - [SAML]：各ユーザーは SAML シングルサインオンサーバーを使用して認証されます。詳細については、「SAML 2.0 シングルサインオン認証 （118 ページ）」を参照してください。

    [IDプロバイダー証明書のオーバーライド（Override Identity Provider Certificate）]：選択すると、SAML プロバイダーのプライマリ ID プロバイダー証明書が、接続プロファイルまたは SAML アプリケーションに固有の IDP 証明書でオーバーライドされます。IdP 証明書をドロップダウンから選択します。

Microsoft Azure は、同じエンティティ ID に対して複数のアプリケーションをサポートできます。各アプリケーション（異なる接続プロファイルにマップされている）には、一意の証明書が必要です。現在の接続プロファイルのシングル サインオン オブジェクトの既存のエンティティ ID を保持し、別の IdP 証明書を使用する場合は、このオプションを選択できます。

これにより、Microsoft Azure SAML ID プロバイダーごとに複数の SAML アプリケーションがサポートされるようになります。

プライマリ ID 証明書は、シングル サインオン サーバー オブジェクトに構成されます。

シングル サインオン サーバー オブジェクトの構成の詳細については、シングルサインオンサーバーの追加を参照してください。

[SAMLログインエクスペリエンス（SAML Login Experience）] を選択して、SAML Web 認証用のブラウザを構成します。

- [VPNクライアント組み込みブラウザ（VPN client embedded browser）]：Web 認証の場合に VPN クライアントに組み込まれているブラウザを使用するには、このオプションを選択します。認証は VPN 接続にのみ適用されます。
- [デフォルトOSブラウザ（Default OS Browser）]：WebAuthN（Web 認証の FIDO2 標準）をサポートするデフォルトまたはネイティブブラウザのオペレーティングシステムを構成するには、このオプションを選択します。このオプションは、生体認証などの Web 認証方法のシングルサインオン（SSO）サポートを有効にします。

  デフォルトのブラウザには、Web 認証用の外部ブラウザパッケージが必要です。Default-External-Browser-Package パッケージがデフォルトで構成されています。デフォルトの外部ブラウザパッケージを変更するには、リモートアクセス VPN ポリシーを編集し、**[詳細（Advanced）]** で、ファイルを選択し、**[AnyConnectクライアントイメージ（AnyConnect Client Images）]**、**[セキュアクライアントイメージ（Secure Client Images）]**、**[パケットファイル（Package File）]** の順に選択します。

  次を選択して、新しいパッケージファイルを追加することもできます。**Objects** > **Object Management** > **VPN** > **Secure Client File**、**[セキュアクライアントファイルを追加（Add Secure Client File）]** の順に選択します。

- [クライアント証明書のみ（Client Certificate Only）]：各ユーザー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、ユーザー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ー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。

  マシン証明書とユーザー証明書を使用して VPN クライアントを認証するには、[Enable multiple certificate authentication] を選択します。

複数の証明書認証を有効にしている場合は、次のいずれかの証明書を選択してユーザー名をマッピングし、VPN ユーザーを認証できます。

- [最初の証明書（First Certificate）]：VPN クライアントから送信されたマシン証明書からユーザー名をマッピングするには、このオプションを選択します。
- [2番目の証明書（Second Certificate）]：クライアントから送信されたユーザー証明書からユーザー名をマッピングするには、このオプションを選択します。

（注）
複数の証明書認証を有効にしない場合、ユーザー証明書（2 番目の証明書）がデフォルトで認証に使用されます。

クライアント証明書のユーザー名が含まれる [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 全体をユーザー名として使用（Use entire DN as username）] オプションを選択した場合、ユーザー 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、ユーザー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されます。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（ユーザー ID）
- UPN（ユーザー プリンシパル名）

- [クライアント証明書とAAA（Client Certificate & AAA）]：各ユーザーはクライアント証明書とAAAサーバーの両方を使用して認証されます。認証に必要な証明書と AAA 設定を選択します。

  どの認証方式を選択する場合にも、[ユーザー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。

- [クライアント証明書とSAML（Client Certificate & SAML）]：各ユーザーはクライアント証明書と SAML サーバーの両方を使用して認証されます。認証に必要な証明書と SAML の設定を選択します。

  - [証明書とSAMLのユーザー名が同じ場合にのみ接続を許可する（Allow connection only if username from certificate and SAML are the same）]：証明書のユーザー名が SAML シングルサインオンユーザー名と一致する場合にのみ VPN 接続を許可するときに選択します。
  - [認証用のクライアント証明書からユーザー名を使用する（Use username from client certificate for Authorization）]：認証のためにクライアント証明書からユーザー名を選択するオプションを選ぶ場合、クライアント証明書から選択するようにフィールドを設定する必要があります。

    特定のフィールドをユーザー名としてマップするか、認証に識別名（DN）全体を使用するかを選択できます。

    - [マップ固有フィールド（Map Specific Field）]：選択すると、クライアント証明書のユーザー名が含まれます。[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全体をユーザー名として使用（Use entire DN as username）]：承認用にユーザーアイデンティティが自動的に取得されます。

  ダイナミック アクセス ポリシー（DAP）を作成して、ユーザー固有の SAML アサーション属性またはユーザー名を DAP 証明書属性に一致させることもできます。DAP の AAA 基準設定を構成するを参照してください。

- [認証サーバー（Authentication Server）]：認証とは、ユーザー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、ユーザーの識別を行う方法です。認証には、有効なユーザー 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。

サーバーをすでに追加している場合は、リストから認証サーバーを選択します。あるいは、認証サーバーを作成します。

- [ローカル（LOCAL）]：Firewall Threat Defense のローカルデータベースがユーザー認証に使用されます。ローカル認証を設定するには、Firewall Threat Defense がバージョン 7.0 以降である必要があります。
  - [Local Realm]：ローカルレルムを選択するか、[Add] をクリックしてレルムを設定します。「LDAP レルムまたは Active Directory（AD）レルムおよびレルムディレクトリを作成する」を参照してください。
- [レルム（Realm）]：LDAP または AD レルムを設定します。LDAP レルムまたは Active Directory（AD）レルムおよびレルムディレクトリを作成する を参照してください。
- [RADIUS サーバーグループ（RADIUS Server Group）]：RADIUS サーバーグループオブジェクトを RADIUS サーバーとともに追加します。RADIUS サーバーグループの追加 を参照してください。
- [Single Sign-On Server]：SAML 認証用のシングル サインオン サーバー オブジェクトを作成します。「シングルサインオンサーバーの追加」を参照してください。

[Fallback to LOCAL Authentication]：ローカルデータベースが設定されていれば、ユーザーはローカルデータベースを使用して認証され、AAA サーバーグループが使用できない場合でも VPN トンネルを確立できます。

- [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ー名とパスワードを Secure Client ログイン画面に入力するには VPN ユーザーが必要です。認証サーバーまたはクライアント証明書からセカンダリ ユーザー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ー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つ目のユーザー名とパスワードのセカンダリ認証のサーバーグループ（AAA サーバー）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ーを LDAP または Active Directory レルムに、セカンダリ認証を RADIUS サーバーに設定できます。

  （注）
  デフォルトでは、セカンダリ認証は必要ありません。

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

- [Fallback to LOCAL Authentication]：ローカルデータベースが設定されていれば、ユーザーはローカルデータベースを使用して認証され、AAA サーバーグループが使用できない場合でも VPN トンネルを確立できます。

[セカンダリ認証のユーザー名（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ー名とパスワードを入力するようユーザーに要求します。
- [プライマリ認証ユーザー名を使用（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ーからユーザー名が取得されます。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ー名をマップ（Map username from client certificate）]：クライアント証明書からセカンダリ ユーザー名が事前に入力されます。

  複数の証明書認証を有効にしている場合は、次のいずれかの証明書を選択できます。

  - [First Certificate]：VPN クライアントから送信されたマシン証明書からユーザー名をマッピングするには、このオプションを選択します。
  - [Second Certificate]：クライアントから送信されたユーザー証明書からユーザー名をマッピングするには、このオプションを選択します。
  - クライアント証明書のユーザー名を含む[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）全体をユーザー名として使用（Use entire DN (Distinguished Name) as username）] オプションを選択した場合はユーザー 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。

  - [ユーザーログインウィンドウに証明書からユーザー名を事前に入力（Prefill username from certificate on user login window）]：ユーザーが Secure Client 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ー名を事前に入力します。
    - [ログイン ウィンドウでユーザー名を非表示にする（Hide username in login window）]：セカンダリ ユーザー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ーには表示されず、ユーザーが事前に入力されたユーザー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 ユーザー名を使用（Use secondary username for VPN session）]：VPN セッション中のユーザー アクティビティのレポートにセカンダリ ユーザー名を使用します。

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ー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、ユーザー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ー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。

  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（8 ページ）を参照してください。

  RADIUS サーバーが接続プロファイルのユーザー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、ユーザーまたはユーザーグループに複数の承認属性を構成できます。RADIUS サーバーに構成される承認属性は、ユーザーまたはユーザーグループに固有にできます。ユーザーが認証されると、これらの特定の承認属性が Firewall Threat Defense デバイスにプッシュされます。

  （注）
  許可サーバーから所得した AAA サーバー属性は、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、[ユーザー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ー名が承認データベース内に存在することを確認します。ユーザー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。

- 許可サーバーとしてレルムを選択する場合は、LDAP 属性マップを設定する必要があります。認証と認可に単一のサーバーを選択することも別のサーバーを選択することもできます。[LDAP 属性マップの設定（Configure LDAP Attribute Map）] をクリックして、認可用の LDAP 属性マップを追加します。

  （注）
  Firewall Threat Defense は、認可サーバーとして SAML アイデンティティ プロバイダーをサポートしていません。SAML ID プロバイダーの背後にある Active Directory が Firewall Management Center および Firewall Threat Defense を介して到達可能な場合は、次の手順で認可を設定できます。

  - AD サーバーのレルムを追加します。LDAP レルムまたは Active Directory（AD）レルムおよびレルムディレクトリを作成する を参照してください。
  - リモートアクセス VPN 接続プロファイルで認可サーバーとしてレルムオブジェクトを選択します。
  - 選択したレルムの LDAP 属性マップを設定します。

  LDAP 属性マップの設定の詳細については、LDAP 属性マッピングの設定 （60 ページ）を参照してください。

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ー（Accounting Server）]：アカウンティングは、ユーザーがアクセスしているサービス、およびユーザー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 サーバーはユーザー アクティビティを RADIUS サーバーに報告します。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、ユーザー名、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 サーバー 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。

- [ユーザー名からレルムを削除（Strip Realm from username）]：ユーザー名を AAA サーバーに渡す前に、ユーザー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、ユーザー名からドメインが削除され、認証用の AAA サーバーに送信されます。デフォルトでは、このオプションはオフになっています。
- [ユーザー名からグループを削除（Strip Group from username）]：ユーザー名を AAA サーバーに渡す前に、ユーザー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、ユーザー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 ユーザー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。

関連トピック

権限および属性のポリシー実施の概要 （8 ページ）
レルムを管理する

Secure Firewall Threat Defense の RADIUS サーバー属性

Firewall 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 サーバーから、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。

（注） Secure Firewall 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。

次のユーザー認可属性が Firewall Threat Defense デバイスから RADIUS サーバーに送信されます。

- RADIUS 属性 146 および 150 は、認証および認可の要求の場合に Firewall Threat Defense デバイスから RADIUS サーバーに送信されます。
- 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、Firewall Threat Defense デバイスから RADIUS サーバーに送信されます。

表 *2 : Secure Firewall Threat Defense* から *RADIU* サーバーに送信される *RADIUS* 属性

属性	属性番号	シンタックス、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 = Secure Client SSL VPN、6 = Secure Client IPsec VPN（IKEv2）
セッション タイプ	151	整数	シングル	1 = Secure Client SSL VPN、2 = Secure Client IPsec VPN（IKEv2）

表 *3 :* サポートされる *RADIUS* 認証属性

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Access-Hours	Y	1	文字列	シングル	時間範囲の名前（Business-hours など）

属性名	Firewall Threat Defense	属性番号	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	Y	86	文字列	シングル	アクセス リスト属性の両方が、Firewall Defense デバイスで設定されている ACL 使用します。スマート CLI 拡張アクセス オブジェクト タイプを使用して、これら 作成します（**[デバイス（Device）]** > **[詳（Advanced Configuration）]** > **[スマート（Smart CLI）]** > **[オブジェクト（Object** します）。 これらのACLは、着信(Firewall Threat De イスに入るトラフィック)または発信(Fire Defenseデバイスから出るトラフィック)フィックフローを制御します。
Access-List-Outbound	Y	87	文字列	シングル	
Address-Pools	Y	217	文字列	シングル	Firewall Threat Defense デバイスで定義さ トワークオブジェクトの名前。リモート VPN へのクライアント接続のアドレスプ て使用されるサブネットを識別します。 クト（Objects）]ページでネットワークオ トを定義し、次にネットワークオブジェ ループポリシーまたは接続プロファイル けます。
Allow-Network-Extension-Mode	Y	64	ブール	シングル	0 = 無効1 = 有効
Authenticated-User-Idle-Timeout	Y	50	整数	シングル	1 ～ 35791394 分
Authorization-DN-Field	Y	67	文字列	シングル	有効な値：UID、OU、O、CN、L、SP、 T、N、GN、SN、I、GENQ、DNQ、SER use-entire-name
Authorization-Required		66	整数	シングル	0 = いいえ 1 = はい
Authorization-Type	Y	65	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP
Banner1	Y	15	文字列	シングル	Cisco VPN リモートアクセスセッション IKEv1、Secure Client SSL-TLS/DTLS/IKEv クライアントレス SSL）に対して表示され 文字列
Banner2	Y	36	文字列	シングル	Cisco VPN リモートアクセスセッション IKEv1、Secure Client SSL-TLS/DTLS/IKEv クライアントレス SSL）に対して表示され 文字列Banner2 文字列は Banner1 文字列に ます（設定されている場合）。

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Cisco-IP-Phone-Bypass	Y	51	整数	シングル	0 = 無効1 = 有効
Cisco-LEAP-Bypass	Y	75	整数	シングル	0 = 無効1 = 有効
Client Type	Y	150	整数	シングル	1 = Cisco VPN Client（IKEv1） 2 = Secure Cli VPN 3 = Clientless SSL VPN 4 = Cut-Through- = L2TP/IPsec SSL VPN 6 = Secure Client IPsec （IKEv2）
Client-Type-Version-Limiting	Y	77	文字列	シングル	IPsec VPN のバージョン番号を示す文字列
DHCP-Network-Scope	Y	61	文字列	シングル	IP アドレス
Extended-Authentication-On-Rekey	Y	122	整数	シングル	0 = 無効1 = 有効
Framed-Interface-Id	Y	96	文字列	シングル	割り当てられた IPv6 インターフェイス ID。 割り当てられた IPv6 アドレスを作成するた Framed-IPv6-Prefix と組み合わせます。例： Framed-Interface-ID=1:1:1:1 と Framed-IPv6-Prefix=2001:0db8::/64 を組み合わ と、IP アドレス 2001:0db8::1:1:1:1 が得られ
Framed-IPv6-Prefix	Y	97	文字列	シングル	割り当てられた IPv6 プレフィックスと長さ に割り当てられた IPv6 アドレスを作成するた Framed-Interface-Id と組み合わせます。例： フィックス 2001:0db8::/64 と Framed-Interface-Id=1:1:1:1 を組み合わせると ドレス 2001:0db8::1:1:1:1 が得られます。こ を使用して、フレームインターフェイス Id せずに IP アドレスを割り当てることができ これには、プレフィックス長/128 を使用し なIPv6アドレスを割り当てます（たとえば、 ム化された IPv6 プレフィックス = 2001: 0db 1/128）。
Group-Policy	Y	25	文字列	シングル	リモート アクセス VPN セッションのグルー リシーを設定します。次のいずれかの形式 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。

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IE-Proxy-Bypass-Local		83	整数	シングル	0 = なし 1 = ローカル
IE-Proxy-Exception-List		82	文字列	シングル	改行（\n）区切りの DNS ドメインのリス
IE-Proxy-PAC-URL	Y	133	文字列	シングル	PAC アドレス文字列
IE-Proxy-Server		80	文字列	シングル	IP アドレス
IE-Proxy-Server-Policy		81	整数	シングル	1 = 変更なし 2 = プロキシなし 3 = 自動検 ンセントレータ設定を使用する
IKE-KeepAlive-Confidence-Interval	Y	68	整数	シングル	10 ～ 300 秒
IKE-Keepalive-Retry-Interval	Y	84	整数	シングル	2 ～ 10 秒
IKE-Keep-Alives	Y	41	ブール	シングル	0 = 無効1 = 有効
Intercept-DHCP-Configure-Msg	Y	62	ブール	シングル	0 = 無効1 = 有効
IPsec-Allow-Passwd-Store	Y	16	ブール	シングル	0 = 無効1 = 有効
IPsec-Authentication		13	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP（認可のみ ドメイン 4 = SDI 5 = 内部 6 = RADIUS で 認証 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	Y	42	ブール	シングル	0 = 無効1 = 有効
IPsec-Backup-Server-List	Y	60	文字列	シングル	サーバー アドレス（スペース区切り）
IPsec-Backup-Servers	Y	59	文字列	シングル	1 = クライアントが設定したリストを使用 クライアント リストを無効化して消去す クアップ サーバー リストを使用する
IPsec-Client-Firewall-Filter-Name		57	文字列	シングル	クライアントにファイアウォール ポリシ 配信するフィルタの名前を指定します。
IPsec-Client-Firewall-Filter-Optional	Y	58	整数	シングル	0 = 必須 1 = オプション
IPsec-Default-Domain	Y	28	文字列	シングル	クライアントに送信するデフォルト ドメ 1 つだけ指定します（1 ～ 255 文字）。
IPsec-IKE-Peer-ID-Check	Y	40	整数	シングル	1 = 必須 2 = ピア証明書でサポートされる チェックしない
IPsec-IP-Compression	Y	39	整数	シングル	0 = 無効1 = 有効
IPsec-Mode-Config	Y	31	ブール	シングル	0 = 無効1 = 有効

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IPsec-Over-UDP	Y	34	ブール	シングル	0 = 無効1 = 有効
IPsec-Over-UDP-Port	Y	35	整数	シングル	4001 ～ 49151。デフォルトは 10000 です。
IPsec-Required-Client-Firewall-Capability	Y	56	整数	シングル	0 = なし 1 = リモート FW Are-You-There（A 定義されているポリシー 2 = Policy pushed C サーバーからのポリシー
IPsec-Sec-Association		12	文字列	シングル	セキュリティ アソシエーションの名前
IPsec-Split-DNS-Names	Y	29	文字列	シングル	クライアントに送信するセカンダリ ドメイ リストを指定します（1 ～ 255 文字）。
IPsec-Split-Tunneling-Policy	Y	55	整数	シングル	0 = スプリット トンネリングなし 1 = スプリ ンネリング 2 = ローカル LAN を許可
IPsec-Split-Tunnel-List	Y	27	文字列	シングル	スプリット トンネルの包含リストを記述し トワークまたは ACL の名前を指定します。
IPsec-Tunnel-Type	Y	30	整数	シングル	1 = LAN-to-LAN 2 = リモート アクセス
IPsec-User-Group-Lock		33	ブール	シングル	0 = 無効1 = 有効
IPv6-Address-Pools	Y	218	文字列	シングル	IP ローカル プール IPv6 の名前
IPv6-VPN-Filter	Y	219	文字列	シングル	ACL 値
L2TP-Encryption		21	整数	シングル	ビットマップ： 1 = 暗号化が必要 2 = 40 ビ 128 ビット 8 = ステートレスが必要 15 = 40/1 トで暗号化/ステートレスが必要
L2TP-MPPC-Compression		38	整数	シングル	0 = 無効1 = 有効
Member-Of	Y	145	文字列	シングル	カンマ区切りの文字列。例： `Engineering, Sales` ダイナミック アクセス ポリシーで使用でき 属性。グループ ポリシーは設定されません
MS-Client-Subnet-Mask	Y	63	ブール	シングル	IP アドレス
NAC-Default-ACL		92	文字列		ACL
NAC-Enable		89	整数	シングル	0 = いいえ 1 = はい
NAC-Revalidation-Timer		91	整数	シングル	300 ～ 86400 秒

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
NAC-Settings	Y	141	文字列	シングル	NAC ポリシーの名前
NAC-Status-Query-Timer		90	整数	シングル	30 ～ 1800 秒
Perfect-Forward-Secrecy-Enable	Y	88	ブール	シングル	0 = いいえ 1 = はい
PPTP-Encryption		20	整数	シングル	ビットマップ： 1 = 暗号化が必要 2 = 40 128 ビット 8 = ステートレスが必要 15 = 4 トで暗号化/ステートレスが必要
PPTP-MPPC-Compression		37	整数	シングル	0 = 無効1 = 有効
Primary-DNS	Y	5	文字列	シングル	IP アドレス
Primary-WINS	Y	7	文字列	シングル	IP アドレス
Privilege-Level	Y	220	整数	シングル	0 ～ 15 の整数。
Required-Client- Firewall-Vendor-Code	Y	45	整数	シングル	1 = Cisco Systems（Cisco Integrated Client = Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco Systems（Cisco Intrusion Prevention Agent を使用）
Required-Client-Firewall-Description	Y	47	文字列	シングル	文字列
Required-Client-Firewall-Product-Code	Y	46	整数	シングル	シスコ製品： 1 = Cisco Intrusion Prevention Security Age Cisco Integrated Client（CIC） Zone Labs 製品： 1 = Zone Alarm 2 = Zone 3 = Zone Labs Integrity NetworkICE 製品： 1 = BlackIce Defender Sygate 製品： 1 = Personal Firewall 2 = Per Firewall Pro 3 = Security Agent
Required-Individual-User-Auth	Y	49	整数	シングル	0 = 無効1 = 有効
Require-HW-Client-Auth	Y	48	ブール	シングル	0 = 無効1 = 有効
Secondary-DNS	Y	6	文字列	シングル	IP アドレス
Secondary-WINS	Y	8	文字列	シングル	IP アドレス
SEP-Card-Assignment		9	整数	シングル	未使用

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Session Subtype	Y	152	整数	シングル	0 = なし 1 =クライアントレス 2 =クライアン クライアントのみ Session Subtype が適用されるのは、Session （151）属性の値が 1、2、3、または 4 の場 です。
Session Type	Y	151	整数	シングル	0 = なし 1 = Secure Client SSL VPN 2 = Secur IPSec VPN（IKEv2） 3 = クライアントレス S 4 = クライントレス電子メールプロキシ 5 = VPN Client（IKEv1） 6 = IKEv1 LAN-LAN 7 = LAN-LAN 8 = VPN ロードバランシング
Simultaneous-Logins	Y	2	整数	シングル	0-2147483647
Smart-Tunnel	Y	136	文字列	シングル	スマート トンネルの名前
Smart-Tunnel-Auto	Y	138	整数	シングル	0 = ディセーブル 1 = イネーブル 2 = 自動ス
Smart-Tunnel-Auto-Signon-Enable	Y	139	文字列	シングル	ドメイン名が付加された Smart Tunnel Auto リストの名前
Strip-Realm	Y	135	ブール	シングル	0 = 無効1 = 有効
SVC-Ask	Y	131	文字列	シングル	0=ディセーブル 1=イネーブル 3=デフォル ビスをイネーブルにする 5 = デフォルト ク ントレスをイネーブルにする （2 と 4 は使 い）
SVC-Ask-Timeout	Y	132	整数	シングル	5 ～ 120 秒
SVC-DPD-Interval-Client	Y	108	整数	シングル	0 = オフ 5 ～ 3600 秒
SVC-DPD-Interval-Gateway	Y	109	整数	シングル	0 = オフ 5 ～ 3600 秒
SVC-DTLS	Y	123	整数	シングル	0 = False 1 = True
SVC-Keepalive	Y	107	整数	シングル	0 = オフ、15 ～ 600 秒
SVC-Modules	Y	127	文字列	シングル	文字列（モジュールの名前）
SVC-MTU	Y	125	整数	シングル	MTU 値 256 ～ 1406 バイト
SVC-Profiles	Y	128	文字列	シングル	文字列（プロファイルの名前）
SVC-Rekey-Time	Y	110	整数	シングル	0 = ディセーブル 1 ～ 10080 分

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Tunnel Group Name	Y	146	文字列	シングル	1 ～ 253 文字
Tunnel-Group-Lock	Y	85	文字列	シングル	トンネル グループの名前または「none」
Tunneling-Protocols	Y	11	整数	シングル	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = I 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2 相互排他。0 ～ 11、16 ～ 27、32 ～ 43、 有効な値。
Use-Client-Address		17	ブール	シングル	0 = 無効1 = 有効
VLAN	Y	140	整数	シングル	0 ～ 4094
WebVPN-Access-List	Y	73	文字列	シングル	アクセス リスト名
WebVPN ACL	Y	73	文字列	シングル	デバイスの WebVPN ACL 名
WebVPN-ActiveX-Relay	Y	137	整数	シングル	0 = 無効 その他 = 有効
WebVPN-Apply-ACL	Y	102	整数	シングル	0 = 無効1 = 有効
WebVPN-Auto-HTTP-Signon	Y	124	文字列	シングル	予約済み
WebVPN-Citrix-Metaframe-Enable	Y	101	整数	シングル	0 = 無効1 = 有効
WebVPN-Content-Filter-Parameters	Y	69	整数	シングル	1 = Java ActiveX 2 = Java スクリプト 4 = = イメージに含まれるクッキー
WebVPN-Customization	Y	113	文字列	シングル	カスタマイゼーションの名前
WebVPN-Default-Homepage	Y	76	文字列	シングル	URL（たとえば http://example-example.co
WebVPN-Deny-Message	Y	116	文字列	シングル	有効な文字列（500 文字以内）
WebVPN-Download_Max-Size	Y	157	整数	シングル	0x7fffffff
WebVPN-File-Access-Enable	Y	94	整数	シングル	0 = 無効1 = 有効
WebVPN-File-Server-Browsing-Enable	Y	96	整数	シングル	0 = 無効1 = 有効
WebVPN-File-Server-Entry-Enable	Y	95	整数	シングル	0 = 無効1 = 有効
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	Y	78	文字列	シングル	オプションのワイルドカード（*）を使用 マ区切りの DNS/IP（たとえば、*.cisco.c 192.168.1.*、wwwin.cisco.com）
WebVPN-Hidden-Shares	Y	126	整数	シングル	0 = なし 1 = 表示される

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-Home-Page-Use-Smart-Tunnel	Y	228	ブール	シングル	クライアントレス ホーム ページをスマート ル経由で表示する場合にイネーブルにしま
WebVPN-HTML-Filter	Y	69	Bitmap	シングル	1 = Java ActiveX 2 = スクリプト 4 = イメージ8 キー
WebVPN-HTTP-Compression	Y	120	整数	シングル	0 = オフ 1 = デフレート圧縮
WebVPN-HTTP-Proxy-IP-Address	Y	74	文字列	シングル	http= または https= プレフィックス付きの、 区切りの DNS/IP:ポート（例：http=10.10.10. https=11.11.11.11:443）
WebVPN-Idle-Timeout-Alert-Interval	Y	148	整数	シングル	0 ～ 30。0 = ディセーブル。
WebVPN-Keepalive-Ignore	Y	121	整数	シングル	0 ～ 900
WebVPN-Macro-Substitution	Y	223	文字列	シングル	無制限。
WebVPN-Macro-Substitution	Y	224	文字列	シングル	無制限。
WebVPN-Port-Forwarding-Enable	Y	97	整数	シングル	0 = 無効1 = 有効
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	98	整数	シングル	0 = 無効1 = 有効
WebVPN-Port-Forwarding-HTTP-Proxy	Y	99	整数	シングル	0 = 無効1 = 有効
WebVPN-Port-Forwarding-List	Y	72	文字列	シングル	ポート転送リスト名
WebVPN-Port-Forwarding-Name	Y	79	文字列	シングル	名前の文字列（例、「Corporate-Apps」）。 このテキストでクライアントレス ポータル ページのデフォルト文字列「Application Acc 置き換えられます。
WebVPN-Post-Max-Size	Y	159	整数	シングル	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	Y	149	整数	シングル	0 ～ 30。0 = ディセーブル。
WebVPN Smart-Card-Removal-Disconnect	Y	225	ブール	シングル	0 = 無効1 = 有効
WebVPN-Smart-Tunnel	Y	136	文字列	シングル	スマート トンネルの名前
WebVPN-Smart-Tunnel-Auto-Sign-On	Y	139	文字列	シングル	ドメイン名が付加されたスマート トンネル インオン リストの名前
WebVPN-Smart-Tunnel-Auto-Start	Y	138	整数	シングル	0 = 無効1 = 有効2 = 自動スタート

属性名	Firewall Threat Defense	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-Smart-Tunnel-Tunnel-Policy	Y	227	文字列	シングル	「e ネットワーク名」、「i ネットワーク「a」のいずれか。ここで、ネットワークマート トンネル ネットワークのリストす。e はトンネルが除外されることを示ンネルが指定されることを示し、a はすべネルを示します。
WebVPN-SSL-VPN-Client-Enable	Y	103	整数	シングル	0 = 無効1 = 有効
WebVPN-SSL-VPN-Client-Keep- Installation	Y	105	整数	シングル	0 = 無効1 = 有効
WebVPN-SSL-VPN-Client-Required	Y	104	整数	シングル	0 = 無効1 = 有効
WebVPN-SSO-Server-Name	Y	114	文字列	シングル	有効な文字列
WebVPN-Storage-Key	Y	162	文字列	シングル	
WebVPN-Storage-Objects	Y	161	文字列	シングル	
WebVPN-SVC-Keepalive-Frequency	Y	107	整数	シングル	15 ～ 600 秒、0=オフ
WebVPN-SVC-Client-DPD-Frequency	Y	108	整数	シングル	5 ～ 3600 秒、0=オフ
WebVPN-SVC-DTLS-Enable	Y	123	整数	シングル	0 = 無効1 = 有効
WebVPN-SVC-DTLS-MTU	Y	125	整数	シングル	MTU 値は 256 ～ 1406 バイトです。
WebVPN-SVC-Gateway-DPD-Frequency	Y	109	整数	シングル	5 ～ 3600 秒、0=オフ
WebVPN-SVC-Rekey-Time	Y	110	整数	シングル	4 ～ 10080 分、0=オフ
WebVPN-SVC-Rekey-Method	Y	111	整数	シングル	0（オフ）、1（SSL）、2（新しいトンネ
WebVPN-SVC-Compression	Y	112	整数	シングル	0（オフ）、1（デフォルトの圧縮）
WebVPN-UNIX-Group-ID (GID)	Y	222	整数	シングル	UNIX での有効なグループ ID
WebVPN-UNIX-User-ID (UIDs)	Y	221	整数	シングル	UNIX での有効なユーザー ID
WebVPN-Upload-Max-Size	Y	158	整数	シングル	0x7fffffff
WebVPN-URL-Entry-Enable	Y	93	整数	シングル	0 = 無効1 = 有効
WebVPN-URL-List	Y	71	文字列	シングル	URL リスト名
WebVPN-User-Storage	Y	160	文字列	シングル	
WebVPN-VDI	Y	163	文字列	シングル	設定のリスト

表 *4 :* 送信される *RADIUS* 属性 *Secure Firewall Threat Defense*

属性	属性番号	シンタックス、タイプ	シングルまたはマルチ値	説明または値
Address-Pools	217	文字列	シングル	Firewall Threat Defense 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。リモートアクセス 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。[オブジェクト]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	ユーザがログインしたときに表示されるバナー。
Banner2	36	文字列	シングル	ユーザがログインしたときに表示されるバナーの 2 番目の部分。Banner2 が Banner1 に追加されます。
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 サーバーで ACL 名で参照されます。ACL 設定が Firewall 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。リモートアクセス VPN の [グループポリシー（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。次のいずれかの形式を使用できます。 • 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。Firewall Threat Defense 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。

ISE から返される IE-Proxy-Server-Method 属性の値を次のいずれかに設定する必要があります。

- IE_PROXY_METHOD_PACFILE: 8
- IE_PROXY_METHOD_PACFILE_AND_AUTODETECT: 11
- IE_PROXY_METHOD_PACFILE_AND_USE_SERVER: 12
- IE_PROXY_METHOD_PACFILE_AND_AUTODETECT_AND_USE_SERVER: 15

上記の値のいずれかが IE-Proxy-Server-Method 属性に使用されている場合にのみ、Firewall Threat Defense はプロキシ設定を配信します。

接続プロファイルのエイリアスの作成または更新

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、Secure Firewall 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。

手順

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

ステップ 2 変更するポリシーの [編集（Edit）] をクリックします。

ステップ 3 エイリアスを作成または更新する接続プロファイルで [編集（Edit）] をクリックします。

ステップ 4 [エイリアス（Aliases）] 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。

ステップ 7 変更を保存します。

関連トピック

接続プロファイルの設定 （29 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。

手順

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、[+] をクリックし、[アクセスインターフェイスの追加（Add Access Interface）] ダイアログボックス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）が有効になり、Cisco Secure Client の AnyConnect VPN モジュールは 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。

SSL 設定と、TLS および DTLS バージョンを指定するには、SSL 設定についてを参照してください。

Cisco Secure Client の AnyConnect VPN モジュールの SSL 設定の設定については、グループポリシーの Secure Clientオプションを参照してください。

- [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。

- [ユーザー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、このチェックボックスをオンにすると、ユーザー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。
- **[HTTP のみの VPN Cookie の有効化（Enable HTTP-only VPN Cookies）]**：ブラウザとその HTTP セッションへの Cookie データのアクセスを制限して、サーバーでのみデータを使用できるようにするには、このチェックボックスをオンにします。このオプションは、クロスサイト スクリプティング攻撃からの保護に役立ちます。

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 **サービスアクセス制御**を設定します。[サービスアクセスオブジェクト（Service Access Object）] ドロップダウンリストからサービス アクセス オブジェクトを選択するか、[+] をクリックして新しいオブジェクトを作成します。

サービス アクセス オブジェクトを使用して、バージョン 7.7 以降の Firewall Threat Defense デバイス上で VPN へのリモート クライアント アクセスを制御できます。このオブジェクトは、VPN 認証の前に、クライアントに対して地理位置情報ベースのアクセス制御を提供します。デフォルトでは、RA VPN はアクセス制御されないため、リモートクライアントは、サービス アクセス オブジェクトで指定されていない限り、任意の地理位置から接続できます。詳細については、地理位置情報に基づくリモートユーザーの VPN アクセスの管理 （93 ページ）およびサービスアクセスオブジェクトの設定を参照してください。

ステップ 9 [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 サーバー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、Secure Firewall Threat Defense デバイスのアクセス コントロール ポリシーの更新 （19 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 10 [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（Interface）

リモートアクセス VPN の高度なオプションの設定

Cisco Secure Client イメージ

Secure Client イメージ

Secure Client は Firewall 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、リモートユーザー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、リモートユーザーは、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、Secure Clientをダウンロードしてインストールすることができます。Firewall 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、ユーザーの認証時に Firewall 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 Secure Client 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。

Secure Firewall 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。ユーザー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 Secure Client イメージファイルをダウンロードします。

関連トピック

Secure Firewall Management Center への Secure Client イメージの追加 （55 ページ）

Secure Firewall Management Center への Secure Client イメージの追加

[Secure Clientファイル（Secure Client File）] オブジェクトを使用して、Secure Client イメージを Secure Firewall 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、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 Secure Client イメージ （54 ページ） を参照してください。

手順

ステップ 1 **Devices** > **VPN** > **Remote Access**、一覧されているリモートアクセスポリシーを選択して編集したら、**[詳細（Advanced）]** タブを選択します。 を選択します。

ステップ 2 [追加（Image）] をクリックして、Secure Client イメージを追加します。

ステップ 3 [Secure Clientイメージ（Secure Client Images）] ダイアログの [使用可能なSecure Clientイメージ（Available Secure Client Images）] 部分で [追加（Add）] をクリックします。

ステップ 4 使用可能な Secure Client イメージの [名前（Name）] と [説明（Description）]（オプション）を入力します。

ステップ 5 [参照（Browse）]をクリックし、アップロードするクライアントイメージを見つけて選択します。

ステップ 6 [保存（Save）] をクリックしてイメージを Firewall Management Center にアップロードします。

クライアントイメージを Secure Firewall Management Center にアップロードすると、イメージのオペレーティングシステム情報が自動的に表示されます。

ステップ 7 クライアントイメージの順序を変更するには、[並べ替えボタンを表示（Show re-order buttons）] をクリックして、クライアントイメージを上下に移動します。

関連トピック

Cisco Secure Client イメージ （54 ページ）

リモートアクセス VPN クライアントの Secure Client 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Secure Client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クライアント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、Secure Firewall 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 Secure Client イメージを更新するのに役立ちます。Secure Client 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 Secure Client イメージ ファイルをダウンロードします。
- Secure Firewall Management Center の Web インターフェイスで、**Objects** > **Object Management** > **VPN** > **Secure Client File**に移動し、新しい [Secure Client] イメージ ファイルを追加します。

手順

ステップ 1 Secure Firewall Management Center Web インターフェイスで、[**Devices** > **VPN** > **Remote Access**] を選択します

ステップ 2 更新するリモートアクセス VPN ポリシーで [編集（Edit）] をクリックします。

ステップ 3 **[詳細（Advanced）]** ドロップダウンメニューから **[AnyConnectクライアントイメージ（AnyConnect Client Images）][Secure Clientイメージ（Secure Client Image）]** を選択し、**[追加（Add）]**をクリックします。

ステップ 4 **[利用可能なSecure Clientイメージ（Available Secure Client 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）] 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 [OK] をクリックします。

ステップ 6 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 Secure Firewall Threat Defense デバイスで新しい Secure Client イメージが更新されます。新しい VPN ユーザーが 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 Secure Client イメージがダウンロードされます。既存の VPN ユーザーの場合、Secure Client イメージは次の VPN セッションで更新されます。

Secure Firewall Management Center への Cisco Secure Client 外部ブラウザパッケージの追加

ローカルディスクにすでに保存されている Secure Client 外部ブラウザパッケージのイメージがある場合は、この手順を使用して、それを Secure Firewall Management Center にアップロードします。外部ブラウザパッケージをアップロードしたら、リモートアクセス VPN 接続用に外部ブラウザパッケージを更新できます。

[Secure Clientファイル（Secure Client File）] オブジェクトを使用して、外部ブラウザパッケージファイルを Secure Firewall Management Center にアップロードできます。詳細については、ファイルオブジェクトを参照してください。

注意事項

- Firewall Threat Defense デバイスに追加できる外部ブラウザパッケージは 1 つだけです。
- 外部ブラウザパッケージが Firewall Management Center に追加された後、リモートアクセス VPN 構成で外部ブラウザが有効になった後にのみ、ブラウザが Firewall Threat Defense にプッシュされます。

手順

ステップ 1 Secure Firewall Management Center Web インターフェイスで、**Devices** > **VPN** > **Remote Access**、一覧されているリモートアクセスポリシーを選択して編集したら、**[詳細（Advanced）]** タブを選択します。 を選択します

ステップ 2 **[Secure Clientイメージ（Secure Client Images）]** ページの **[Secure Client外部ブラウザパッケージ（Secure Client External Browser Package）]** の部分で、[追加（Add）] をクリックします。

ステップ 3 Secure Client パッケージの [名前（Name）] と [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外部ブラウザパッケージを見つけます。

ステップ 5 [保存（Save）] をクリックしてイメージを Secure Firewall Management Center にアップロードします。

（注）
既存の外部ブラウザパッケージを使用してリモートアクセス VPN 接続を更新する場合は、[パッケージファイル（Package File）] ドロップダウンからファイルを選択します。

ステップ 6 リモート アクセス VPN ポリシーを保存します。

関連トピック

Cisco Secure Client イメージ （54 ページ）

リモート アクセス VPN のアドレス割り当てポリシー

Firewall 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、Firewall 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、IPv6 ポリシーを試す必要があります。

- [承認サーバーを使用（Use Authorization Server）]：ユーザーごとに外部承認サーバー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、**Objects** > **Object Management** > **Network** ペインでサーバを構成します。この方法は IPv4 の割り当てポリシーに使用できます。

  DHCP ネットワーク範囲の構成の詳細については、グループ ポリシー一般オプションを参照してください。
- [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、**Objects** > **Object Management** > **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ことを許可（Allow 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。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 （29 ページ）
リモート アクセス VPN 認証 （6 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ー証明書をマッチングするルールを定義できます。証明書マップにより、セキュアゲートウェイでの証明書認証が可能になります。

ルール、または証明書マップは、証明書マップオブジェクトで定義されます。

手順

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）]**を選択します。

ステップ 4 [接続プロファイルマッピングの全般設定（General Settings for Connection Profile Mapping）] ペインから次のオプションを選択します。

選択肢は優先順位に基づいています。最初の選択肢が一致しない場合、オプションリストの次の選択肢が順番にマッチングされます。ルールが満たされたときにマッチングが完了します。ルールが満たされない場合、このページの下部に一覧表示されているデフォルトの接続プロファイルが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が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）]：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、このオプションを有効にします。

（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、リモートユーザー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) [証明書マップ名（Certificate Map Name）] 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 [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。

ユーザー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 承認サーバーがグループ 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） Firewall Threat Defense にグループポリシー属性の継承はありません。ユーザーについては、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 サーバー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 ポリシーがユーザー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 **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 **[詳細設定（Advanced）]** > **[グループポリシー（Group Policies）]** > **[追加（Add）]**を選択します。

ステップ 4 [使用可能なグループポリシー（Available Group Policy）] リストからグループポリシーを選択し、[追加（Add）] をクリックします。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 1 つ以上選択できます。

ステップ 5 [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。

ステップ 6 変更を保存します。

関連トピック

グループ ポリシー オブジェクトの設定

LDAP 属性マッピングの設定

LDAP 属性名により、LDAP ユーザーまたはグループの属性名が、シスコで理解される名前にマッピングされます。この属性マップにより、Active Directory（AD）または LDAP サーバーに存在する属性が、シスコの属性名と同一視されるようになります。任意の標準 LDAP 属性を既知のベンダー指定属性（VSA）にマッピングできます。1 つ以上の LDAP 属性を 1 つ以上の Cisco LDAP 属性にマッピングできます。リモートアクセス VPN 接続の確立中に AD または

LDAP サーバーが Firewall Threat Defense デバイスに認証を返すと、Firewall Threat Defense デバイスは、その情報を使用して、Secure Client が接続を完了する方法を調整できます。

VPN ユーザーにさまざまなアクセス許可や VPN コンテンツを提供する場合は、VPN サーバーでさまざまな VPN ポリシーを設定し、クレデンシャルに基づいてこれらのポリシーセットを各ユーザーに割り当てることができます。これを Firewall Threat Defense で実現するには、LDAP 属性マップを使用して LDAP 認可を設定します。LDAP を使用してグループポリシーをユーザーに割り当てるには、LDAP 属性をマッピングするマップを設定する必要があります。

LDAP 属性マップは、次の 3 つのコンポーネントで構成されます。

- [レルム（Realm）]：LDAP 属性マップの名前を指定します。名前は、選択したレルムに基づいて生成されます。
- [属性名マッピング（Attribute Name Mapping）]：LDAP ユーザーまたはグループの属性名を、シスコで理解される名前にマッピングします。
- [属性値マッピング（Attribute Value Mapping）]：LDAP ユーザーまたはグループの属性の値を、選択した名前マッピングのシスコ属性の値にマッピングします。

LDAP 属性マップで使用されるグループポリシーは、リモートアクセス VPN 構成のグループポリシーのリストに追加されます。リモートアクセス VPN 構成からグループポリシーを削除すると、関連付けられた LDAP 属性マッピングも削除されます。

バージョン 6.4 ～ 6.6 では、FlexConfig を使用してのみ LDAP 属性マップを設定できます。詳細については、「Configure AnyConnect Modules and Profiles Using FlexConfig」を参照してください。

バージョン 7.0 以降では、次の手順を使用できます。

手順

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 **[詳細設定（Advanced）]** > **[LDAP 属性マッピング（LDAP Attribute Mapping）]** をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [LDAP 属性マップの設定（Configure LDAP Attribute Map）] ページで、[レルム（Realm）] を選択して属性マップを設定します。

ステップ 6 [追加（Add）] をクリックします。

複数の属性マップを設定できます。各属性マップについて、名前マップと値マップを設定する必要があります。

（注）
LDAP 属性マップを作成する際は、次のガイドラインに従ってください。

- 1 つの LDAP 属性について少なくとも 1 つのマッピングを設定します。同じ LDAP 属性名を持つ複数のマッピングは許可されません。
- LDAP 属性マップを作成するには、少なくとも 1 つの名前マップを設定します。
- リモートアクセス VPN 構成の接続プロファイルに関連付けられていない LDAP 属性マップは削除できます。
- シスコと LDAP の**両方**の属性名および値について、LDAP 属性マップで正しいスペルと大文字/小文字を使用してください。

a) [LDAP 属性名（LDAP Attribute Name）] を指定し、リストから必要な [シスコ属性名（Cisco Attribute Name）] を選択します。
b) [値マップの追加（Add Value Map）] をクリックし、[LDAP 属性値（LDAP Attribute Value）] と [シスコ属性値（Cisco Attribute Value）] を指定します。

さらに値マップを追加するには、この手順を繰り返します。

ステップ 7 [OK] をクリックして LDAP 属性マップの設定を完了します。

ステップ 8 [保存（Save）] をクリックして LDAP 属性マッピングへの変更を保存します。

例

詳細な例については、「Configure RA VPN with LDAP Authentication and Authorization for FTD」を参照してください。

関連トピック

リモートアクセス VPN の AAA 設定 （32 ページ）
権限および属性のポリシー実施の概要 （8 ページ）

VPN ロード バランシングの設定

VPN ロードバランシングについて

Firewall Threat Defense の VPN ロードバランシングを使用すると、2 つ以上のデバイスを論理的にグループ化し、デバイス間でリモートアクセス VPN セッションを均等に分散できます。VPN ロードバランシングを使用すると、ロードバランシンググループ内のデバイス間で Secure Client VPN セッションが共有されます。

VPN ロードバランシングは、スループットまたはその他の要因を考慮しない単純なトラフィックの分散に基づいています。VPN ロードバランシンググループは、2 つ以上の Firewall Threat Defense デバイスで構成されます。1 つのデバイスがディレクタとして機能し、その他のデバイスはメンバーデバイスとなります。グループのデバイスは、完全に同じタイプである必要はなく、同じソフトウェアバージョンや構成を使用する必要もありません。リモートアクセス VPN をサポートするすべての Firewall Threat Defense デバイスがロードバランシンググループ

に参加できます。Firewall Threat Defense は、Secure Client SAML 認証を使用した VPN ロードバランシングをサポートしています。

VPN ロードバランシング グループ内のすべてのアクティブなデバイスがセッションの負荷を伝送します。VPN ロードバランシングにより、トラフィックはグループ内の最も負荷の少ないデバイスに転送され、負荷はすべてのデバイス間に分散されます。これにより、システム リソースが効率的に使用され、パフォーマンスが向上し、ハイ アベイラビリティが実現されます。

VPN ロードバランシングのコンポーネント

VPN ロードバランシングのコンポーネントは次のとおりです。

- **ロードバランシング グループ**：VPN セッションを共有するための 2 つ以上の Firewall Threat Defense デバイスの仮想グループ。

  VPN ロードバランシング グループは、同じリリースまたは混合リリースの Firewall Threat Defense デバイスで構成できますが、各デバイスでリモートアクセス VPN 構成がサポートされている必要があります。

  VPN ロードバランシングのグループ設定の構成 （64 ページ）およびロードバランシングの追加設定の構成 （65 ページ）を参照してください。

- **ディレクタ**：グループの 1 つのデバイスがディレクタとして機能します。グループ内の他のメンバー間に負荷を分散させ、VPN セッションの提供に参加します。

  ディレクタは、グループ内のすべてのデバイスをモニターし、各デバイスの負荷を追跡して、その負荷に基づいてセッションの負荷を分散します。ディレクタの役割は、1 つの物理デバイスに結び付けられるものではなく、デバイス間でシフトできます。たとえば、現在のディレクタで障害が発生すると、グループ内のメンバーデバイスの 1 つがその役割を引き継いで、すぐに新しいディレクタになります。

- **メンバー**：グループ内のディレクタ以外のデバイスは、メンバーと呼ばれます。ロードバランシングに参加し、リモートアクセス VPN 接続を共有します。

  参加デバイスの設定の構成 （66 ページ）。

VPN ロードバランシングの前提条件

- **証明書**：Firewall Threat Defense の証明書には、接続のリダイレクト先となるディレクタおよびメンバーの IP アドレスまたは FQDN が含まれている必要があります。そうしないと、証明書は信頼できないと見なされます。証明書ではサブジェクト代替名（SAN）またはワイルドカード証明書を使用する必要があります。

- [グループURL（Group URL）]：VPN ロードバランシング グループ IP アドレスのグループ URL を接続プロファイルに追加します。グループの URL を指定すると、ユーザーがログイン時にグループを選択する必要がなくなります。

- [IPアドレスプール（IP Address Pool）]：メンバーデバイスの一意の IP アドレスプールを選択し、メンバーデバイスごとに Firewall Management Center の IP アドレスプールをオーバーライドします。

- ネットワークアドレス変換（NAT）の背後にあるデバイスは、ロードバランシンググループに含めることもできます。

VPN ロード バランシングに関するガイドラインと制限事項

- VPN ロードバランシングはデフォルトでは無効になっています。VPN ロードバランシングは明示的にイネーブルにする必要があります。
- 同じ場所にある Firewall Threat Defense デバイスのみをロードバランシンググループに追加できます。
- ロードバランシンググループには、少なくとも 2 つの Firewall Threat Defense デバイスが必要です。
- Firewall Threat Defense 高可用性のデバイスは、ロードバランシンググループに参加できます。
- ネットワークアドレス変換（NAT）の背後にあるデバイスは、ロードバランシンググループに含めることもできます。
- メンバーまたはディレクタのデバイスがダウンすると、そのデバイスが提供するリモートアクセス VPN 接続が切断されます。VPN 接続を再度開始する必要があります。
- 各デバイスのアイデンティティ証明書には、サブジェクト代替名（SAN）またはワイルドカードが必要です。

VPN ロードバランシングのグループ設定の構成

VPN ロードバランシングを有効にし、ロードバランシンググループのすべてのメンバーに適用できるグループ設定を指定することができます。グループを作成するときに、ロードバランシングの参加設定を指定できます。

手順

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

ステップ 2 更新するリモートアクセス VPN ポリシーで [編集（Edit）] をクリックします。

ステップ 3 **[詳細設定（Advanced）]** > **[ロードバランシング（Load Balancing）]** をクリックします。

ステップ 4 [メンバーデバイス間のロードバランシングを有効にする（Enable Load balancing between member devices）] トグルボタンをクリックして、ロードバランシングを有効にします。
[グループ設定の編集（Edit Group Configuration）] ページが開きます。グループパラメータは、ロードバランシンググループの下のすべてのデバイスに適用されます。

ステップ 5 必要に応じて、[グループIPv4アドレス（Group IPv4 Address）] と [グループIPv6アドレス（Group IPv6 Address）] を指定します。

ここで指定する IP アドレスはロードバランシンググループ全体で使用され、ディレクタは着信 VPN 接続用にこの IP アドレスを開きます。

ステップ 6 ロードバランシンググループの [通信インターフェイス（Communication Interface）] を選択します。[追加（Add）] をクリックして、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追加します。

通信インターフェイスは、ディレクタとメンバーが負荷に関する情報を共有するためのプライベート インターフェイスです。

ステップ 7 ディレクタとグループ内のメンバー間の通信に使用する [UDPポート（UDP Port）] を入力します。デフォルトのポートは 9023 です。

ステップ 8 [IPSec暗号化（IPsec Encryption）] トグルボタンをオンにして、ディレクタとメンバーの間の通信における IPsec 暗号化 を有効にします。

この暗号化を有効にすると、事前共有キーを使用して、ディレクタとメンバーの間に IPsec トンネルが確立されます。

[IPsec暗号化（IPsec Encryption）] オプションを有効にして Firewall Threat Defense デバイスをアップグレードまたはダウングレードする場合、展開の失敗を防ぐために、Firewall Management Center と Firewall Threat Defense の間に設定の不一致がないことを確認してください。

ステップ 9 IPSec 暗号化の [暗号化キー（Encryption Key）] を入力し、暗号化キーを確認します。

ステップ 10 **[OK]** をクリックします。

ロードバランシングの追加設定の構成

VPN ロードバランシングの追加設定には、FQDN および IKEv2 リダイレクトが含まれます。

手順

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

ステップ 2 更新するリモートアクセス VPN ポリシーで [編集（Edit）] をクリックします。

ステップ 3 **[詳細設定（Advanced）]** > **[ロードバランシング（Load Balancing）]** をクリックします。

ステップ 4 まだ有効にしていない場合は、[メンバーデバイス間のロードバランシングを有効にする（Enable Load balancing between member devices）] トグルボタンをオンにして、ロードバランシングを有効にします。

ステップ 5 [設定（Settings）] をクリックします。

ステップ 6 完全修飾ドメイン名を使用したリダイレクトを有効にするには、[IPの代わりにFQDNをピアデバイスに送信する（Send FQDN to peer devices instead of IP）] トグルボタンをオンにします。

デフォルトでは、Firewall Threat Defense は VPN ロードバランシングのリダイレクトで IP アドレスだけをクライアントに送信します。

ステップ 7 [IKEv2リダイレクト（IKEv2 Redirect）] フェーズのいずれかを選択します。

- **[SA認証中のリダイレクト（Redirect during SA authentication）]**
- [SA初期化中のリダイレクト（Redirect during SA initialization）]

ステップ 8 [OK] をクリックします。

ステップ 9 変更を保存します。

参加デバイスの設定の構成

デバイスの参加設定では、デバイスが VPN ロードバランシングでどのように負荷を共有するかを決定します。デバイスでVPNロードバランシングを有効にし、デバイス固有のプロパティを定義することにより、参加するデバイスを設定します。これらの値はデバイスによって異なります。ロードバランシングに参加しているデバイスの優先順位番号を指定できます。優先順位番号が大きいほど、そのデバイスは、他のデバイスよりもディレクタになる可能性が高くなります。ただし、グループのディレクタになるデバイスを選択することはできません。

手順

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

ステップ 2 変更するリモートアクセス VPN ポリシーの横にある [編集（Edit）] をクリックします。

ステップ 3 **[詳細設定（Advanced）]** > **[ロードバランシング（Load Balancing）]** をクリックします。

ステップ 4 まだ有効にしていない場合は、[メンバーデバイス間のロードバランシングを有効にする（Enable Load balancing between member devices）] トグルボタンをオンにして、ロードバランシングを有効にします。

ステップ 5 [デバイスの参加（Device Participation）] 設定を構成します。

[デバイスの参加（Device Participation）] セクションには、選択したリモートアクセス VPN 設定のすべてのターゲットデバイスが一覧表示されます。これらのデバイスは、着信 VPN セッションの負荷を共有するように設定できます。

a) [ロードバランシング（Load Balancing）] トグルボタンをオンにしてデバイスのロードバランシングを有効にし、[編集（Edit）] をクリックします。

b) デバイスの [優先順位（Priority）] を入力します。

デフォルトでは、デバイスの優先順位は 5 に設定されています。1 ～ 10 の番号を選択できます。

c) デバイスが NAT の背後にある場合は、VPN インターフェイスの IP アドレスに [IPv4 NAT] または [IPv6 NAT] アドレスを指定します。

d) [OK] をクリックします。

ステップ 6 [保存（Save）] をクリックして、リモートアクセス VPN ポリシー設定を保存します。

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 （52 ページ）を参照してください。

手順

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）] 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 （67 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）] で、選択した VPN ポリシーの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 （52 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、Secure Client 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一覧表示されます。詳細については、リモート アクセス VPN での IKE ポリシー （70 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。Firewall Threat Defense がサポートしているのは Secure Client IKEv2 クライアントのみです。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 （72 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）] で、選択した VPN ポリシーの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 （52 ページ）を参照してください。

手順

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、[編集（Edit）] をクリックして暗号マップの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 サーバーは、HTTPS（SSL）アクセスを提供します。これにより、Secure Client ダウンローダは、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 サーバーを有効にしない場合、ユーザーは、Secure Client 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、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）] を選択：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。

  （注）
  トラフィックフロー機密保持（TFC）パケットを有効にすると、VPN トンネルがアイドル状態になることが防止されます。そのため、TFC パケットを有効にすると、グループポリシーで設定された VPN アイドルタイムアウトが期待どおりに機能しません。グループ ポリシーの詳細オプションを参照してください。

  - 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（Interface）

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 キー交換）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） Firewall 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とモジュラス 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、1 つの IKE プロポーザルを作成することもできますが、複数の異なるプロポーザルを作成して、最も望ましいオプションに高い優先順位を設定することも検討してください。IKEv2 では、ポリシー オブジェクトは認証の指定は行わず、他のポリシーで認証の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 Secure Client のエンドポイントを接続する場合に、選択した VPN 設定で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 （70 ページ）を参照してください。

（注） Firewall 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。

手順

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）] 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。

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

手順

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。

Cisco Secure Client のカスタマイズ

Management Center を使用して Secure Client のカスタマイズを設定し、VPN ヘッドエンドに展開できます。ユーザーが Secure Client から接続すると、Threat Defense デバイスによりこのカ

スタマイズ設定がエンドポイントに配布されます。管理者は、エンドポイントで次の要素をカスタマイズできます。

表 *5 : Management Center* で使用可能な *Secure Client* のカスタマイズ

カスタマイゼーション	説明	詳細
GUI テキストとメッセージ	Secure Client GUI テキストと情報/エラーメッセージをカスタマイズまたはローカライズします。	Secure Client GUI テキストとメッセージのカスタマイズとローカライズ （76 ページ）
アイコンとイメージ	Secure Client GUI のロゴ、画像、またはアイコンをカスタマイズします。	Secure Client のアイコンと画像のカスタマイズ （78 ページ）
スクリプト	クライアントが VPN セッションを確立または切断するときに、エンドポイントデバイスにスクリプトを展開します。	Secure Client を使用したエンドポイントデバイスでのスクリプトの展開 （80 ページ）
バイナリ	Secure Client API を使用してカスタムアプリケーションを展開します。	Cisco Secure Client API を使用したカスタムアプリケーションの展開 （82 ページ）
カスタム インストーラ トランスフォーム	Secure Client インストーラをカスタマイズします。	Secure Client インストーラのカスタマイズ （83 ページ）
Localized Installer Transforms	クライアントインストーラをローカライズします。	クライアントインストーラのローカライズ （83 ページ）

Secure Client のカスタマイズの注意事項と制約事項

注意事項

- `DfltCustomization` として定義されたオブジェクトに xml ファイルをインポートしていることを確認します。カスタマイゼーション オブジェクトをインポートするとき、Firewall Management Center は XML コードの有効性をチェックします。

  次に例を示します。

  ```
  hostname# import webvpn customization DfltCustomization
  disk0:/csm/defaultcustomizationwebvpn.xml
  ```

- カスタマイズ コマンドを展開する前に、 Windowsの Cisco Secure Client ヘッドエンド デプロイメント パッケージをリモート アクセス VPN ポリシーに追加します。このパッケージは、Windows、 MacOS、または Linux クライアントをサポートする場合に含める必要があります。

一般的な制限事項

- CLI を使用して Threat Defense 上で直接設定された 7.4 以前のカスタマイズがある場合、Management Center は展開時にこれらのカスタマイズを削除します。
- クラスタリングはサポートされません。

表 *6 : Secure Client* のカスタマイズの制約事項

カスタマイゼーション	制限事項

GUI テキストおよびメッセージのカスタマイズ	• このカスタマイズを使用する前に、Secure Client を再起動する必要があります。
	• 右から左に記述する言語はサポートされていません。
	• 一部の文字列はフィールド長がハードコードされているため、GUI で切り捨てられます。
	• 一部のメッセージは、クライアントでハードコードされています。次に例を示します。
	  • ステータスメッセージ（更新中）
	  • 信頼できないサーバーメッセージ
	  • 遅延アップデートメッセージ
	• ローカリゼーションはバージョン固有です。
	管理者が古い Secure Client バージョンのテンプレートに基づいて変換テーブルを作成した場合、新しいメッセージはリモートユーザーには表示されません。管理者は、テーブルに新しいメッセージが含まれるように、最新のテンプレートを変換テーブルとマージする必要があります。マージを実行するには、Gettext などのサードパーティ製のツールを利用できます。

カスタマイゼーション	制限事項
アイコンと画像のカスタマイズ	• このカスタマイズを使用する前に、Secure Client を再起動する必要があります。 • カスタマイゼーション オブジェクト名は、Secure Client GUI ファイル名と一致する必要があります。ファイル名はオペレーティングシステムごとに異なり、大文字と小文字が区別されます。各 OS のファイル名、拡張子、およびサイズの詳細については、Cisco Secure Client 管理者ガイド [英語] を参照してください。 • 画像のサイズが正しくないと適切に表示されません。Management Center または Threat Defense デバイスは、画像のサイズを検証しません。 • MacOS は、Secure Client のイメージとアイコンのカスタマイズをサポートしていません。
カスタマイズされたスクリプトの展開	• Secure Client は、1 つの OnConnect スクリプトおよび 1 つの OnDisconnect スクリプトのみを実行します。ただし、これらのスクリプトが別のスクリプトを起動する場合があります。 • スクリプトは、ユーザーに呼び出し権限がある関数のみを実行できます。 • Start Before Logon（SBL）GUI から OnConnect スクリプトを起動することはできません。
Cisco Secure Client API（バイナリ）を使用したカスタムアプリケーションの展開	• このカスタマイズを使用した後、Management Center に更新されたバージョンの Secure Client を展開すると、クライアントは更新をダウンロードし、カスタム UI を置き換えます。
クライアントインストーラのカスタマイズ	• このカスタマイズは、Windows でのみ使用できます。

Secure Client GUI テキストとメッセージのカスタマイズとローカライズ

Secure Client GUI テキストと情報/エラーメッセージをカスタマイズできます。GUI テキストとすべてのメッセージをカスタマイズして、設定した言語で表示することもできます。

GUI テキストとメッセージのカスタマイズ

GUI テキストまたはメッセージをカスタマイズするには、メッセージファイル内のメッセージを編集します。メッセージを更新して、エラーメッセージに詳細情報を含めることができます。次に例を示します。

- ログインダイアログボックスのラベルを変更します（[パスワード（Password）] を [ドメインパスワード（Domain Password）] に変更するなど）。
- エラーメッセージにサポート連絡先の詳細を追加します。

GUI テキストとメッセージのローカライズ

Threat Defense デバイスは、変換テーブルを使用して、Secure Client に表示されるラベルとユーザーメッセージを翻訳します。ユーザーがリモートアクセス VPN に接続すると、Secure Client はエンドポイントに設定されているロケールを識別し、翻訳ファイルをダウンロードします。Threat Defense デバイスは 128 のロケールをサポートしています。デフォルトでは、Secure Client は英語でインストールされます。

- Cisco Secure Client 5.0 の場合、さまざまな言語のデフォルトのローカリゼーションファイルがアプリケーションに含まれます。
- AnyConnect クライアント 4.x の場合、いくつかの言語のローカリゼーションファイルを Cisco.com からダウンロードして、Management Center にアップロードできます。

Secure Client GUI のテキストおよびメッセージをカスタマイズする方法

始める前に

1 つ以上のリモートアクセス VPN ポリシーを設定します。

手順

ステップ 1 Secure Client パッケージまたは Cisco.com から基本テンプレートまたは翻訳ファイルを取得します（AnyConnect.po など）。

ステップ 2 テキストエディタを使用して、翻訳を追加したり、ラベルやメッセージをカスタマイズしたりします。

ステップ 3 各 **msgid** に対応する **msgstr** 文字列を更新します。

ステップ 4 ファイルを保存します。

ステップ 5 新しい Secure Client のカスタマイズオブジェクトを作成します。

a) **Objects** > **Object Management** > **VPN** > **Secure Client Customization**を選択します。
b) [Secure Clientのカスタマイズの追加（Add Secure Client Customization）] をクリックします。
c) カスタマイズの名前と説明を入力します。
d) [カスタマイズタイプ（CustomizationType）] ドロップダウンリストから、[GUIテキストとメッセージ（GUI Text and Messages）] を選択します。
e) [言語（Language）] ドロップダウンリストから、翻訳を追加する言語を選択します。
f) [参照（Browse）] をクリックし、翻訳ファイルを選択します。サポートされているファイル拡張子は、.po、.mo、および .txt です。

ステップ 6 リモートアクセス VPN ポリシーにカスタマイズを追加します。

a) **Devices** > **VPN** > **Remote Access**を選択します。
b) リモートアクセス VPN ポリシーの編集アイコンをクリックします。
c) [詳細（Advanced）] > [Secure Clientのカスタマイズ（Secure Client Customizations）] > [ローカリゼーション（Localization）] をクリックします。
d) [+] をクリックして翻訳ファイルを選択します。
e) [追加（Add）] をクリックします。
f) [OK] をクリックします。

ステップ 7 **[保存（Save）]** をクリックします。

ステップ 8 これで、[展開（Deploy）] > [展開（Deployment）] を選択し、割り当てたデバイスにポリシーを展開します。変更はポリシーを展開するまで有効になりません。

次のタスク

Secure Client のカスタマイズを確認します。詳細については、「Secure Client のカスタマイズの確認 （84 ページ）」を参照してください。

Secure Client のアイコンと画像のカスタマイズ

Management Center を使用して、Secure Client GUI のロゴ、画像、およびアイコンをカスタマイズできます。

Secure Client GUI のロゴ、画像、およびアイコンをカスタマイズするには、Management Center で Secure Client カスタマイゼーション オブジェクトを作成する必要があります。このカスタマイゼーション オブジェクトの名前は、Secure Client GUI ファイル名と一致している必要があります。ファイル名はオペレーティングシステムごとに異なり、大文字と小文字が区別されます。各 OS のファイル名、拡張子、およびサイズの詳細については、Cisco Secure Client 管理者ガイド [英語] を参照してください。

たとえば、Windows クライアントの企業ロゴを置き換える場合は、`company_logo` という名前のカスタマイゼーション オブジェクトを作成し、リモートアクセス VPN ポリシーに追加する必要があります。カスタマイゼーション オブジェクトに別の名前を使用した場合、Secure Client インストーラによってコンポーネントが変更されません。ただし、独自の実行ファイルを展開して GUI をカスタマイズする場合、カスタマイゼーション オブジェクトに任意の名前を付けることができます。

すべてのイメージファイルの場所：

- Windows：**%PROGRAMFILES%\Cisco\Cisco Secure Client\res**
- Linux：**/opt/cisco/secureclient/resources** または **/opt/cisco/anyconnect/resources**
- macOS：サポート対象外

（注） リモートアクセス VPN 接続が確立すると、ロゴまたは画像がクライアント ディレクトリにダウンロードされます。更新されたロゴまたは画像がクライアントに表示されるように、クライアントを再起動してください。

Secure Client の画像およびアイコンをカスタマイズする方法

始める前に

1 つ以上のリモートアクセス VPN ポリシーを設定します。

手順

ステップ 1 正しい拡張子を使用し、正しいサイズでアイコンまたは画像を作成します。

画像のサイズが正しくないと適切に表示されません。Management Center または Threat Defense デバイスは、画像のサイズを検証しません。

ファイル名、拡張子、およびサイズの詳細については、『Cisco Secure Client Administrator Guide』を参照してください。

ステップ 2 新しい Secure Client のカスタマイズオブジェクトを作成します。

a) **Objects** > **Object Management** > **VPN** > **Secure Client Customization**を選択します。
b) [Secure Clientのカスタマイズの追加（Add Secure Client Customization）] をクリックします。
c) カスタマイズオブジェクトの名前と説明を入力します。

このカスタマイズオブジェクトの名前は、Secure Client GUI ファイル名と一致している必要があります。ファイル名の詳細については、『Cisco Secure Client Administrator Guide』を参照してください。

d) [カスタマイズタイプ（CustomizationType）] ドロップダウンリストから、[アイコンと画像（Icon and Images）] を選択します。
e) [プラットフォーム（Platform）] ドロップダウンリストから、プラットフォームを選択します。
f) [参照（Browse）] をクリックし、ファイルを選択します。サポートされている拡張子は、.png、.ico、および .jpeg です。
g) 手順 2a ～ f を繰り返して、複数のアイコンおよび画像を追加します。

ステップ 3 カスタムオブジェクトをリモートアクセス VPN ポリシーに追加します。

a) **Devices** > **VPN** > **Remote Access**を選択します。
b) リモートアクセス VPN ポリシーの編集アイコンをクリックします。
c) [詳細（Advanced）] > [Secure Clientのカスタマイズ（Secure Client Customizations）] > [アイコンと画像（Icons and Images）] をクリックします。
d) [+] をクリックしてファイルを選択します。

e) [追加（Add）] をクリックします。
f) [OK] をクリックします。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 これで、[展開（Deploy）] > [展開（Deployment）] を選択し、割り当てたデバイスにポリシーを展開します。変更はポリシーを展開するまで有効になりません。

次のタスク

Secure Client のカスタマイズを確認します。詳細については、「Secure Client のカスタマイズの確認 （84 ページ）」を参照してください。

Secure Client を使用したエンドポイントデバイスでのスクリプトの展開

Secure Client では、次のイベントが発生したときに、スクリプトをダウンロードして実行できます。

- Threat Defense による新しいクライアント VPN セッションの確立。このイベントによって起動するスクリプトが OnConnect スクリプトであり、このファイル名プレフィックスが必要です。VPN セッションを再接続しても、このスクリプトは起動しません。
- Threat Defense によるクライアント VPN セッションの切断。このイベントによって起動するスクリプトが OnDisconnect スクリプトであり、このファイル名プレフィックスが必要です。

これらのスクリプトは非同期に実行され、接続の確立または切断を遅らせることはありません。任意の拡張子を指定でき、エンドポイントで実行可能である必要があります。Secure Client は、ファイル名で OnConnect および onDisconnect スクリプトを識別します。ファイル拡張子に関係なく、OnConnect または OnDisconnect で始まるファイルを検索します。

この機能の例をいくつか示します。

- VPN の接続時にグループポリシーを更新する。
- VPN の接続時にネットワークドライブをマウントする。
- VPN の切断時にネットワークドライブをアンマウントする。

スクリプトを有効にするには、VPN プロファイルの [スクリプトの有効化（Enable Scripting）] オプションをオンにします。デフォルトでは、クライアントによってスクリプトが起動することはありません。クライアントは、スクリプトを特定の言語で記述する必要はありません。スクリプトを実行できるアプリケーションをクライアントコンピュータにインストールする必要があります。クライアントでスクリプトを起動するためには、このスクリプトをコマンドラインから実行する必要があります。

Secure Client では、ユーザーがログインして VPN セッションを確立した後でないと、スクリプトを起動できません。Start Before Logon（SBL）GUI から OnConnect スクリプトを起動することはできません。ユーザーのログイン後にスクリプトを起動するには、VPN プロファイルの [Post SBL OnConnectスクリプトを有効にする（Enable Post SBL On Connect Script）] オプション

をオンにする必要があります。Secure Client は 32 ビットアプリケーションです。スクリプトを 64 ビット Windows バージョンで実行すると、32 ビットバージョンの cmd.exe が使用されます。

Secure Client 用にカスタマイズされたスクリプトを追加する方法

始める前に

1. リモートアクセス VPN を設定します。
2. VPN プロファイルでスクリプト化を有効化します。
3. VPN プロファイルをリモートアクセス VPN グループポリシーに追加します。

手順

ステップ 1 プラットフォームの OnConnect および OnDisconnect スクリプトを作成します。

ステップ 2 新しい Secure Client のカスタマイズオブジェクトを作成します。

a) **Objects** > **Object Management** > **VPN** > **Secure Client Customization**を選択します。
b) [Secure Clientのカスタマイズの追加（Add Secure Client Customization）] をクリックします。
c) カスタマイズの名前と説明を入力します。
d) [カスタマイズタイプ（CustomizationType）] ドロップダウンリストから、[スクリプト（Scripts）]を選択します。
e) [プラットフォーム（Platform）] ドロップダウンリストから、プラットフォームを選択します。
f) 次のいずれかを選択します。
   - [接続時（On Connect）]：OnConnect スクリプトを選択します。
   - [切断時（On Disconnect）]：OnDisconnect スクリプトを選択します。
g) [参照（Browse）] をクリックして、エンドポイントで実行するスクリプトを選択します。

ステップ 3 リモートアクセス VPN ポリシーにカスタマイズを追加します。

a) **Devices** > **VPN** > **Remote Access**を選択します。
b) リモートアクセス VPN ポリシーの編集アイコンをクリックします。
c) [詳細（Advanced）] > [Secure Clientのカスタマイズ（Secure Client Customizations）] > [ローカリゼーション（Localization）] をクリックします。
d) [+] をクリックして翻訳ファイルを選択します。
e) [追加（Add）] をクリックします。
f) [OK] をクリックします。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 これで、[展開（Deploy）] > [展開（Deployment）] を選択し、割り当てたデバイスにポリシーを展開します。変更はポリシーを展開するまで有効になりません。

次のタスク

Secure Client のカスタマイズを確認します。詳細については、「Secure Client のカスタマイズの確認 （84 ページ）」を参照してください。

Cisco Secure Client API を使用したカスタムアプリケーションの展開

Windows、Linux、または MacOs マシンの場合、Secure Client API を使用するカスタムクライアントを作成して展開できます。このクライアントのバイナリファイルを使用して、Secure Client GUI または CLI バイナリファイルを置き換えることができます。

実行可能ファイルは、管理センターにインポートしたロゴイメージなどの任意のリソースファイルを呼び出すことができます。独自の実行可能ファイルを展開する場合、リソースファイルに任意のファイル名を使用できます。

次の表に、オペレーティングシステムごとのクライアント実行可能ファイルのファイル名を示します。

表 *7: Secure Client* 実行可能ファイルのファイル名

クライアント OS	クライアント GUI ファイル	クライアント CLI ファイル
Windows	vpnui.exe	vpncli.exe
Linux	vpnui	vpn
MacOS	管理センターの展開ではサポートされていません。ただし、Altiris Agent などの他の手段によって、クライアント GUI を置き換える macOS 用の実行ファイルを展開できます。	vpn

Cisco Secure Client API を使用してカスタムアプリケーションを展開する方法

始める前に

1 つ以上のリモートアクセス VPN ポリシーを設定します。

手順

ステップ 1 Cisco Secure Client API を使用してカスタムアプリケーションを作成します。

ステップ 2 新しい Secure Client のカスタマイズオブジェクトを作成します。

a) **Objects** > **Object Management** > **VPN** > **Secure Client Customization**を選択します。

b) [Secure Clientのカスタマイズの追加（Add Secure Client Customization）] をクリックします。

c) カスタマイズの名前と説明を入力します。

d) [カスタマイズタイプ（CustomizationType）] ドロップダウンリストから、[バイナリ（Binary）]を選択します。
e) [プラットフォーム（Platform）] ドロップダウンリストから、プラットフォームを選択します。
f) [参照（Browse）] をクリックして、カスタムアプリケーションを選択します。

ステップ 3 リモートアクセス VPN ポリシーにカスタマイズを追加します。

a) **Devices** > **VPN** > **Remote Access**を選択します。
b) リモートアクセス VPN ポリシーの編集アイコンをクリックします。
c) [詳細（Advanced）] > [Secure Clientのカスタマイズ（Secure Client Customizations）] > [バイナリ（Binaries）] をクリックします。
d) [+] をクリックして翻訳ファイルを選択します。
e) [追加（Add）] をクリックします。
f) [OK] をクリックします。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 これで、[展開（Deploy）] > [展開（Deployment）] を選択し、割り当てたデバイスにポリシーを展開します。変更はポリシーを展開するまで有効になりません。

Secure Client インストーラのカスタマイズ

クライアント インストーラ プログラムで展開するカスタムトランスフォームを作成して、Secure Client GUI をカスタマイズできます。トランスフォームを Management Center にインポートして、Threat Defense デバイスに展開できます。Threat Defense は、クライアント インストーラ プログラムを使用して、この変換をエンドポイントに展開します。

（注） このカスタマイズは、Windows でのみ使用できます。

クライアントインストーラのローカライズ

Cisco Secure Client のインストーラに表示されるメッセージを翻訳できます。Management Center はトランスフォームを使用して、インストーラに表示されるメッセージを翻訳します。トランスフォームによってインストレーションが変更されますが、元のセキュリティ署名 MSI は変化しません。これらのトランスフォームではインストーラ画面だけが翻訳され、クライアント GUI 画面は翻訳されません。

Cisco Secure Client のすべてのリリースには、ローカライズされたトランスフォームが含まれています。このトランスフォームは、管理者が新しいソフトウェアを含む Cisco Secure Client パッケージをアップロードすると、必ず Management Center にアップロードできます。ローカリゼーション トランスフォームを使用する場合は、新しい Cisco Secure Client パッケージをアップロードする際に、必ず Cisco.com の最新リリースでローカリゼーション トランスフォームをアップデートしてください。

クライアントインストーラのカスタマイズまたはローカライズ方法

始める前に

1 つ以上のリモートアクセス VPN ポリシーを設定します。

手順

ステップ 1 カスタマイズまたはローカライズされたトランスフォームを作成します。

ステップ 2 新しい Secure Client のカスタマイズオブジェクトを作成します。

a) **Objects** > **Object Management** > **VPN** > **Secure Client Customization**を選択します。
b) [Secure Clientのカスタマイズの追加（Add Secure Client Customization）] をクリックします。
c) カスタマイズの名前と説明を入力します。
d) [カスタマイズタイプ（Customization Type）] ドロップダウンリストから、[カスタマイズされたインストーラトランスフォーム（Customized Installer Transform）] または [ローカライズされたインストーラトランスフォーム（Localized Installer Transform）] を選択します。
e) [プラットフォーム（Platform）] ドロップダウンリストから、プラットフォームを選択します。
f) [参照（Browse）] をクリックし、トランスフォームを選択します。

ステップ 3 リモートアクセス VPN ポリシーにカスタマイズを追加します。

a) **Devices** > **VPN** > **Remote Access**を選択します。
b) リモートアクセス VPN ポリシーの編集アイコンをクリックします。
c) [詳細（Advanced）] > [Secure Clientのカスタマイズ（Secure Client Customizations）] > [カスタム インストーラ トランスフォーム（Custom Installer Transforms）] または [ローカライズされたインストーラ トランスフォーム（Localized Installer Transforms）] をクリックします。
d) [+] をクリックしてトランスフォームを選択します。
e) [追加（Add）] をクリックします。
f) [OK] をクリックします。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 これで、[展開（Deploy）] > [展開（Deployment）] を選択し、割り当てたデバイスにポリシーを展開します。変更はポリシーを展開するまで有効になりません。

Secure Client のカスタマイズの確認

展開の検証

展開が完了したら、Management Center で展開を検証します。**Transcript Details** ( ) アイコンをクリックして、カスタマイズ用に生成されたコマンドを確認します。

例

1. 以下の例は、GUI テキストおよびメッセージのカスタマイズの文字変換に関する詳細を示しています：カスタマイズされたプロンプトによる Secure Client en_us のローカリゼーション。

```
import webvpn translation-table AnyConnect language en-us disk0:/AnyConnect_en-us.po
```

2. 以下の例は、カスタマイズされたアイコンおよび画像の文字変換に関する詳細を示しています：Secure Client ロゴの ABC ロゴへのカスタマイズ。

```
import webvpn AnyConnect-customization type resource platform win name company_logo.png
 disk0:/company_logo.png
```

3. 以下の例は、カスタマイズされた OnConnect および OnDisconnect スクリプトのトランスクリプトの詳細を示しています。接続時スクリプトはネットワークドライブをマウントし、切断時スクリプトはネットワークドライブをアンマウントします。

```
import webvpn AnyConnect-customization type binary platform win name
  scripts_OnConnect_mount.bat disk0:/mount.bat
import webvpn AnyConnect-customization type binary platform win name
  scripts_OnDisconnect_unmount.bat disk0:/unmount.bat
```

Threat Defense コマンドを使用したカスタマイズの確認

Threat Defense で次のコマンドを使用して、カスタマイズを確認します。

- **show import webvpn translation-table detailed**：使用可能な変換テーブルが表示されます。

```
HQ-FTD# show import webvpn translation-table detailed
 Translation Tables' Templates:
   AnyConnect           ia4DaAXNSvl5pZboQRGJcs9KMXY=
   customization
 Translation Tables:
   fr                   customization        BWWodsOt1PbvDvYOp8hLb3W7a64=
   ja                   customization        lNvUk1+qTLNZyNrBcApMQPHnm1M=
   ru                   customization        UqyKyUAcjR+xTGUtdiIFnoIiW5U=
```

- **show import webvpn AnyConnect-customization detailed**：Secure Client カスタマイズの詳細情報が表示されます。

```
HQ-FTD# show import webvpn AnyConnect-customization detailed
OEM resources for AnyConnect client:
  linux-64/binary/scripts_OnConnect_conn.sh           w6+n7z80D/8AR+ul2f7DvTmcDTw=
  linux-64/binary/scripts_OnDisconnect_discon.sh      jx5LJC2XBEmEkGeww59CAkszvnI=
  linux-64/resource/company-logo.png                  GsfBDroqGSQEEwuBDS/3DJNVv88=
  win/binary/scripts_OnConnect_mount.bat              dzjfsLYYft/XMlPlzskKl+Wv1bw=
  win/binary/scripts_OnDisconnect_unmount.bat         k6xlKhF1l2IRyJu08+sdYXgKNgM=
  win/resource/company_logo.png                       cmEvxwqvtaS+Pz/6sb9n3NZudS4=
```

Secure Client でのカスタマイズの確認

- Secure Client で、[メッセージ履歴（Message History）] タブをクリックして、カスタマイズがダウンロードされたことを確認します。

  DART ツールを使用して、クライアント側の診断を表示します。

表 *8 : Secure Client* でのカスタマイズの確認

カスタマイゼーション	検証
GUIテキストおよびメッセージのカスタマイズ	• Secure Client の言語ローカリゼーションまたはカスタマイズされたファイルが次の場所にあるかどうかを確認します。 • Windows：%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\l10n\<language-code>\LC_MESSAGES（AnyConnect バージョン 4.9 以前） • Windows：%ProgramData%\Cisco\Cisco Secure Client\l10n\<language-code>\LC_MESSAGES（Secure Client バージョン 5.0 以降） • Mac OS および Linux：/opt/cisco/anyconnect/l10n/<LANGUAGE-CODE>/LC_MESSAGES /opt/cisco/secureclient/l10n/<LANGUAGE-CODE>/LC_MESSAGES • ローカライズまたはカスタマイズされたファイルの内容を確認し、それらにカスタマイズまたはローカライズされた文字列があるかどうかを確認します。例：AnyConnect.mo
画像およびアイコンのカスタマイズ	• Secure Client のカスタマイズされたファイルが次の場所にあるかどうかを確認します。 • Windows：%PROGRAMFILES%\ Cisco\Cisco AnyConnect Secure Mobility Client\res\（AnyConnect バージョン 4.10 以前） • Windows：%PROGRAMFILES%\ Cisco\Cisco Secure Client\UI\res（Cisco Secure Client 5.0 以降） • Linux：/opt/cisco/anyconnect/resources または /opt/cisco/secureclient/resources • カスタマイズされたアイコンまたは画像ファイルの内容を確認します。

カスタマイゼーション	検証

カスタマイズされた OnConnect および OnDisconnect スクリプト	• カスタマイズされたスクリプトが次の場所にあるかどうかを確認します。
	  • Windows：%ProgramData%\Cisco\Cisco Secure Client\Script（Cisco Secure Client 5.0 以降）
	  • Windows：%ProgramData%\Cisco\ Cisco AnyConnect Secure Mobility Client\Script（AnyConnect バージョン 4.9 以前）
	  • Mac OS および Linux：/opt/cisco/anyconnect/script または /opt/cisco/secureclient/vpn/script
	• スクリプトを確認します。

Secure Client 管理 VPN トンネルの設定

管理 VPN トンネルは、VPN ユーザーが VPN に接続しなくても、クライアントシステムの電源が入るたびに社内ネットワークへの接続を提供します。これにより、組織はソフトウェアのパッチと更新でエンドポイントを最新の状態に保つことができます。ユーザーが開始した VPN トンネルが確立されると、管理トンネルは切断されます。

このセクションでは、Firewall Threat Defense での Secure Client 管理 VPN トンネルの設定に関する情報を提供します。Firewall Management Center インターフェイスを使用して Firewall Threat Defense で Secure Client 管理トンネルを設定するには、次の設定が必要です。

- 証明書ベースの認証とグループ URL を使用する**接続プロファイル**。
- **Secure Client 管理 VPN プロファイルファイル**。必要に応じて、グループ URL およびバックアップサーバーを使用してサーバーを設定します。
- 管理 VPN プロファイル、明示的に含まれるネットワークによるスプリットトンネリング、およびクライアント バイパス プロトコルを使用し、バナーがなしの**グループポリシー**。

Secure Client 管理 VPN トンネルを設定する詳細な手順については、Firewall Threat Defense での Secure Client 管理 VPN トンネルの設定 （88 ページ）を参照してください。

Secure Client 管理 VPN トンネルの要件と前提条件

ソフトウェア要件および設定要件

Firewall Management Center Web インターフェイスを使用する Firewall Threat Defense を使用して Secure Client 管理トンネルを設定する前に、次のものが揃っていることを確認します。

- Firewall Threat Defense および Firewall Management Center バージョン 6.7.0 以降を使用していることを確認します。

- Secure ClientSecure Client VPN Web 展開パッケージ 4.7 以降をダウンロードし、Firewall Threat Defense リモートアクセス VPN にアップロードします。
- 接続プロファイルで証明書認証が設定されていることを確認します。
- グループポリシーでバナーが設定されていないことを確認します。
- 管理トンネルグループポリシーのスプリットトンネリング設定を確認します。

証明書の要件

- Firewall Threat Defense にはリモートアクセス VPN の有効な ID 証明書が必要であり、ローカル認証局（CA）からのルート証明書が Firewall Threat Defense に存在する必要があります。
- 管理 VPN トンネルに接続するエンドポイントには、有効な ID 証明書が必要です。
- Firewall Threat Defense の ID 証明書の CA 証明書をエンドポイントにインストールし、エンドポイントの CA 証明書を Firewall Threat Defense にインストールする必要があります。
- 同じローカル CA によって発行された ID 証明書がマシンストア内に存在する必要があります。

  証明書ストア（Windows の場合）および/またはシステムキーチェーン（MacOS の場合）内です。

Secure Client 管理 VPN トンネルの制限事項

- Secure Client 管理 VPN トンネルは証明書認証のみをサポートし、AAA ベースの認証はサポートしていません。
- パブリックまたはプライベートのプロキシ設定はサポートされていません。
- 管理 VPN トンネルが接続されている場合、Secure Client のアップグレードと AnyConnect モジュールのダウンロードはサポートされません。

Firewall Threat Defense での Secure Client 管理 VPN トンネルの設定

手順

ステップ 1 ウィザードを使用してリモートアクセス VPN ポリシー構成を作成します。

リモートアクセス VPN の構成については、新規リモート アクセス VPN 接続の設定 （14 ページ）を参照してください。

ステップ 2 管理 VPN トンネルの接続プロファイル設定を構成します。

（注）

Secure Client 管理 VPN トンネルにのみ使用する新しい接続プロファイルを作成することをお勧めします。

a) 作成したリモートアクセス VPN ポリシーを編集します。
b) 管理 VPN トンネルに使用する接続プロファイルを選択して編集します。
c) **[AAA]** にドロップダウン メニューから、**[認証方式（Authentication Method）]** を選択し、**[クライアント証明書のみ（Client Certificate Only）]** をクリックします。必要に応じて、許可とアカウンティングの設定を構成します。
d) 接続プロファイルの [エイリアス（Aliases）] タブをクリックします。
e) [URLエイリアス（URL Aliases）] の下にある [追加（+）（Add (+)）] をクリックし、接続プロファイルの [URLエイリアス（URL Alias）] をクリックします。
f) [有効（Enabled）] をクリックして、URL を有効にします。
g) [OK] をクリックし、[保存（Save）] をクリックして接続プロファイル設定を保存します。

接続プロファイル設定の詳細については、接続プロファイルの設定 （29 ページ）を参照してください。

ステップ 3 **Secure Client プロファイルエディタを使用して、管理トンネルプロファイルを作成します。**

a) Cisco Software Download Center から Secure Client **VPN Management Tunnel Standalone Profile Editor** をまだダウンロードしていない場合はダウンロードします。
b) VPN ユーザーに必要な設定を使用して管理トンネルプロファイルを作成し、ファイルを保存します。
c) 接続プロファイルで構成したグループ URL を使用して、[サーバーリスト（Server List）] でサーバーを構成します。

プロファイルエディタを使用した管理プロファイルの作成方法の詳細については、*Cisco Secure Client（AnyConnect を含む）管理者ガイド* [英語] を参照してください。

ステップ 4 **管理トンネルオブジェクトを作成します。**

a) Secure Firewall Management Center Web インターフェイスで、**Objects** > **Object Management** > **VPN** > **Secure Client File** に移動します。
b) **[Secure Clientファイルの追加（Add Secure Client File）]** をクリックします。
c) Secure Client ファイルの [名前（Name）] を指定します。
d) [参照（Browse）] をクリックし、保存した管理トンネル プロファイル ファイルを選択します。
e) [ファイルタイプ（File Type）] ドロップダウンをクリックし、**[Secure Client管理VPNプロファイル（Secure Client Management VPN Profile）]** を選択します。
f) [保存（Save）] をクリックします。

（注）
グループポリシーの Secure Client 設定を作成または更新するときに、管理トンネルオブジェクトも作成します。グループポリシーの Secure Clientオプションを参照してください。

ステップ 5 **管理プロファイルをグループポリシーに関連付け、グループポリシー設定を構成します。**

管理トンネル VPN 接続に使用する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に管理 VPN プロファイルを追加する必要があります。ユーザーが接続すると、グループポリシーにすでにマッピングされているユーザー VPN トンネルとともに管理 VPN プロファイルがダウンロードされ、管理 VPN トンネル機能が有効になります。

注意
[バナーなし（No Banner）]：グループポリシー設定でバナーが設定されていないことを確認します。バナー設定は、**[グループポリシー（Group Policy）]** > **[一般設定（General Settings）]** > **[バナー（Banner）]** で確認できます。

a) 管理 VPN トンネル用に作成した接続プロファイルを編集します。
b) **[グループ ポリシーの編集（Edit Group Policy）]** > **[Secure Client]** > **[管理プロファイル（Management Profile）][グループ ポリシーの編集（Edit Group Policy）]**をクリックし、**[AnyConnect] [Secure Client]**を選択します。その後、**[管理プロファイル（Management Profile）]** をクリックします。
c) [管理VPNプロファイル（Management VPN Profile）] ドロップダウンをクリックし、作成した管理プロファイル ファイル オブジェクトを選択します。

（注）
[+] をクリックして、新しい Secure Client 管理 VPN プロファイルオブジェクトを追加することもできます。

d) [保存（Save）] をクリックします。

ステップ 6 グループポリシーにスプリットトンネリングを設定します。

a) **[グループ ポリシーの編集（Edit Group Policy）]**をクリックし、**[全般（General）]** を選択します。そして、**[スプリット トンネリング（Split Tunneling）]** をクリックします。
b) [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）] ドロップダウンから [以下に指定したネットワークをトンネリングする（Tunnel networks specified below）] を選択します。
c) スプリット トンネル ネットワーク リスト タイプとして [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）] を選択し、管理 VPN トンネル経由のトラフィックを許可するために必要なアクセスリストを選択します。
d) [保存（Save）] をクリックして、スプリットトンネリング設定を保存します。

[Secure Client][カスタム属性（Custom Attribute）]

Secure Client 管理 VPN トンネルには、デフォルトでスプリット インクルード トンネリング構成が必要です。スプリットトンネリングを使用してすべてをトンネリングする管理 VPN トンネルを展開するようにグループポリシーで Secure Client カスタム属性を設定する場合、Firewall Management Center 6.7 Web インターフェイスは Secure Client カスタム属性をサポートしていないため、FlexConfig を使用して設定できます。

次に、Secure Client カスタム属性のコマンド例を示します。

```
webvpn
 anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed
anyconnect-custom-data ManagementTunnelAllAllowed true true
group-policy MGMT_Tunnel attributes
 anyconnect-custom ManagementTunnelAllAllowed value true
```

ステップ 7 リモートアクセス VPN ポリシーを展開、検証、およびモニターします。

a) 管理 VPN トンネル構成を Firewall Threat Defense に展開します。

（注）
クライアントシステムは、Firewall Threat Defense リモートアクセス VPN に 1 回接続して、管理トンネル VPN プロファイルをクライアントマシンにダウンロードする必要があります。

b) **[Cisco AnyConnect セキュア モビリティ クライアント（AnyConnect Secure Mobility Client）][セキュア モビリティ クライアント（Secure Mobility Client）]**で Secure Client 管理 VPN トンネルを確認します。そして、**[VPN]** を選択し、**[統計（Statistics）]** をクリックします。

show vpn-sessiondb anyconnect コマンドを使用して、Firewall Threat Defense コマンドプロンプトで管理 VPN セッションの詳細を確認することもできます。

c) Firewall Management Center Web インターフェイスで、[分析（Analysis）] をクリックして、管理トンネルセッション情報を表示します。

関連トピック

接続プロファイルの設定 （29 ページ）
Firewall Threat Defense グループ ポリシー オブジェクト

複数証明書認証

複数証明書ベースの認証を使用すると、Firewall Threat Defense で SSL または IKEv2 EAP フェーズで Secure Client を使用して VPN アクセスを許可するためにユーザーのアイデンティティ証明書を認証することに加えて、マシンまたはデバイス証明書を検証して、デバイスが会社支給のデバイスであることを確認できます。

複数証明書オプションを使用すると、証明書を通じたマシンとユーザー両方の証明書認証が可能になります。このオプションを使用しない場合は、マシンまたはユーザーのいずれかの証明書認証のみを実行できます。両方は実行できません。

複数証明書認証のガイドラインと制限事項

（注） 複数の証明書認証を設定する場合は、Cisco Secure Client のプロファイル設定で **AutomaticCertSelection** の値を true に設定してください。

- 複数証明書認証では、現在、証明書の数が 2 に制限されています。
- Secure Client で、複数証明書認証のサポートが示されている必要があります。そうでない場合、ゲートウェイで従来の認証方法のいずれかが使用されるか、接続に失敗します。

Secure Client バージョン 4.4.04030 以降では、複数証明書ベースの認証がサポートされています。

- Secure Client では、RSA ベースの証明書のみがサポートされています。
- Secure Client 集約認証の間は、SHA256、SHA384、および SHA512 ベースの証明書のみがサポートされています。
- 証明書認証を SAML 認証と組み合わせることはできません。

複数証明書認証の設定

始める前に

複数証明書認証を設定する前に、各 Firewall Threat Defense デバイスの ID 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が設定されていることを確認します。詳細については、証明書マップオブジェクトを参照してください。

手順

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

ステップ 2 リモートアクセス VPN ポリシーを選択し、[編集（Edit）] をクリックします。

（注）
リモートアクセス VPN を設定していない場合は、[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 複数証明書認証を設定するには、接続プロファイルを選択して [編集（Edit）] します。

ステップ 4 [AAA] 設定をクリックし、[認証方式（Authentication Method）] > [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）] を選択します。

（注）
[クライアント証明書と AAA（Client Certificate & AAA）] の認証方式を選択した場合は、[認証サーバー（Authentication Server）] を選択します

ステップ 5 [複数の証明書認証を有効にする（Enable multiple certificate authentication）] チェックボックスを選択します。

ステップ 6 [クライアント証明書からのユーザー名のマッピング（Map username from client certificate）] に 1 つの証明書を選択します。

- [First Certificate]：VPN クライアントから送信されたマシン証明書からユーザー名をマッピングするには、このオプションを選択します。
- [Second Certificate]：クライアントから送信されたユーザー証明書からユーザー名をマッピングするには、このオプションを選択します。

証明書のみの認証が有効になっている場合は、クライアントから送信されたユーザー名が、VPN セッションのユーザー名として使用されます。AAA と証明書の認証が有効になっている場合は、VPN セッションのユーザー名は事前入力オプションに基づいています。

（注）
クライアント証明書のユーザー名が含まれる [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（識別名）全体をユーザー名として使用（Use entire DN (Distinguished Name) as username）] オプションを選択した場合はユーザー 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、ユーザーを拡張証明書認証に使用される接続プロファイル DN ルールと照合するときに識別子として使用できます。

[クライアント証明書とAAA（Client Certificate & AAA）] の認証を選択した場合、[ユーザーログインウィンドウに証明書からユーザー名を事前に入力（Prefill username from certificate on user login window）] オプションを選択すると、ユーザーが Cisco Secure Client の AnyConnect VPN モジュール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ー名を事前に入力されます。

- [ログイン ウィンドウでユーザー名を非表示にする（Hide username in login window）]：セカンダリ ユーザー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ーには表示されず、ユーザーが事前に入力されたユーザー名を変更しないようにします。

ステップ 7 リモートアクセス VPN に必要な AAA 設定と接続プロファイル設定を設定します。

ステップ 8 接続プロファイルとリモートアクセス VPN の設定を保存し、Firewall Threat Defense デバイスに展開します。

関連トピック

リモートアクセス VPN の AAA 設定 （32 ページ）

地理位置情報に基づくリモートユーザーの VPN アクセスの管理

地理位置情報に基づいて、ユーザーのリモートアクセス VPN 接続を管理できます。特定の国または地域からの VPN 接続を許可または拒否するルールを設定することで、コンプライアンス要件を満たし、セキュリティを強化できます。これらのロケーションベースの基準を満たさない接続は、認証Microsoft Entra IDにブロックされ、詳細が、Firewall Management Center（**Devices** > **Troubleshoot** > **Troubleshooting Logs**）に記録されます。

この機能は Secure Client のすべてのバージョンに対応しています。

前提条件

Firewall Threat Defense デバイスはバージョン 7.7.0 以降である必要があります。

地理位置情報に基づくリモートユーザーの VPN アクセスの管理のワークフロー

手順	タスク	詳細情報
1	リモート クライアントに位置情報ベースのアクセス制御を許可するポリシーを定義します。	サービスアクセスオブジェクトの設定
2	ポリシーを使用してリモート アクセス VPN 設定を更新します。	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（52 ページ）
3	デバイスに設定を展開します。	—
4	クライアントを Firewall Threat Defense デバイスに接続した後、次のようにします。 1. **リモートアクセス VPN** ダッシュボードで、アクティブなリモートアクセス VPN セッションを確認します。 2. **Devices** > **Troubleshoot** > **Troubleshooting Logs** で、拒否されたリモートアクセス VPN セッションのログを確認します。	サービス アクセス ポリシーの監視とトラブルシューティング （95 ページ）

地理位置情報に基づいたリモート アクセス VPN ユーザの管理に関するガイドラインと制約事項

注意事項

- サービス アクセス オブジェクトでは、地理位置情報オブジェクト（国、大陸、または地理位置情報オブジェクト）を使用する場合、それを 1 つのルールでだけ使用します。
- これらのルールは並べ直すことができないため、正しい順序でサービス アクセス ルールを設定してください。

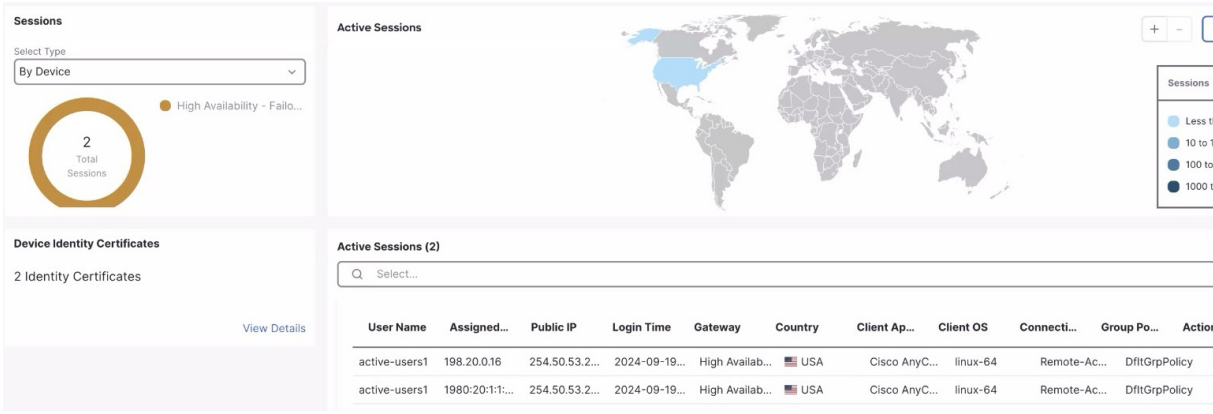
制限事項

- クラスタリングはサポートされません。
- 位置情報ベースの未分類 IP アドレスは、地理的な発信元に応じて分類されません。このような未分類の IP アドレスの場合、Firewall Management Center はデフォルトのサービス アクセス ポリシー アクションを強制します。
- IETF RFC1918 アドレスからの接続は、サービス アクセス ポリシーの設定に関係なく、地理位置情報ベースのリモートアクセス VPN に対して許可されます。

サービス アクセス ポリシーの監視とトラブルシューティング

リモートアクセス VPN ダッシュボードでのアクティブなリモートアクセス VPN セッションの監視

Overview > **Dashboards** > **Remote Access VPN**を選択します。

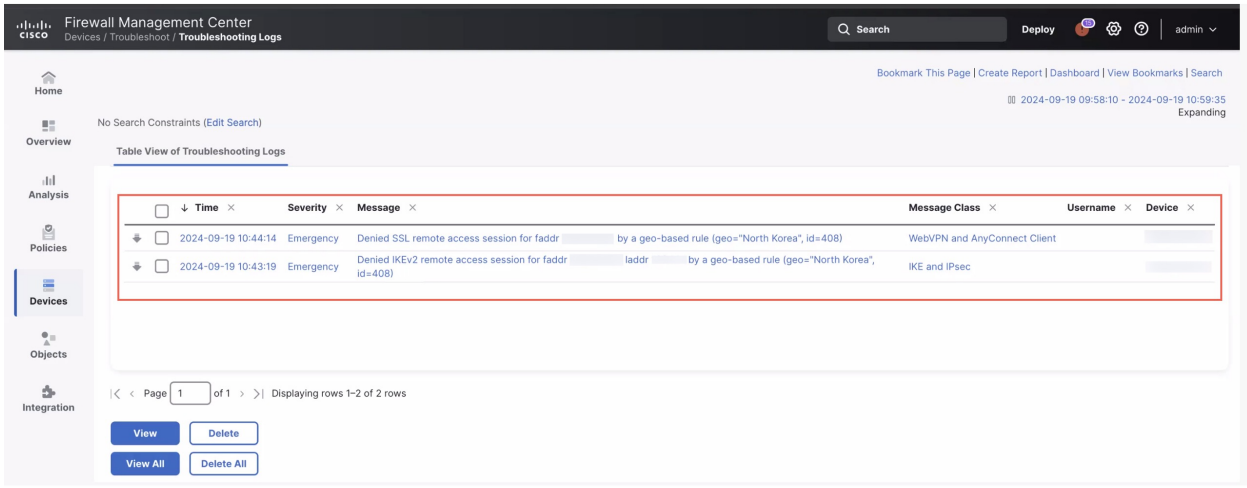


拒否されたリモートアクセス VPN セッションの監視

拒否されたリモートアクセス VPN セッションの **Devices** > **Troubleshoot** > **Troubleshooting Logs** での監視拒否されたリモートアクセス VPN セッションを表示するには、Firewall Threat Defense で syslog 設定を構成する必要があります。

1. **Devices** > **Platform Settings** を選択し、Threat Defense ポリシーを作成するか編集します。
2. 左側のペインで、[Syslog] をクリックします。
3. [ロギングのセットアップ（Logging Setup）] タブをクリックします。
4. [Enable Logging] チェックボックスをオンにします。
5. **[VPN ログ（VPN Logs）]** ラジオボタンをクリックします。
6. **[ロギング レベル（Logging Level）]** ドロップダウン リストから、**[6- 情報（6-informational）]** を選択します。
7. **[保存（Save）]** をクリックします。

（注） **[すべてのログ（All Logs）]** オプションが 0 ～ 2 の **[ロギングレベル（Logging Level）]** で設定されている場合、拒否されたリモートアクセス VPN セッションは表示できません。



サービス アクセスポリシーを確認する

Firewall Threat Defense デバイスの CLI から次のコマンドを実行します。

- **show running-config service-access**：ユーザー定義のサービス アクセス ポリシーを表示します。

```
firepower#show running-config service-access
   service-access deny geolocation OBJGRP_Asia1
   service-access permit interface outside ra-ssl-client geolocation OBJGRP_India
   service-access deny ra-ikev2 geolocation any
```

- **show service-access**：ユーザー定義のサービス アクセス ポリシーの詳細を表示します。

```
firepower# show service-access
1 outside          : ra-ikev2 ra-ssl-client (permit) hits = 8288
  Last hit time    : 10:58:10.038 IST Tue Jul 16 2024
  object-group     : FMC_INTERNAL_XXY
2 any              : ra-ikev2 ra-ssl-client (deny) hits = 123
  Last hit time    : 11:23:12.032 IST Tue Jul 17 2024
  object-group     : any


firepower# show service-access detail
1 outside          : ra-ikev2 ra-ssl-client (permit) hits = 8288
  Last hit time    : 10:58:10.038 IST Tue Jul 16 2024
  object-group     : FMC_INTERNAL_XXY
  geolocation      : Egypt(818) Jordan(400)
                     Iran (Islamic Republic of)(364)
                     Saudi Arabia(682)
```

- **show geodb**：地理位置情報テーブルの詳細を表示します。

  show geodb {**ipv4** | **ipv6** | **counters** | **context**} [**location** *country_name* | **lookup** *ip_address*] [**detail**]

  - **show geodb** {**ipv4** | **ipv6**}：IPv4 または IPv6 アドレス マッピングの総数を表示します。

```
firepower# show geodb ipv4
 Geolocation Table - IPv4
 Total number of mappings available: 532507
```

```
Last geolocation data read time:  17:02:13.000 IST Thu Jul 18 2024
Running geolocation update version: 2024-02-15-019
```

- **show geodb** { **ipv4** | **ipv6** } **location** *country_name* **detail**：IPv4 または IPv6 アドレス マッピングの詳細を表示します。

```
firepower# show geodb ipv4 location Antarctica detail
Geolocation Table - IPv4
id=0x00007fff82c284e0, geo_id=10, hits=0
        range_lower=77.70.176.176, range_upper=77.70.176.183
id=0x00007fff82cca360, geo_id:10, hits=0
     range_lower=79.110.169.69, range_upper=79.110.169.69
Total number of mappings available: 28
```

- **show geodb counters**：アクティブ、許可、および拒否されたセッションの詳細を表示します。

```
firepower# show geodb counters
current   - ongoing sessions
permitted - cumulative permitted sessions
denied    - cumulative denied sessions
Location                current          permitted      denied
Egypt                     0                  0             5
India                     45                 1345          45
```

- **show geodb** { **ipv4** | **ipv6lookup** *ip_address*：特定の IPv4 または IPv6 アドレスの地理位置情報を表示します。

```
firepower# show geodb ipv4 lookup 223.223.128.24
Geolocation of 223.223.128.24 is "India" (356) with id=0x000015114d0aa330
Matching network range: 223.223.128.0 - 223.223.159.255
```

サービス アクセス ポリシーのトラブルシューティング

- **Syslogs**

  リモート アクセス VPN サービス アクセスの syslog を有効にします。

  1. **Devices** > **Platform Settings**を選択します。
  2. プラットフォーム設定ポリシーを作成または編集します。
  3. 左側のペインで、[Syslog] をクリックします。
  4. **[ロギングのセットアップ（Logging Setup）]** タブをクリックし、**[ロギングの有効化（Enable Logging）]** チェックボックスをオンにします。
  5. **[Syslog 設定（Syslog Settings）]** タブをクリックして、サービス アクセス syslog 751031 および 716166 の syslog を有効にします。

- コマンド

  - ユーザー定義のサービス アクセス ポリシーの詳細を表示するには **show running-config service-access** コマンドおよび **show service-access** コマンドを使用します。

- 地理位置情報テーブルの詳細を表示するには、**show geodb** コマンドを使用します。
- **debug geolocation <debug-level>** コマンドを使用して、地理位置情報に関連するデバッグログをキャプチャします。デバッグ レベルは 1（エラー）、2（警告）、3 と 4（情報）、5（デバッグ）、または 255（すべてデバッグ）のいずれかです。
- サービス アクセス ポリシーのヒット カウントなどの地理位置情報テーブルのカウンタをクリアするには、**clear geodb counters** コマンドを使用します。ただし、このコマンドを使用してロケーションの実際の許可カウンタおよび拒否カウンタをクリアすることはできません。これらのカウンタは、デバイスを再起動した後にのみクリアできます。

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 （32 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 ユーザーの認証

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 Firewall 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。

手順

ステップ 1 Secure Firewall Management Center Web インターフェイスで、[**Devices** > **VPN** > **Remote Access**] を選択します

ステップ 2 リモートアクセスポリシーを選択し、[編集（Edit）]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]** > **[認証方式（Authentication Method）]** > **[クライアント証明書のみ（Client Certificate Only）]** をクリックします。

この認証方式では、ユーザー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、ユーザー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ー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ー名を含む [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、それぞれのデフォルト値である [CN（共通名）（CN (Common Name)）] と [組織ユニット（OU）（OU (Organisational Unit)）] が表示されます。[DN全体をユーザー名として使用（Use entire DN as username）] オプションを選択した場合、ユーザー 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、ユーザー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（ユーザー ID）
  - UPN（ユーザー プリンシパル名）
- どの認証方式を選択する場合にも、[ユーザー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 （32 ページ）を参照してください。

ステップ 5 変更を保存します。

関連トピック

接続プロファイルの設定 （29 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 サーバー経由での VPN ユーザー認証の設定

クライアント証明書と認証サーバーの両方を使用するようにリモートアクセス VPN 認証を設定する場合、VPN クライアント認証は、クライアント証明書の検証と AAA サーバー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 Firewall 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する証明書登録オブジェクトを設定します。
- RADIUS サーバー グループ オブジェクトと、このリモートアクセス VPN ポリシー設定で使用する 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 サーバーに Secure Firewall Threat Defense デバイスからアクセスできることを確認します。

手順

ステップ 1 Secure Firewall Management Center Web インターフェイスで、[**Devices** > **VPN** > **Remote Access**] を選択します

ステップ 2 認証を更新するリモートアクセス VPN ポリシーの [編集（Edit）] をクリックするか、[追加（Add）] をクリックして新しい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 ポリシーを作成する場合は、接続プロファイル設定の選択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] に移動し、[認証方式（Authentication Method）] ドロップダウンから、[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]：[認証サーバー（Authentication Server）] に [RADIUS] を選択した場合、デフォルトで許可サーバー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 サーバー（Accounting Server）] を選択します。認証サーバー 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、[許可サーバー（Authorization Server）] と [アカウンティング サーバー（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）]：クライアント証明書を使用してユーザーを認証します。VPN クライアントエンドポイントでクライアント証明書を設定する必要があります。デフォルトでは、ユーザー名はクライアント証明書フィールドの CN および OU からそれぞれ取得されます。クライアントプロファイルの他のフィールドを使用してユーザー名を指定する場合は、[プライマリ（Primary）] フィールドと [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ー名を含む [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全体をユーザー名として使用（Use entire DN as username）] オプションを選択した場合、ユーザー 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、ユーザー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（ユーザー ID）
- UPN（ユーザー プリンシパル名）

- どの認証方式を選択する場合にも、[ユーザー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 （32 ページ）を参照してください。

ステップ 5 変更を保存します。

関連トピック

接続プロファイルの設定 （29 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 ポリシー管理者がリモートアクセス VPN ユーザー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 （32 ページ）を参照してください。

手順

ステップ 1 Secure Firewall Management Center Web インターフェイスで、[**Devices** > **VPN** > **Remote Access**] を選択します

ステップ 2 更新するリモートアクセス VPN ポリシーで [編集（Edit）] 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の [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）] チェックボックスをオンにして、次のいずれかを選択します。

- [ユーザー通知（Notify User）] : パスワードの有効期限が切れる何日前にユーザーに通知するのか、その日数をボックスで指定します。
- [パスワードの有効期限の日にユーザーに通知（Notify user on the day of password expiration）]

ステップ 6 変更を保存します。

関連トピック

接続プロファイルの設定 （29 ページ）

RADIUS サーバー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、ユーザーがアクセスしたサービスやユーザー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、ユーザーセッションの開始時刻と停止時刻、ユーザー名、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 サーバーは設定されたアカウンティングサーバーにユーザーアクティビティをレポートします。RADIUS サーバーはアカウンティングサーバーとして設定できるため、すべてのユーザーアクティビティ情報が Firewall Management Center から RADIUS サーバーに送信されます。

（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 サーバーまたは個別の RADIUS サーバーを使用できます。

始める前に

- 認証要求またはアカウンティングレコードを受診する RADIUS サーバーで RADIUS グループオブジェクトを設定します。詳細については、RADIUS サーバー グループのオプションを参照してください。
- RADIUS サーバーが Firewall Threat Defense デバイスから到達可能であることを確認します。**Devices** > **Device Management** で Secure Firewall Management Center のルーティングを設定し、**Edit** (✎) をクリックします。次に、**[ルーティング（Routing）]** タブをクリックして RADIUS サーバーへの接続を確認します。

手順

ステップ 1 Secure Firewall Management Center Web インターフェイスで、[**Devices** > **VPN** > **Remote Access**] を選択します

ステップ 2 RADIUS サーバーを設定するリモートアクセスポリシーで [編集（Edit）] をクリックするか、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の **[編集（Edit）]** をクリックして、**[AAA]** を選択します。

ステップ 4 [アカウンティングサーバー（Accounting Server）] ドロップダウンから RADIUS サーバーを選択します。

ステップ 5 変更を保存します。

関連トピック

接続プロファイルの設定 （29 ページ）
リモートアクセス VPN の AAA 設定 （32 ページ）

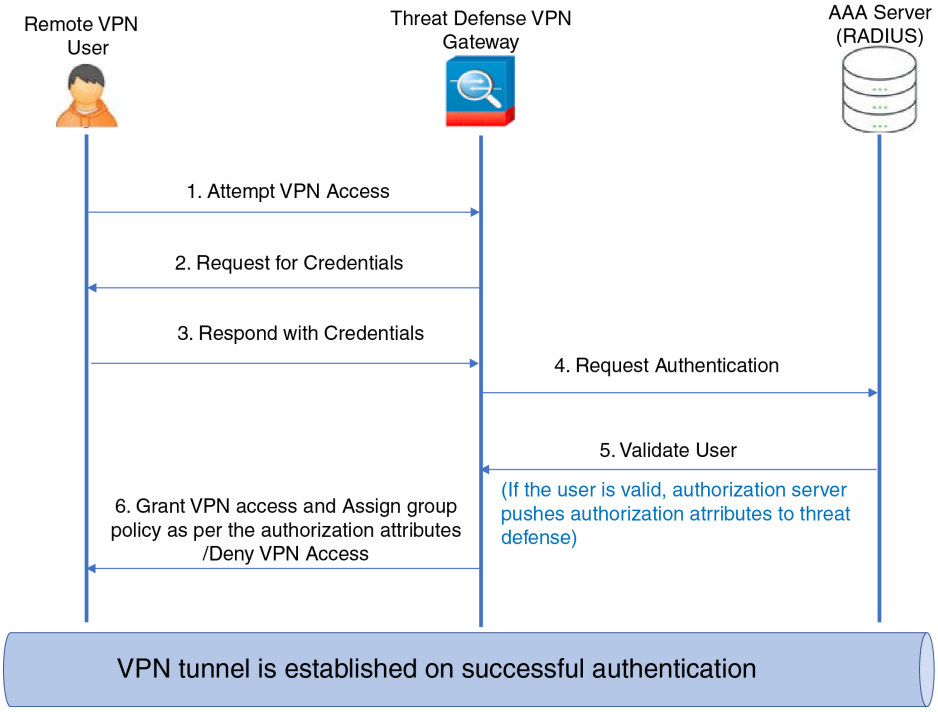
認証サーバーへのグループ ポリシーの選択の委任

ユーザー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）サーバーを設定するか、または現在の接続プロファイルから取得されます。Firewall Threat Defense デバイスが、接続プロファイルで設定されている属性と競合する外部 AAA サーバーから属性を受信した場合は、AAA サーバー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。ユーザーまたはユーザー 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ーに適用されます。

詳細については、『Cisco Identity Services Engine Administrator Guide』の「Configure Standard Authorization Policies」の項およびSecure Firewall Threat Defense の RADIUS サーバー属性 （39 ページ）を参照してください。

図 *1 : AAA* サーバーによるリモート 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 （29 ページ）

許可サーバーによるグループ 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 ユーザーが 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ー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、ユーザーまたはユーザー 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 サーバー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ーに委任できます。ユーザーが認証されると、これらの特定の承認属性が Firewall Threat Defense デバイスにプッシュされます。

始める前に

許可サーバーとして 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。

手順

ステップ 1 Secure Firewall Management Center Web インターフェイスで、[**Devices** > **VPN** > **Remote Access**] を選択します

ステップ 2 リモートアクセスポリシーを選択し、[編集（Edit）] 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、認証サーバーとして 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 サーバーで参照でき、許可サーバー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 Firewall Threat Defense デバイス上に設定を展開します。

ステップ 6 許可サーバーで、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ーにグループ ポリシーを設定すると、そのグループポリシーは、ユーザーが認証された後にリモート アクセス VPN ユーザー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

ユーザー 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ーまたはユーザー 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 サーバー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。

手順

ステップ 1 Secure Firewall Management Center Web インターフェイスで、[**Devices** > **VPN** > **Remote Access**] を選択します

ステップ 2 リモートアクセスポリシーを選択し、[編集（Edit）] 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）] をクリックするか、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、**[ユーザー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、ユーザーまたはユーザー 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 サーバー 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ー/ユーザー グループの許可プロファイルを設定して、ISE または RADIUS サーバー サーバーを設定します。

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 サーバーを承認サーバー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 （29 ページ）

ユーザー 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ーまたはユーザー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、Cisco Secure Client の AnyConnect VPN モジュールを使用して接続するときに選択するユーザーのグループエイリアスや URL が表示されないようにできます。

たとえば、モバイル ユーザー、会社支給のラップトップのユーザー、個人のラップトップのユーザーなど、異なる VPN ユーザー グループに組織が特定の設定を使用する場合は、それらの各ユーザー グループに固有の接続プロファイルを設定し、ユーザーが 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。

Cisco Secure Client の AnyConnect VPN モジュールのデフォルトでは、Firewall Management Center に設定されていて、Firewall 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）のリストが表示されます。カスタム接続プロファイルが設定されていない場合、Cisco Secure Client の AnyConnect VPN モジュールには DefaultWEBVPNGroup 接続プロファイルが表示されます。次の手順を使用して、1 つの接続プロファイルをユーザー グループに適用します。

始める前に

- Secure Firewall 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。証明書からユーザー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 サーバーを設定し、グループ ポリシーを認証サーバーに関連付けます。

手順

ステップ 1 Secure Firewall Management Center Web インターフェイスで、[**Devices** > **VPN** > **Remote Access**] を選択します

ステップ 2 リモートアクセスポリシーを選択し、[編集（Edit）] 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）] を選択し、[ログイン時にユーザー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、Cisco Secure Client の AnyConnect VPN モジュールから接続するユーザーには、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 （29 ページ）

リモートアクセス VPN クライアントの Secure Client プロファイルの更新

Secure Client プロファイルは、Secure Client 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ー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ー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。

プロファイルを作成するには、独立した構成ツールである GUI ベースの Secure Client プロファイルエディタ を使用できます。スタンドアロン プロファイル エディタを使用して、Secure Client プロファイルを新規作成したり、既存の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 Secure Client（AnyConnect を含む）管理者ガイド [英語] の該当するリリースの「Secure Client 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 Firewall 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 （16 ページ）を参照してください。
- Secure Firewall Management Center Web インターフェイスで、**Objects** > **Object Management** > **VPN** > **Secure Client File** に移動し、新しい Secure Client イメージを追加します。

手順

ステップ 1 Secure Firewall Management Center Web インターフェイスで、[**Devices** > **VPN** > **Remote Access**] を選択します

ステップ 2 リモートアクセス VPN ポリシーを選択し、[編集（Edit）] 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）] > **[Secure Client]**> [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）] 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

RADIUS ダイナミック認証

Secure Firewall Threat Defense は、RADIUS サーバーを使用して、ダイナミック アクセス コントロール リスト（ACL）またはユーザーごとの 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ー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 サーバーをサポートするように設定する必要があります。ユーザーが認証を試みる場合、RADIUS サーバーによってダウンロード可能 ACL、または ACL 名が Firewall 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。Secure Firewall 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 サーバーグループの追加
インターフェイス（Interface）
RADIUS ダイナミック認証の設定 （110 ページ）
Secure Firewall Threat Defense の RADIUS サーバー属性 （39 ページ）

RADIUS ダイナミック認証の設定

始める前に：

- RADIUS サーバー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 サーバーでダイナミック認証を機能させるためには、Secure Firewall Threat Defense 6.3 以降が必要です。
- Secure Firewall Threat Defense 6.2.3 以前のバージョンでは、RADIUS サーバー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。
- Firewall Threat Defense ポスチャ VPN は、ダイナミック認証または RADIUS 認可変更（CoA）によるグループポリシーの変更をサポートしていません。

表 *9:* 手順

	操作内容	詳細
ステップ 1	Secure Firewall 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 サーバー オブジェクトを設定します。	RADIUS サーバー グループのオプション
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 サーバー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 Firewall Threat Defense から RADIUS サーバーへの接続を確立します。	RADIUS サーバー グループのオプション Cisco Identity Services Engine (Cisco ISE) アイデンティティ ソースの構成方法
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（16 ページ）
ステップ 5	DNS サーバーの詳細とドメイン 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 （22 ページ） DNS サーバ グループ

	操作内容	詳細
ステップ 6	VNP ネットワーク経由で DNS サーバー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

二要素認証

リモート アクセス VPN に対してニ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、ユーザーはユーザー名とスタティック 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 サーバー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。

Secure Firewall Threat Defense は、2 番目の要素のために RSA トークンと Duo Mobile への Duo Push 認証要求を、二要素認証プロセスの最初の要素としての RADIUS または AD サーバーとの組み合わせでサポートします。

RSA 二要素認証の設定

このタスクの概要：

RADIUS サーバーまたは AD サーバーを RSA サーバーの認証エージェントとして設定し、サーバーをリモートアクセス VPN のプライマリ認証ソースとして Secure Firewall 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、ユーザーは RADIUS または AD サーバーで設定されているユーザー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コ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を設定します。

始める前に：

Secure Firewall 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 サーバー上で以下の操作を実行します。

- RADIUS または Active Directory サーバー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ーに割り当て、トークンをユーザーに配布します。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 サーバー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 サーバーを追加して、共有秘密を指定します。

表 *10* : 手順

	操作内容	詳細
ステップ 1	Secure Firewall 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 サーバー グループを作成します。	RADIUS サーバー 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 サーバー グループのオプション （注） RADIUS または AD サーバーは、RSA サーバーで認証エージェントとして設定されているサーバーと同じである必要があります。 二要素認証の場合は、Secure Client 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（16 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 （32 ページ）

	操作内容	詳細
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。このアプローチでは、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 サーバー（または AD サーバー）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 サーバー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 サーバーと、関連付けられている RADIUS サーバーの両方で設定されたユーザー名を使用してユーザー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 パスコード**。*my-password*,123456 など。
- **push**。my-password,pushなど。push は、ユーザー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**。my-password,smsなど。smsを使用して、新しいパスコードのバッチを含むSMSメッセージをユーザのモバイルデバイスに送信するようにDuoに指示します。**sms** を使用すると、ユーザの認証試行は失敗します。その後、ユーザは再認証し、2 番目の認証ファクタとして新しいパスコードを入力する必要があります。
- phone。my-password,phoneなど。電話機のコールバックを使用して認証するには、**phone** を使用します。

例を含むログインオプションの詳細については、https://guide.duo.com/anyconnect を参照してください。

始める前に：

Firewall 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ユーザー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 Secure Firewall 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 サーバーは RADIUS サーバー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/cisco-firepower#configure-the-proxy 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 サーバーの詳細、Firewall Threat Defense デバイス、Duo プロキシ サーバーの詳細、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 サーバー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 *11* : 手順

	操作内容	詳細
ステップ 1	Secure Firewall 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 サーバー グループを作成します。	RADIUS サーバー グループのオプション
ステップ 3	RADIUS サーバーをホストとして指定して、新しい RADIUS サーバー グループ内に RADIUS サーバー 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 サーバー オプション （注） 二要素認証の場合は、Secure Client 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（16 ページ）

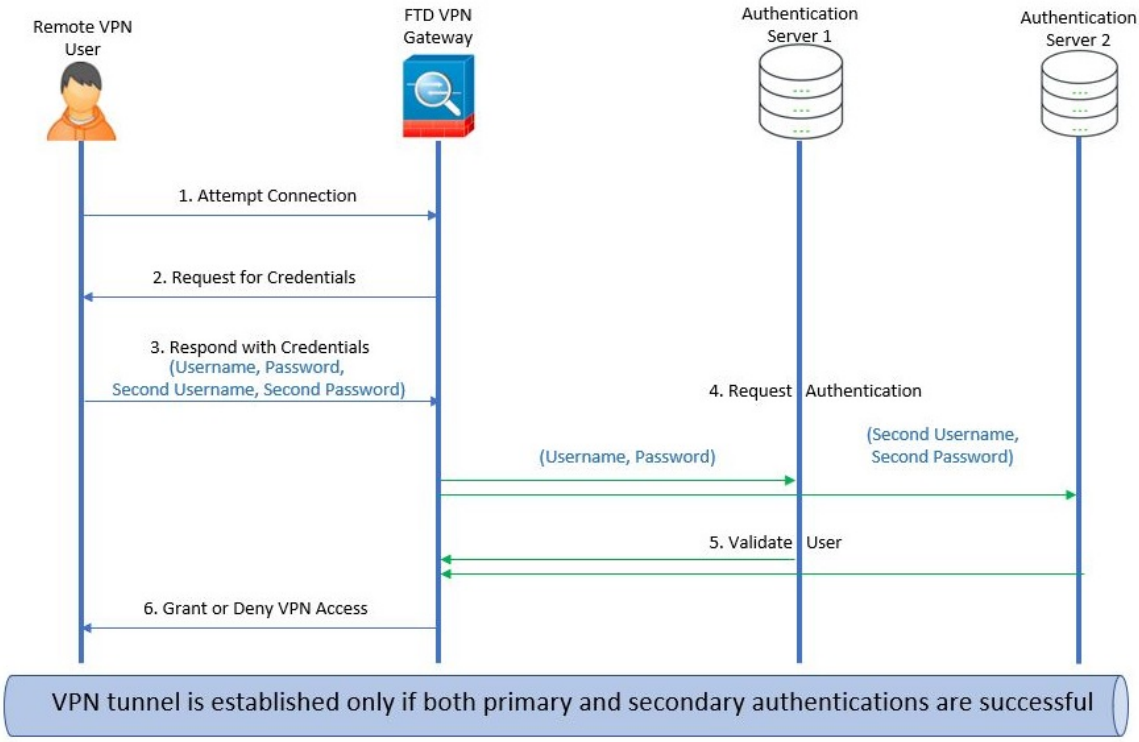
	操作内容	詳細
ステップ 5	認証サーバーとして RADIUS を選択し、Duo プロキシ サーバーを指定して作成した RADIUS サーバー グループを認証サーバーとして選択します。	リモートアクセス VPN の AAA 設定 （32 ページ）
ステップ 7	設定変更を展開します。	設定変更の展開

セカンダリ認証

Secure Firewall 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ーを使用して、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、Secure Client VPN のユーザーは 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。

Secure Firewall 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 *2:* 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 （116 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ー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 サーバー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）サーバーの設定：プライマリおよびセカンダリ認証サーバー、必要な ID 証明書。認証サーバーには、RADIUS サーバー、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 サーバーに Secure Firewall Threat Defense デバイスからアクセスできることを確認します。ルーティングを設定します（**Devices** > **Device Management** で、 **Edit** (✎) をクリックします。次に、**[デバイス（Device）] > [ルーティング（Routing）]**）タブをクリックして AAA サーバーへの接続を確認します。

手順

ステップ 1 Secure Firewall Management Center Web インターフェイスで、**Devices** > **VPN** > **Remote Access** を選択します。

ステップ 2 リモートアクセスポリシーを選択し、[編集（Edit）]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]** > **[認証方式（Authentication Method）]**、[AAA] または [クライアント証明書とAAA（Client Certificate & AAA）] をクリックします。

- [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 サーバーの両方を使用して認証されます。

  - [AAA]：[認証サーバー（Authentication Server）] に [RADIUS] を選択した場合、デフォルトで許可サーバー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 サーバー（Accounting Server）] を選択します。認証サーバー 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、[許可サーバー（Authorization Server）] と [アカウンティング サーバー（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、[ユーザー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ー名とパスワードを Secure Client ログイン画面に入力するには VPN ユーザーが必要です。認証サーバーまたはクライアント証明書からセカンダリ ユーザー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ー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つ目のユーザー名とパスワードのセカンダリ認証のサーバーグループ（AAA サーバー）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ーを LDAP または Active Directory レルムに、セカンダリ認証を RADIUS サーバーに設定できます。

  （注）
  デフォルトでは、セカンダリ認証は必要ありません。

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

  [セカンダリ認証のユーザー名（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ー名とパスワードを入力するようユーザーに要求します。
  - [プライマリ認証ユーザー名を使用（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ーからユーザー名が取得されます。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ー名をマップ（Map username from client certificate）]：クライアント証明書からセカンダリ ユーザー名が事前に入力されます。
    - クライアント証明書のユーザー名を含む [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）全体をユーザー名として使用（Use entire DN (Distinguished Name) as username）] オプションを選択した場合はユーザー 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。

- [ユーザーログインウィンドウに証明書からユーザー名を事前に入力（Prefill username from certificate on user login window）]：ユーザーが Secure Client 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ー名を事前に入力します。
  - [ログイン ウィンドウでユーザー名を非表示にする（Hide username in login window）]：セカンダリ ユーザー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ーには表示されず、ユーザーが事前に入力されたユーザー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 ユーザー名を使用（Use secondary username for VPN session）]：VPN セッション中のユーザー アクティビティのレポートにセカンダリ ユーザー名を使用します。

詳細については、「リモートアクセス VPN の AAA 設定 （32 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 （29 ページ）

SAML 2.0 シングルサインオン認証

SAML シングルサインオン認証について

セキュリティ アサーション マークアップ言語（SAML）は、別のコンテキストでのセッションを使用してアプリケーションにユーザーをログインさせるためのオープンスタンダードです。ユーザーが Active Directory（AD）ドメインまたはイントラネットにログインしている場合、組織はすでにユーザーのアイデンティティを認識しています。このアイデンティティ情報を使用し、SAML を使用して Web ベースのアプリケーションなどの他のアプリケーションにユーザーをログインさせます。個々のアプリケーションはログイン情報を保存する必要がなく、ユーザーは個々のアプリケーションの異なるログイン情報セットを覚えて管理する必要はありません。SAML シングルサインオン（SSO）は、ユーザーのアイデンティティをある場所（アイデンティティ プロバイダー）から別の場所（サービスプロバイダー）に転送することによって機能します。

SAML シングルサインオンとの連携：Secure Firewall Threat Defense

Secure Firewall Threat Defense デバイスは、Secure Client を使用したリモートアクセス VPN 接続で SAML 2.0 シングルサインオン（SSO）認証をサポートします。Secure Firewall Threat Defense で SAML 2.0 SSO を構成するには、次のものが必要です。

- **アイデンティティ プロバイダー（IdP）**：Duo Access Gateway がアイデンティティ プロバイダーとして機能し、ユーザー認証を実行してアサーションを発行します。

- **サービスプロバイダー（SP）**：Firewall Threat Defense デバイスがサービスプロバイダーとして機能し、アイデンティティ プロバイダーから認証アサーションを取得します。
- **VPN クライアント**：Secure Client は、組み込みブラウザを介して SAML 2.0 認証を実行します。

SAML 2.0 に関する注意事項と制約事項

- Firewall Threat Defense は、SAML 認証用に次のシグニチャをサポートしています。
  - RSA および HMAC を使用する SHA1
  - RSA および HMAC を使用する SHA2
- Firewall Threat Defense は、すべての SAML IdP でサポートされる SAML 2.0 Redirect-POST バインディングをサポートしています。
- Firewall Threat Defense は SAML SP としてのみ機能します。ゲートウェイ モードやピア モードでアイデンティティ プロバイダーとして動作することはできません。
- SAML ドメインに一致する AD レルムに関連付けられた ID ポリシーがある場合、SAML 認証ユーザーにアクセスポリシーを適用できます。ただし、Azure AD のテナント ID を Threat Defense デバイス上の関連するレルム ID にマッピングする追加設定が必要となるため、Azure AD SAML では機能しません。
- DAP 評価で使用可能な SAML 認証属性は（AAA サーバーから RADIUS 認証応答で送信される RADIUS 属性と同様に）サポートされていません。Firewall Threat Defense は、DAP ポリシーで SAML 対応グループポリシーをサポートします。ただし、ユーザー名属性は SAML ID プロバイダーによってマスクされるため、SAML 認証の使用中はユーザー名属性を確認できません。
- 認証アサーションが適切に処理され、タイムアウトが適切に機能するように、Firewall Threat Defense の管理者は、Firewall Threat Defense と SAML IdP とのクロック同期を確保する必要があります。
- Firewall Threat Defense の管理者は、次の点を考慮して、Firewall Threat Defense と IdP の両方で有効な署名証明書を保持する責任があります。
  - Firewall Threat Defense に IdP を設定する際には、IdP の署名証明書が必須です。
  - Firewall Threat Defense は、IdP から受け取った署名証明書に対して失効チェックを行いません。
- SAML アサーションには、NotBefore と NotOnOrAfter 条件があります。Firewall Threat Defense SAML に設定されているタイムアウトと、これらの条件との相関関係は次のとおりです。
  - NotBefore とタイムアウトの合計が NotOnOrAfter よりも早い場合は、タイムアウトが NotOnOrAfter に優先します。

- NotBefore + タイムアウトが NotOnOrAfter よりも遅い場合は、NotOnOrAfter が有効になります。
- NotBefore 属性が存在しない場合、Firewall Threat Defense はログイン要求を拒否します。NotOnOrAfter 属性が存在せず、SAML タイムアウトが設定されていない場合、Firewall Threat Defense はログイン要求を拒否します。

- 二要素認証（プッシュ、コード、パスワード）のチャレンジ/応答中に FQDN が変更されるため、Firewall Threat Defense がクライアントとのプロキシを強制的に認証する、内部 SAML を使用した展開では Firewall Threat Defense は Duo と連携しません。
- Secure Client で SAML を使用する場合は、次の注意事項に従ってください。
  - 信頼できないサーバー証明書は、組み込みブラウザでは許可されません。
  - 組み込みブラウザ SAML 統合は、CLI モードまたは SBL モードではサポートされません。
  - Web ブラウザに確立された SAML 認証は Secure Client と共有されず、その逆も同じです。
  - 設定に応じて、組み込みブラウザ搭載のヘッドエンドに接続するときに、さまざまな方法が使用されます。たとえば、Secure Client では IPv6 接続よりも IPv4 接続の方が好ましく、組み込みブラウザでは IPv6 の方が好ましい場合もあります。あるいは、その逆もあります。同じく、プロキシを試して障害が発生したのに Secure Client がどのプロキシにもフォールバックしない場合もあれば、プロキシを試して障害が発生した後で組み込みブラウザがナビゲーションを停止する場合もあります。
  - SAML 機能を使用するためには、Firewall Threat Defense の Network Time Protocol（NTP）サーバーを IdP NTP サーバーと同期する必要があります。
  - 内部 IdP を使用してログインした後に SSO で内部サーバーにアクセスすることはできません。
  - SAML IdP NameID 属性は、ユーザーのユーザー名を特定し、認証、アカウンティング、および VPN セッション データベースに使用されます。
- SAML は Start Before Logon（SBL）をサポートしていません。
- SAML アサーションで受信した複数の属性はサポートされていません。
- ファイアウォールは、Firewall Management Center（**Objects** > **Object Management** > **AAA Server** > **Single Sign-on Server**）で作成したシングル サインオン サーバー オブジェクトの SAML オブジェクト名としてアイデンティティ プロバイダー エンティティ ID を使用します。したがって、1 つのファイアウォールで同じアイデンティティ プロバイダーのエンティティ ID を持つ複数の SAML オブジェクトを使用することはできません。

SAML シングルサインオン認証の設定

始める前に

Firewall Threat Defense リモートアクセス VPN で SAML シングルサインオンを設定する前に、次の作業が完了していることを確認してください。

- Duo でアカウントを作成する。
- Duo Access Gateway をダウンロードしてインストールする。
- SAML アイデンティティ プロバイダー（Duo）から次を取得する。
  - アイデンティティ プロバイダー エンティティ ID URL
  - サインイン URL
  - サインアウト URL
  - アイデンティティ プロバイダー証明書
- SAML シングル サインオン サーバー オブジェクトを作成する。詳細については、シングルサインオンサーバーの追加を参照してください。

（注） リモートアクセス VPN ポリシーウィザードを使用して新しいポリシーを作成する際に、[接続プロファイル（Connection Profile）] 設定でシングル サインオン サーバー オブジェクトを作成できます。

手順

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

ステップ 2 SAML 認証を設定するリモートアクセス VPN ポリシーの横にある [編集（Edit）] をクリックします。新しいポリシーを作成する場合は、[追加（Add）] をクリックします。

ステップ 3 変更する接続プロファイルで [編集（Edit）] をクリックします。

ステップ 4 [AAA] 設定を選択し、[認証方法（Authentication Method）] ドロップダウンから [SAML] を選択します。

ステップ 5 [認証サーバー（Authentication Server）] として、必要な SAML シングルサインオンサーバーを選択します。

ステップ 6 リモートアクセス VPN に必要な設定を指定します。

ステップ 7 Firewall Threat Defense デバイスでリモートアクセス VPN ポリシーを保存および展開します。

関連トピック

リモートアクセス VPN の AAA 設定 （32 ページ）

SAML 認証の設定

SAML 認証について

SAML認証は、AAAおよびダイナミック アクセスポリシー（DAP）フレームワーク内のSAMLアサーションで配信されるユーザー属性をサポートしています。SAMLアサーション属性は、アイデンティティプロバイダーで名前と値のペアとして設定でき、文字列として解析されます。受信された属性は、DAP レコード内で選択基準を定義するときに使用できるように、DAP で使用できるようになります。SAML アサーション cisco_group_policy は、VPN セッションに適用されるグループポリシーを決定するために使用されます。

ダイナミック アクセス ポリシーの属性表現

DAP テーブルでは、DAP 属性は次の形式で表されます。

```
aaa.saml.name = "value”
```

例：aaa.saml.department = ”finance"

この属性は、次のように DAP 選択で使用できます。

```
<attr>
<name>aaa.saml.department</name>
<value>finance</value>
<operation>EQ</operation>
</attr>
```

複数値属性

複数値属性も DAP でサポートされていて、DAP テーブルにインデックスが付けられます。

```
aaa.saml.name.1 = "value”
aaa.saml.name.2 = "value"
```

Active Directory の memberOf 属性

Active Directory（AD）の memberOf 属性には、LDAP クエリによる処理方法と一致する、特別な処理が行われます。

グループ名は、DN の CN 属性によって表されます。

承認サーバーから受信された属性の例：

```
memberOf = "CN=FTD-VPN-Group,OU=Users,OU=TechspotUsers,DC=techspot,DC=us"
 memberOf = "CN=Domain Admins,OU=Users,DC=techspot,DC=us”
```

ダイナミック アクセス ポリシーの属性：

```
aaa.saml.memberOf.1 = "FTD-VPN-Group”
aaa.saml.memberOf.2 = "Domain Admins"
```

cisco_group_policy 属性の解釈

group-policy は、SAML アサーション属性によって指定できます。Firewall Threat Defense が "cisco_group_policy" 属性を受信すると、対応する値を使用して接続 group-policy が選択されます

SAML 認証の設定

始める前に

DUO などのシングルサインオンサーバーを設定し、必要なアイデンティティ プロバイダー（IdP）およびサービスプロバイダー（SP）の設定を完了していることを確認します。

詳細については、SAML 2.0 シングルサインオン認証 （118 ページ）を参照してください。

手順

ステップ 1 シングル サインオン サーバー オブジェクトを構成します（まだ構成していない場合）。

a) **Objects** > **Object Management** > **AAA Server** > **Single Sign-on Server**を選択します。
b) [シングルサインオンサーバーの追加（Add Single Sign-on Server）] をクリックします。
c) シングルサインオンサーバーの詳細を入力して [保存（Save）] をクリックします。

詳細については、シングルサインオンサーバーの追加を参照してください。

ステップ 2 リモートアクセス VPN 接続プロファイルで SAML 認証を設定します。

a) **Devices** > **VPN** > **Remote Access**を選択します。
b) SAML 認証を設定するリモートアクセス VPN ポリシーで [編集（Edit）] をクリックするか、新しいポリシーを作成します。
c) 必要な接続プロファイルを編集し、[AAA] を選択します。
d) [認証サーバー（Authentication Server）] ドロップダウンからシングルサインオン サーバー オブジェクトを選択します。
e) リモートアクセス VPN の設定を保存します。

ステップ 3 DAP ポリシーで SAML 基準を照合します。

a) **Devices** > **VPN** > **Dynamic Access Policy** を選択します。
b) 新しい DAP を作成するか、既存の DAP を編集します。
c) DAP レコードを作成するか、既存のレコードを編集します。
d) **[AAA基準（AAA Criteria）]** > **[SAML基準（SAML Criteria）]** > **[SAML基準の追加（Add SAML Criteria）]** をクリックします。
e) SSO サーバーから返された SAML アサーションに基づいて SAML 基準を作成します。

ステップ 4 リモートアクセス VPN の設定を展開します。

関連トピック

接続プロファイルの設定 （29 ページ）

Firewall Threat Defense グループ ポリシー オブジェクト

拡張 Secure Client 設定

Firewall Threat Defense での Secure Client モジュールの設定

Secure Client は、さまざまな Cisco エンドポイント セキュリティ ソリューションと統合することが可能で、複数の Secure Client モジュールを使ってセキュリティを強化できます。

管理対象ヘッドエンド Firewall Threat Defense を使用して、エンドポイントに Secure Client モジュールを配布して管理できます。ユーザーが Firewall Threat Defense に接続すると、Secure Client と必要なモジュールがエンドポイントにダウンロードされ、インストールされます。

バージョン 6.7 以降では、Firewall Management Center によって管理されるヘッドエンド Firewall Threat Defense を使用して、Secure Client モジュールをエンドポイントに配布して管理できます。その後これらのモジュールは、対応するシスコのエンドポイント セキュリティ ソリューションと統合されます。

バージョン 6.4 ～ 6.6 では、FlexConfig を使用して Firewall Threat Defense でこれらのモジュールとプロファイルを有効にできます。詳細については、「Configure AnyConnect Modules and Profiles Using FlexConfig」を参照してください。

利点

Firewall Threat Defense を使用して Secure Client モジュールをエンドポイントに配布して管理すると、以下のタスクを簡単に実行できます。

- 各エンドポイントでの Secure Client モジュールとプロファイルの配布および管理。
- 各エンドポイントでの Secure Client のアップグレード。

Secure Client モジュールのタイプ

AMP イネーブラ

このモジュールを使用して、エンドポイントに Secure Endpointを展開します。このモジュールは、企業内でローカルにホストされているサーバーからエンドポイントに Secure Endpoint をプッシュします。このモジュールが提供する追加のセキュリティエージェントは、ネットワーク内の潜在的なマルウェア脅威を検出し、検出した脅威を削除して企業を保護します。

Cisco Secure Client 5.0 では、AMP イネーブラは macOS 専用です。Windows 版 Cisco Secure Client は、Cisco Secure Endpoint との完全な統合を提供します。

ISE ポスチャ

このモジュールを使用して、Cisco Identity Services Engine（ISE）を使用してウイルス対策、スパイウェア対策、オペレーティングシステムなどのエンドポイント ポスチャ チェックを実行

し、エンドポイントのコンプライアンスを評価します。ISE は、次世代のアイデンティティおよびアクセス コントロールポリシーを提供します。ISE ポスチャは、クライアント側評価を実行します。クライアントは、ヘッドエンドからポスチャ要件ポリシーを受信し、ポスチャ データ収集を実行し、結果をポリシーと比較し、評価結果をヘッドエンドに返します。

ネットワークの可視性

このモジュールを使用して、ネットワーク可視性モジュールを使用してエンドポイントアプリケーションの使用状況をモニタリングします。潜在的な動作の異常を発見し、情報に基づいたネットワーク設計の意思決定を行うことができます。キャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析に関して、企業内管理者の実行能力を向上させます。使用状況データを Cisco Stealthwatch などの NetFlow 分析ツールと共有できます。

Umbrella ローミングセキュリティ

Cisco Umbrella ローミング セキュリティ サービスを使用した DNS レイヤセキュリティのために、このモジュールを使用できます。Cisco Umbrella はコンテンツフィルタリング、複数ポリシー、強力なレポート、Active Directory の統合などの機能を提供します。

Web セキュリティ

このモジュールを使用して、Cisco Talos を搭載した Cisco Secure Web Appliance（SWA）を有効にします。モジュールは、危険なサイトをブロックし、不明なサイトへのユーザーのアクセスを許可する前にサイトをテストして、エンドポイントを保護します。オンプレミスの WSA またはクラウドベースの Cisco Cloud Web Security のいずれかを介して、Web セキュリティを展開できます。このモジュールは、リリース 4.5 および Secure Client 5.0 の AnyConnect パッケージには含まれていません。

Network Access Manager

このモジュールはセキュアなレイヤ 2 ネットワークを提供し、有線およびワイヤレスネットワークにアクセスするためのデバイス認証を実行します。Network Access Managerは、セキュアなアクセスに必要なユーザおよびデバイス アイデンティティならびにネットワーク アクセス プロトコルを管理します。

Network Access Manager は macOS または Linux には対応していません。

Start Before Login

Start Before Login（SBL）により、ユーザーは Windows へのログイン前に、企業インフラへの VPN 接続を確立できます。SBL モジュールのインストール後、Secure Client VPN プロファイルで SBL を有効にし、リモートアクセス VPN グループポリシーに追加する必要があります。

DART

診断およびレポートツール（DART）はシステムログと他の診断情報を照合して、AnyConnect のインストールと接続の問題をトラブルシュートします。このデータは、トラブルシューティングのために Cisco TAC に送信できます。

6.7 以降のバージョンのデフォルトでは、DART は新しい RA VPN グループポリシーで有効になっていません。6.6 以前のバージョンでは、DART はデフォルトで有効になっています。

フィードバック

カスタマー エクスペリエンス フィードバック（CEF）モジュールにより、使用している、また有効にしたモジュールおよび機能の情報を取得できます。この情報によりユーザーエクスペリエンスを把握できるため、シスコは Secure Client の品質、信頼性、パフォーマンス、ユーザーエクスペリエンスを継続して改善できます。Secure Client は、フィードバックモジュールをエンドポイントにダウンロードしません。フィードバックデータが Cisco フィードバックサーバーに送信されます。

Secure Client モジュールの設定の前提条件

- 使用するモジュールに応じて、関連する製品を設定します。
- Cisco Software Download Center からローカルホストに、以下の Secure Client 関連パッケージをダウンロードします。
  - 必要なプラットフォーム用の Cisco Secure Client ヘッドエンド展開パッケージ。

    このパッケージはヘッドエンド用で、すべての Secure Client モジュールが含まれています。Windows の場合、ファイル名は cisco-secure-client-win-5.0.03076-webdeploy-k9.pkg です。
  - Profile Editor：プロファイルを必要とするモジュールのプロファイルを作成します。

    Secure Client には、一部のモジュールに対して Secure Client プロファイルが必要です。プロファイルには、モジュールを有効にし、対応するセキュリティサービスに接続するための設定が含まれています。Profile Editor は Windows のみをサポートします。

    次の表に、クライアントプロファイルを必要とするモジュールを示します。

Secure Client モジュール	クライアントプロファイルが必要
AMP イネーブラ	対応
ISE ポスチャ	対応
Network Access Manager	対応
ネットワーク可視性モジュール	対応
Umbrella ローミング セキュア モジュール	対応
Feedback	対応
Web セキュリティ	対応
DART	非対応
Start Before Login	いいえ

- ライセンシング
  - 次のいずれかの Secure Client ライセンスが必要です：Secure Client Premier、Secure Client Advantage、または Secure Client VPN Only
  - Firewall Management Center Essentials ライセンスにより、輸出規制機能が許可される必要があります。

    Management Center でこの機能を確認するには、**System (⚙) > Licenses > Smart Licenses** の順に選択します。

Secure Client モジュールの設定に関するガイドライン

- すべての Secure Client モジュールは、AnyConnect 4.8 以降および Secure Client 5.0 でサポートされています。
- 異なるモジュールは、異なるファイル拡張子を持つプロファイルをサポートします。以下の表に、モジュールと、プロファイルのサポートされているファイル拡張子を示します。

表 *12*：サポートされるプロファイルのファイル拡張子

モジュール	ファイル拡張子
AMP イネーブラ	*.xml、*.asp
Feedback	*.xml
ISE ポスチャ	*.xml、*.isp
Network Access Manager	*.xml、*.nsp
ネットワークの可視性	*.xml、*.nvmsp
Umbrella ローミングセキュリティ	*.xml、*.json
Web セキュリティ	*.xml、*.wsp、*.wso

- クライアントモジュールごとに 1 つのエントリのみを追加できます。モジュールのエントリは編集または削除できます。
- ISE ポスチャと Network Access Manager モジュールを使用する場合は、ISE ポスチャモジュールを使用する前に、Network Access Manager をインストールする必要があります。
- Cisco Umbrella ローミング セキュリティ モジュールを有効にする場合は、VPN グループ ポリシーのスプリットトンネリングで [常にトンネル経由でDNS要求を送信する（Always send DNS requests over tunnel）] オプションを無効にしてください。
- SBL を使用する場合は、Secure Client VPN プロファイルで SBL を有効にする必要があります。

Firewall Threat Defense を使用した Secure Client モジュールの取り付け

始める前に

Secure Client モジュールの設定の前提条件 （126 ページ） および Secure Client モジュールの設定に関するガイドライン （127 ページ） トピックを確認してください。

手順

ステップ 1 管理者は、必要に応じて Secure Client モジュールのプロファイルを作成します。

ステップ 2 管理者は、Firewall Management Center を使用して以下を実行します。

a) モジュールを設定し、リモートアクセス VPN グループポリシーにプロファイルを追加します。

b) Firewall Threat Defense に設定を展開します。

ステップ 3 ユーザーは、Secure Client を使用して Firewall Threat Defense への VPN 接続を開始します。

ステップ 4 Firewall Threat Defense はユーザーを認証します。

ステップ 5 Secure Client は更新を確認します。

ステップ 6 Firewall Threat Defense がエンドポイントで Secure Client モジュールとプロファイルを配布します。

次のタスク

Secure Client モジュールのリモートアクセス VPN グループポリシーの設定 （128 ページ）。

Secure Client モジュールのリモートアクセス VPN グループポリシーの設定

Firewall Management Center によって管理される Firewall Threat Defense を使用して、エンドポイントに Secure Client モジュールをインストールして更新するには、Secure Client モジュール設定でリモートアクセス VPN グループポリシーを更新する必要があります。

始める前に

Firewall Management Center でリモートアクセス VPN ポリシーが設定されていることを確認します。

手順

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

ステップ 2 リモートアクセス VPN ポリシーを選択し、[編集（Edit）] 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、[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）] をクリックします。

ステップ 5 [Secure Client] > [AnyConnect] タブをクリックします。

ステップ 6 [クライアントモジュール（Client Modules）] をクリックします。

ステップ 7 [+] をクリックします。

ステップ 8 [Clientモジュール（Client Module）] ドロップダウンリストからモジュールを選択します。

ステップ 9 [ダウンロードするプロファイル（Profile to download）] ドロップダウンリストからモジュールのプロファイルを選択するか、[+] をクリックしてプロファイルを追加します。

ステップ 10 [モジュールのダウンロードの有効化（Enable module download）] チェックボックスをオンにして、エンドポイントにモジュールをダウンロードします。

ステップ 11 [追加（Add）] をクリックします。

ステップ 12 さらにモジュールを追加する場合は、ステップ 7 ～ 11 を繰り返します。

ステップ 13 [保存（Save）] をクリックします。

次のタスク

1. 設定を Threat Defense に展開します。
2. Secure Client を起動し、VPN プロファイルを選択して VPN に接続します。Secure Client は、設定されたモジュールを VPN にインストールします。
3. 設定を確認します。詳細については、「Secure Client モジュール設定の確認（129 ページ）」を参照してください。

Secure Client モジュール設定の確認

（Firewall Threat Defense）

プロファイルと Secure Client モジュールの設定を表示するには、Firewall Threat Defense で以下のコマンドを使用します。

- **show disk0:**：プロファイルとその設定を表示します。
- **show run webvpn**：Secure Client 設定の詳細を表示します。
- **show run group-policy <ravpn_group_policy_name>**：Secure Client の RA VPN グループポリシーの詳細を表示します。
- **show vpn-sessiondb anyconnect**：アクティブな Secure Client VPN セッションの詳細を表示します。

エンドポイントで

1. Secure Client を使用して、Firewall Threat Defense への VPN 接続を確立します。

2. 設定されたモジュールがダウンロードされ、Secure Client の一部としてインストールされているかどうかを確認します。
3. 設定されたプロファイル（存在する場合）が『すべてのオペレーティングシステムに対するプロファイルの場所』で指定されている場所で使用可能かどうかを確認します。

（Firewall Management Center）

リモートアクセス VPN ダッシュボード（**Overview** > **Dashboards** > **Remote Access VPN**）を使用して、Firewall Management Center でアクティブなリモートアクセス VPN セッションをモニターできます。ユーザーセッションに関連する問題をすばやく特定し、ネットワークとユーザーの問題を軽減できます。

モバイルデバイスでのアプリケーションベース（アプリケーションごとの VPN）のリモートアクセス VPN の設定

Secure Client を使用してモバイルデバイスから VPN 接続を確立すると、個人アプリケーションからのトラフィックを含むすべてのトラフィックが VPN 経由でルーティングされます。

Android または iOS で実行されるモバイルデバイスの場合、VPN トンネルを使用するアプリケーションを制限できます。このアプリケーションベースのリモートアクセス VPN は、Per App VPN と呼ばれます。アプリケーションごとの VPN を使用するには、サードパーティの Mobile Device Manager（MDM）アプリケーションをインストールする必要があります。MDM で VPN トンネル経由で使用できる承認済みアプリケーションのリストを定義する必要があります。Firewall Threat Defense ヘッドエンドでアプリケーションごとの VPN を有効にして、MDM がモバイルデバイスにポリシーを適用できるようにできます。

利点

リモートアクセス VPN を承認済みアプリケーションに制限する利点は以下のとおりです。

- パフォーマンス：企業のネットワーク上の VPN トラフィックを制限し、VPN ヘッドエンドのリソースを解放することができます。
- 保護：モバイルデバイス上の未承認の悪意のあるアプリケーションから、企業の VPN トンネルを保護することができます。

Per App VPN トンネルの設定の前提条件とライセンス

前提条件

- サードパーティの Mobile Device Manager（MDM）をインストールして設定します。

  Firewall Threat Defense ヘッドエンドデバイスではなく、MDM 自体の VPN で許可されるアプリケーションを設定する必要があります。

- Cisco Software Download Center から Cisco AnyConnect 企業アプリケーションセレクタをダウンロードします。

  このツールは、Per App VPN ポリシーを定義するために必要です。

ライセンシング

- Secure Client Premier、または Secure Client Advantage。
- Essentials ライセンスにより輸出規制機能が許可される必要があります。

  Firewall Management Centerでこの機能を確認するには、 **System** (⚙) > **Licenses** > **Specific Licenses**を選択します。

モバイルアプリケーションのアプリケーション ID の決定

モバイルデバイスからアプリケーションベースの VPN を許可するように Firewall Threat Defense ヘッドエンドを設定する前に、トンネルで許可するアプリケーションを決定する必要があります。

ユーザーのモバイルデバイスで、MDM にアプリケーションごとのポリシーを設定することを強く推奨します。これにより、ヘッドエンドの設定が簡素化されます。ヘッドエンドで許可されているアプリケーションのリストを設定することにした場合は、エンドポイントのタイプごとに各アプリケーションのアプリケーション ID を決定する必要があります。

iOS でバンドル ID と呼ばれるアプリケーション ID は、逆引き DNS 名です。ワイルドカードとしてアスタリスクを使用できます。たとえば、*. * はすべてのアプリケーションを示し、com.cisco. * はすべてのシスコアプリケーションを示します。

アプリケーション ID を決定するには、次の手順を実行します。

- **Android**：Web ブラウザで Google Play に移動し、アプリカテゴリを選択します。許可するアプリケーションをクリック（またはマウスオーバー）して、URL を確認します。アプリケーション ID は、URL 内の **id=**パラメータに示されます。たとえば、次は Facebook Messenger の URL であるため、アプリケーション ID は com.facebook.orca です。

  https://play.google.com/store/apps/details?id=com.facebook.orca

  独自のアプリケーションなどの Google Play を通じて入手できないアプリケーションの場合は、パッケージ名ビューアアプリケーションをダウンロードして、アプリケーション ID を抽出します。これらの多くの使用可能アプリケーションがあり、そのいずれかが必要なものを提供しますが、シスコはどれも推奨しません。

- **iOS**：バンドル ID を取得する簡単な方法はありません。次の方法で検索できます。

  1. Chrome などのデスクトップの Web ブラウザを使用して、アプリケーション名を検索します。
  2. 検索結果で、Apple App Store からアプリケーションをダウンロードするためのリンクを探します。たとえば、Facebook Messenger は次のようになります。

     https://apps.apple.com/us/app/messenger/id454638411

3. **id** 文字列の後に数値をコピーします。この例では、**454638411** です。
4. 新しいブラウザウィンドウを開き、次の URL の末尾に数値を追加します。

   https://itunes.apple.com/lookup?id=

   この例では、次のとおりです。https://itunes.apple.com/lookup?id=454638411
5. 通常は1.txtという名前のテキストファイルをダウンロードするように求められます。ファイルをダウンロードします。
6. ワードパッドなどのテキストエディタでファイルを開き、bundleId を検索します。次に例を示します。

   "bundleId":"com.facebook.Messenger"

   この例では、バンドル ID は「com.facebook.Messenger」です。これをアプリケーション ID として使用します。

アプリケーション ID のリストを取得したら、 で説明されているように、ポリシーを設定できます。

アプリケーションベースの VPN トンネルの設定

MDM ソフトウェアをインストールして設定したら、Firewall Threat Defense ヘッドエンドデバイスでアプリケーションベースの VPN を有効にできます。ヘッドエンドで有効にすると、MDM ソフトウェアは、VPN を介して企業のネットワークにトンネリングされるアプリケーションを制御します。

始める前に

- Firewall Management Center にリモートアクセス VPN ポリシーがあることを確認します。
- MDM を使用してアプリケーションごとの VPN を設定し、各デバイスを MDM サーバーに登録します。
- Cisco AnyConnect 企業アプリケーション セレクタ ツールをダウンロードします。

手順

ステップ 1 Cisco AnyConnect 企業アプリケーションセレクタを使用して、Per App VPN ポリシーを定義します。

単純な**すべて許可**のポリシーを作成し、MDM で許可するアプリケーションを定義することを推奨します。ただし、アプリケーションのリストを指定して、ヘッドエンドからリストを許可および制御できます。特定のアプリケーションを含める場合は、一意の名前とアプリケーションのアプリケーション ID を使用して、アプリケーションごとに個別のルールを作成します。アプリケーション ID 取得の詳細については、「モバイルアプリケーションのアプリケーション ID の決定」を参照してください。

AnyConnect 企業アプリケーションセレクタを使用して Android と iOS の両方のプラットフォームをサポートする**すべて許可**のポリシーを作成するには、次の手順を実行します。

a) プラットフォームタイプとして、ドロップダウンリストから [Android] を選択し、以下のオプションを設定します。

- [フレンドリ名（Friendly Name）]：ポリシーの名前を入力します。たとえば、Allow_All とします。
- [アプリケーションID（App ID）]：*.* と入力して、使用可能なすべてのアプリケーションと一致させます。
- 他のオプションはそのままにします。

b) プラットフォームタイプとして、ドロップダウンリストから [iOS] を選択し、以下のオプションを設定します。

- [フレンドリ名（Friendly Name）]：ポリシーの名前を入力します。たとえば、Allow_All とします。
- [アプリケーションID（App ID）]：*.* と入力して、使用可能なすべてのアプリケーションと一致させます。
- 他のオプションはそのままにします。

c) [ポリシー（Policy）]>[ポリシーの表示（View Policy）] を選択して、ポリシーの base64 でエンコードされた文字列を取得します。

この文字列には、Firewall Threat Defense がポリシーを確認できるようにする、暗号化された XML ファイルが含まれています。この値をコピーします。この文字列は、Firewall Threat Defense でアプリケーションごとの VPN を設定するときに必要になります。

ステップ 2 Firewall Management Center を使用して、Firewall Threat Defense ヘッドエンドデバイスでアプリケーションごとの VPN を有効にします。

a) **Devices** > **VPN** > **Remote Access**を選択します。
b) リモートアクセス VPN ポリシーを選択し、[編集（Edit）] をクリックします。
c) 接続プロファイルを選択し、[編集（Edit）] をクリックします。
d) [グループポリシーの編集（Edit Group Policy）] をクリックします。
e) [Secure Client] > [AnyConnect] タブをクリックします。
f) [カスタム属性（Custom Attributes）] をクリックし、[+] をクリックします。
g) [Secure Client属性（Secure Client Attribute）] > [AnyConnect] > [属性（Attribute）] ドロップダウンリストから [Per App VPN] を選択します。
h) [カスタム属性オブジェクト（Custom Attribute Object）] ドロップダウンリストからオブジェクトを選択するか、[+] をクリックしてオブジェクトを追加します。

アプリケーションごとの VPN に新しいカスタム属性オブジェクトを追加する場合は、Cisco AnyConnect Enterprise Application Selector から名前、説明、および base64 でエンコードされたポリシー文字列を入力します。

i) **[Save（保存）]** をクリックします。
j) [追加（Add）] をクリックし、[保存（Save）] をクリックします。

ステップ 3 Firewall Management Center に変更を展開します。

次のタスク

1. Secure Client を起動し、VPN プロファイルを選択して、VPN に接続します。
2. 設定を確認します。詳細については、「アプリケーションごとの設定の確認 （134 ページ）」を参照してください。

アプリケーションごとの設定の確認

（Firewall Threat Defense）

アプリケーションごとの設定を確認するには、Firewall Threat Defense で以下のコマンドを使用します。

- **show run webvpn**
- **show run group-policy <ravpn_group_policy_name>**
- **show run anyconnect-custom-data**

エンドポイントで

エンドポイントが Firewall Threat Defense との VPN 接続を確立したら、以下の手順を実行します。

1. Secure Client の [統計（Statistics）] アイコンをクリックします。
2. [トンネルモード（Tunnel Mode）] は、[すべてのトラフィックをトンネリング（Tunnel All Traffic）] ではなく [アプリケーショントンネル（Application Tunnel）] になります。
3. [トンネリングされたアプリケーション（Tunneled Apps）] には、MDM でトンネリングを有効にしたアプリケーションがリストされます。

リモート アクセス VPN の例

ユーザーあたりの Secure Client 帯域幅を制限する方法

ここでは、ユーザーが Secure Client を使用して Secure Firewall 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 ユーザー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。Firewall 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、単一のユーザーやグループまたは複数のユーザー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、Firewall Threat Defenseは超過した分のトラフィックをドロップします。

手順	操作内容	詳細
1	レルムを作成および設定します。	LDAP レルムまたは Active Directory（AD）レルムおよびレルムディレクトリを作成する
2	新しく作成したレルムで利用可能なユーザーまたはグループの QoS ポリシーおよび QoS ルールを作成します。	• QoS ポリシーの作成については、QoS ポリシーの作成 を参照してください。 • QoS ルールの作成については、QoS ルールの設定 を参照してください。
3	リモートアクセス VPN ポリシーを設定し、ユーザー認証用に新しく作成したレルムを選択します。	新しいリモート アクセス VPN ポリシーの作成（16 ページ）
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

ユーザー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

手順	操作内容	詳細
1	レルムを作成および設定します。	LDAP レルムまたは Active Directory（AD）レルムおよびレルムディレクトリを作成する。
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の作成については、アイデンティティ ポリシーの作成を参照してください。 • アイデンティティルールの作成については、アイデンティティ ルールの作成を参照してください。
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。	アクセス制御への他のポリシーの関連付け
4	リモートアクセス VPN ポリシーを設定し、ユーザー認証用に新しく作成したレルムを選択します。	新しいリモート アクセス VPN ポリシーの作成（16 ページ）

手順	操作内容	詳細
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

Firewall Threat Defense 複数証明書認証の設定

複数証明書ベースの認証

複数証明書ベースの認証により、Firewall Threat Defense はマシンまたはデバイスの証明書を検証できます。リモートアクセス VPN 接続プロファイルでは、証明書ベースの認証に対して複数の証明書を有効にでき、AAA 認証と組み合わせることができます。リモートアクセス VPN 接続プロファイルで複数証明書オプションを使用すると、証明書を介したマシンとユーザーの両方の証明書認証が可能になり、デバイスが企業支給のデバイスであることを確認し、ユーザーのアイデンティティ証明書を認証して RA VPN アクセスを許可できます。管理者は、セッションのユーザー名の取得元（マシン証明書またはユーザー証明書）を選択できます。

複数証明書ベースの認証が設定されている場合、VPN クライアントから 2 つの証明書が取得されます。

- [最初の証明書（First Certificate）]：エンドポイントを認証するためのマシン証明書。
- [2番目の証明書（Second Certificate）]：VPN ユーザーを認証するためのユーザー証明書。

Firewall Threat Defense 証明書の詳細については、Firewall Threat Defense 証明書を管理するを参照してください。

制限事項

- 複数証明書認証では、現在、証明書の数が 2 に制限されています。
- Secure Client では、RSA ベースの証明書のみがサポートされています。
- Secure Client 集約認証の間は、SHA256、SHA384、および SHA512 ベースの証明書のみがサポートされています。
- 証明書認証を SAML 認証と組み合わせることはできません。

証明書からのユーザー名事前入力

ユーザー名事前入力オプションを使用すると、証明書のフィールドを解析して、後続の AAA 認証（プライマリまたはセカンダリ）に使用できます。認証に 2 つの証明書を使用する場合、管理者は、事前入力機能のためにユーザー名を取得する必要がある証明書を選択できます。デフォルトでは、事前入力のユーザー名は、ユーザー証明書（Secure Client から受信する 2 番目の証明書）から取得されます。証明書のみの認証方式が有効になっている場合、事前入力されたユーザー名が VPN セッションのユーザー名として使用されます。AAA と証明書の認証が有効になっている場合は、VPN セッションのユーザー名は事前入力オプションに基づいています。

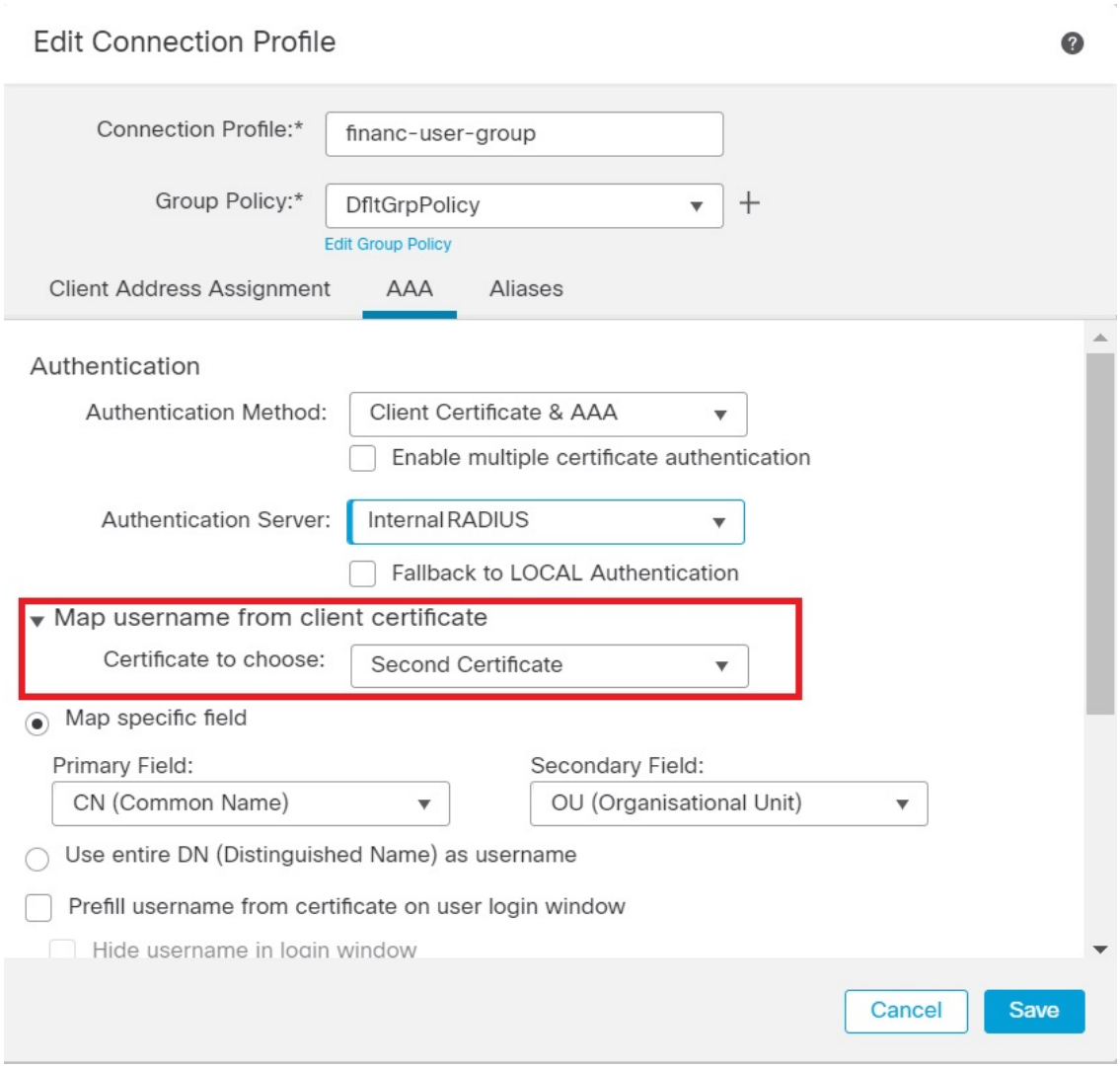
リモートアクセス VPN の複数証明書認証の設定

1. Secure Firewall Management Center Web インターフェイスで、[**Devices** > **VPN** > **Remote Access**] を選択します
2. 既存のリモートアクセスポリシーを編集するか、新しいポリシーを作成してから編集します。

   新しいリモート アクセス VPN ポリシーの作成 （16 ページ）を参照してください。
3. 複数証明書認証を設定するには、接続プロファイルを選択して [編集（Edit）] をクリックします。

   接続プロファイルの設定 （29 ページ）を参照してください。
4. [AAA] を選択してから、[認証方式（Authentication Method）] を選択します。

図 *3*:



- [クライアント証明書のみ（Client Certificate Only）]：ユーザー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、ユーザー名はクライアント証明書フィールドの CN および OU からそれぞれ取得されます。クライアント証明書の他のフィールドにユーザー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ピングします。
- [クライアント証明書とAAA（Client Certificate & AAA）]：ユーザーは、AAA とクライアント証明書の両方の認証タイプを使用して認証されます。

5. [複数の証明書認証を有効にする（Enable multiple certificate authentication）] を選択します。
6. [クライアント証明書からのユーザー名のマッピング（Map username from client certificate）] を選択し、[選択する証明書（Certificate to choose）] ドロップダウンから証明書を選択して、VPN セッションのユーザー名をマシン証明書またはユーザー証明書から選択します。
   - [最初の証明書（First Certificate）]：マシン証明書からのユーザー名をマッピングします。
   - [2番目の証明書（Second Certificate）]：VPN ユーザーを認証するためにユーザー証明書からのユーザー名をマッピングします。
7. 必要な接続プロファイル設定およびリモートアクセス VPN 設定を設定します。
8. 接続プロファイルおよびリモートアクセス VPN ポリシーを保存します。リモートアクセス VPN ポリシーを Firewall Threat Defense に展開します。

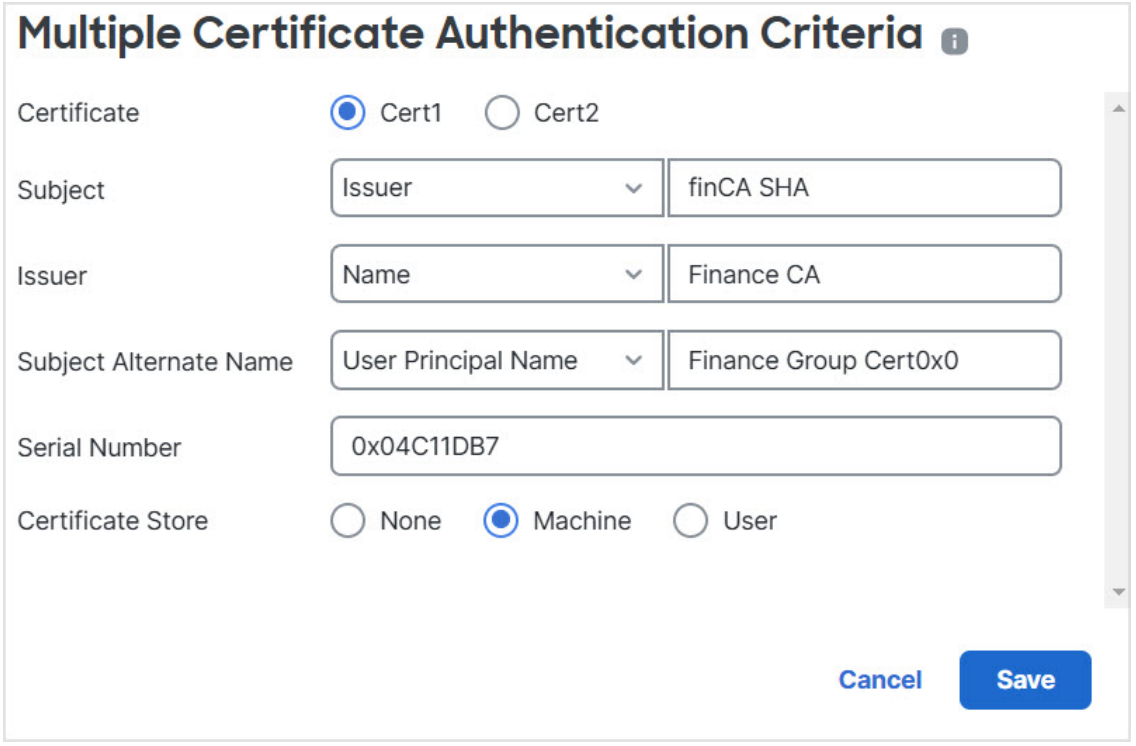
リモートアクセス VPN AAA 設定の詳細については、リモートアクセス VPN の AAA 設定 （32 ページ）を参照してください。

DAP での証明書の設定

DAP レコードで証明書基準属性を設定することもできます。複数証明書認証中に VPN クライアントから受信したユーザーおよびマシンの証明書はダイナミック アクセス ポリシー（DAP）にロードされるため、証明書のフィールドに基づいてポリシーを設定できます。接続試行を認証するために使用された証明書のフィールドに基づいてポリシーを決定できます。

1. **Devices** > **VPN** > **Dynamic Access Policy**を選択します。
2. 既存の DAP ポリシーを編集するか、新しい DAP ポリシーを作成してからポリシーを編集します。
3. 既存の DAP レコードを選択するか、新しい DAP レコードを作成してからレコードを編集します。
4. **[エンドポイント基準（Endpoint Criteria）]** > **[証明書（Certificate）]**を選択します。
5. 一致基準 [すべて（All）] または [任意（Any）] を選択します。
6. [追加（Add）] をクリックして、証明書属性を追加します。

図 *4*:



7. 証明書、[Cert1] または [Cert2] を選択します。
8. [サブジェクト（Subject）] を選択し、証明書のサブジェクト値を指定します。
9. [発行者（Issuer）] を選択し、証明書の発行者名を指定します。
10. [サブジェクト代替名（Subject Alternate Name）] を選択し、サブジェクトの代替名を指定します。
11. [シリアル番号（Serial Number）] を指定します。
12. [証明書ストア（Certificate Store）] を選択します（[なし（None）]、[マシン（Machine）]、または [ユーザー（User）]）。

    このオプションでは、エンドポイントで証明書が選択されたストアを確認する条件を追加します。
13. [保存（Save）] をクリックして、証明書条件の設定を完了します。

    必要な DAP レコード設定を設定し、DAP をリモートアクセス VPN に関連付けます。

DAP の詳細については、ダイナミック アクセス ポリシーを参照してください。

リモート アクセス VPN の履歴

リモートアクセス VPN ダッシュボード

リモートアクセス仮想プライベートネットワーク（RA VPN）を使用すると、リモートユーザーはネットワークに安全に接続できます。RA VPN ダッシュボードでは、デバイス上のアクティブなRA VPNセッションからのリアルタイムデータを監視でき、ユーザーセッションに関連する問題をすばやく特定し、ネットワークとユーザーの問題を軽減できます。

RA VPN ダッシュボード（**Overview** > **Dashboards** > **Remote Access VPN**）は、Firewall Management Center が管理する脅威防御デバイスのアクティブな RA VPN セッションのスナップショットを取得します。

ダッシュボードでは次のことができます。

- ロケーションに基づいたアクティブなユーザーセッションの可視化。
- アクティブなユーザーセッションに関する詳細情報。
- 必要に応じて、セッションを終了することによるユーザーセッションの問題の軽減。
- デバイス、暗号化タイプ、Secure Client バージョン、オペレーティングシステム、および接続プロファイルごとのアクティブなユーザーセッションの分布。
- デバイスのデバイス ID 証明書の有効期限の詳細。

ダッシュボードには以下のウィジェットがあります。

- [アクティブなセッション（Active Sessions）]（表形式ビュー）
- [アクティブなセッション（Active Sessions）]（マップビュー）
- セッション（Sessions）
- [デバイスアイデンティティ証明書（Device Identity Certificates）]

[アクティブなセッション（Active Sessions）]（表形式ビュー）

このウィジェットには、接続されているアクティブなRA VPNユーザーの表形式のビューが表示されます。ユーザー名、割り当てられたIP、パブリックIP、ログイン時間、VPNゲートウェイ（Threat Defense デバイス）、クライアント アプリケーション、クライアント オペレーティング システム、接続プロファイル、グループポリシーなど、アクティブな RA VPN セッションの詳細を確認できます。フィルタを使用して、さまざまな基準に基づいて検索を絞り込むことができ、個々のセッションで以下のアクションも実行できます。

- 特定のユーザーのセッションを終了する。
- 特定の VPN ゲートウェイに接続されている特定のユーザーのすべてのセッションを終了する。

- 特定の VPN ゲートウェイに接続されているすべてのセッションを終了する。

クライアントデバイスがデュアルアドレススタックをサポートし、Firewall Threat Defense デバイスの RA VPN 設定で IPv4 および IPv6 アドレスプールが許可されている場合、クライアントはヘッドエンドデバイスとの RA VPN セッションを確立すると、IPv4 および IPv6 アドレスをクライアントのトンネルインターフェイスに割り当てます。RA VPN セッションには、Threat Defense デバイスの IPv4 アドレスと IPv6 アドレスの 2 つの IP アドレスがあります。Firewall Management Center は、同じユーザーの 2 つのセッションを示しています。1 つは IPv4 アドレス、もう 1 つは IPv6 アドレスで、セッション数は 2 つです。

したがって、デバイスで **show vpn-sessiondb l2l filter ipaddress** コマンドが実行されユーザーからの RA VPN セッションが 1 つしかない場合でも、 Firewall Management Center は 2 つの異なるセッションを示します。

[アクティブなセッション（Active Sessions）]（マップビュー）

このウィジェットには、デバイスの RA VPN セッションを介して接続されているユーザーの場所を可視化するためのインタラクティブなヒートマップが表示されます。

- ユーザーセッションがある国は、青の色合いで表示されます。
- マップの凡例には、国のセッション数とその国に使用される青の色合いとの相関関係を示すスケールが表示されます。
- マップ上にマウスポインタを合わせると、国名とアクティブなユーザーセッションの総数が表示されます。
- ズームイン、ズームアウト、およびリセットのオプションを使用できます。

セッション（Sessions）

このウィジェットでは、デバイス上のアクティブな RA VPN セッションからのリアルタイムデータを監視でき、次の項目に従って、アクティブな RA VPN セッションの分布をフィルタ処理して表示できます。

- [デバイス（Device）]：デバイスごとのセッション数が表示されます。
- [暗号化タイプ（Encryption Type）]：Secure Client SSL または IPsec セッションの数が表示されます。
- [Secure Clientバージョン（Secure Client Version）]：Secure Client バージョンごとのセッションが表示されます。
- [オペレーティングシステム（Operating System）]：オペレーティングシステムごとのセッションが表示されます。Windows、Linux、Mac、モバイル OS など。
- [接続プロファイル（Connection Profile）]：接続プロファイルごとのセッションが表示されます。

[デバイスアイデンティティ証明書（Device Identity Certificates）]

このウィジェットには、RA VPN ゲートウェイのアイデンティティ証明書の有効期限に関する情報が表示されます。期限切れの証明書と、1 か月以内に期限が切れる証明書を確認できます。**[詳細を表示（View Details）]** をクリックして、**Devices** > **Certificates** ページで、証明書を表示します。

VPN セッションとユーザー情報

システムは、VPN 関連アクティビティを含む、ネットワーク上のユーザーアクティビティの詳細を伝達するイベントを生成します。システムのモニタリング機能を使用すると、リモートアクセス VPN の問題が存在するかどうか、および存在する場所を迅速に特定できます。この情報を利用し、ネットワーク管理ツールを使用して、ネットワークおよびユーザの問題を軽減したり、なくしたりすることが可能です。オプションで、必要に応じてリモートアクセス VPN ユーザーをログアウトすることができます。

リモート アクセス VPN アクティブ セッションの表示

Analysis > **Users heading** > **Active Sessions**

ユーザー名、ログイン時間、認証タイプ、割り当て済み/パブリック IP アドレス、デバイスの詳細、クライアントのバージョン、エンドポイント情報、スループット、帯域幅消費グループポリシー、トンネルグループなどのサポート情報を使用して、現在ログインしている VPN ユーザーを任意の時点で表示できます。また、現在のユーザー情報をフィルタ処理し、ユーザーをログアウトし、要約リストからユーザーを削除することもできます。

（注） 高可用性展開で VPN を構成する場合、アクティブな VPN セッションに対して表示されるデバイス名は、ユーザーセッションを識別したプライマリデバイスまたはセカンダリデバイスである可能性があります。

リモート アクセス VPN ユーザー アクティビティの表示

Analysis > **Users heading** > **User Activity**

ネットワーク上のユーザーアクティビティの詳細を表示できます。システムは履歴イベントを記録し、接続プロファイル情報、IP アドレス、位置情報、接続時間、スループット、デバイス情報などの VPN 関連情報が含まれています。

リモートアクセス VPN の履歴

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
地理位置情報ベースの RA VPN	7.7	7.7	国または地域に基づいてリモートアクセス VPN 接続を許可またはブロックできるようになりました。ロケーションベースの基準を満たさない接続は、認証前にブロックされ、監査目的のためにログに記録されます。 新規/変更された画面： • **[オブジェクト（Objects）]** > **オブジェクト管理（Object Management）]** > **[アクセスリスト（Access List）]** > **[サービスアクセス（Service Access）]** • **[デバイス（Devices）]** > **[VPN]** > **[リモートアクセス（Remote Access）]**
VTI ループバック インターフェイスでの IPsec フローオフロード	7.4	任意（Any）	Secure Firewall 3100 および Secure Firewall 4200 デバイスでは、VTI ループバック インターフェイスで IPsec フローオフロードが自動的に有効になります。
Secure Client のカスタマイズ	7.4	任意（Any）	Secure Client のカスタマイズを設定して、VPN ヘッドエンドに展開できます。ユーザーが Secure Client から接続すると、Threat Defense によりこれらのカスタマイズがエンドポイントに配布されます。 • GUI テキストとメッセージ • アイコンとイメージ • スクリプト • バイナリ • Customized Installer Transforms • Localized Installer Transforms 新規/変更された画面： • **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** > **[VPN]** > **[Secure Clientのカスタマイズ（Secure Client Customization）]** • **[デバイス（Device）]** > **[リモートアクセス（Remote Access）]** > **[詳細（Advanced）]** > **[Secure Clientのカスタマイズ（Secure Client Customizations）]**

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
WAN サマリーダッシュボード	7.4	任意（Any）	WAN サマリーダッシュボードには、WAN デバイスとデバイスのインターフェイスのスナップショットが表示されます。 新規/変更された画面： **[概要（Overview）] > [ダッシュボード（Dashboards）] > [SD-WAN サマリー（SD-WAN Summary）]**
リモート アクセス VPN ダッシュボード	7.3	任意（Any）	デバイス上のアクティブなリモートアクセス VPN セッションからのリアルタイム データをモニターできるリモート アクセス VPN（RAVA）ダッシュボード。ユーザーセッションに関連する問題をすばやく特定し、ネットワークとユーザーの問題を軽減できるようにします。 新規/変更された画面： **Overview > Dashboards > Remote Access VPN**
SAML と証明書のサポート	7.2	任意（Any）	証明書と SAML によるユーザー認証をサポートするように、リモートアクセス VPN 構成ウィザードを更新しました。SAML 認証が開始される前に、マシンまたはユーザー証明書を認証するようにリモートアクセス VPN を設定できます。
IPsec フローがオフロードされます。	7.2	任意（Any）	Secure Firewall 3100 では、IPsec フローはデフォルトでオフロードされます。IPsec サイト間 VPN またはリモートアクセス VPN セキュリティアソシエーション (SA) の初期設定後、IPsec 接続はデバイスのフィールドプログラマブル ゲート アレイ (FPGA) にオフロードされるため、デバイスのパフォーマンスが向上します。 FlexConfig と **flow-offload-ipsec** コマンドを使用して構成を変更できます。
複数の IDP トラストポイントのサポート	7.1	任意（Any）	Secure Firewall Management Center は、Microsoft Azure を使用した複数の ID プロバイダートラストポイントをサポートします。Microsoft Azure では、同じエンティティ ID に対して複数のアプリケーションを設定できますが、アイデンティティ証明書は一意である必要があります。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
AnyConnect VPN SAML 外部ブラウザ	7.1	任意（Any）	AnyConnect VPN SAML 外部ブラウザを設定して、パスワードなしの認証、WebAuthn、FIDO、SSO、U2F、Cookie の永続性による SAML エクスペリエンスの向上など、追加の認証の選択肢を有効にできるようになりました。リモートアクセス VPN 接続プロファイルのプライマリ認証方式として SAML を使用する場合は、AnyConnect クライアントが AnyConnect 組み込みブラウザではなく、クライアントのローカルブラウザを使用して Web 認証を実行するように選択できます。このオプションは、VPN 認証と他の企業ログインの間のシングルサインオン（SSO）を有効にします。また、生体認証や Yubikeys など、埋め込みブラウザでは実行できない Web 認証方法をサポートする場合は、このオプションを選択します。 リモートアクセス VPN 接続プロファイルウィザードが更新され、**SAML ログインエクスペリエンス**を設定できるようになりました。
複数証明書認証	7.0	任意（Any）	Secure Firewall Management Center は、Firewall Threat Defense に対して複数証明書ベースの認証をサポートするようになり、AnyConnect クライアントを使用して VPN アクセスを許可するためにユーザーのアイデンティティ証明書を認証することに加えて、マシンまたはデバイス証明書を検証して、デバイスが会社支給のデバイスであることを確認できます。
VPN ロードバランシング	7.0	任意（Any）	VPN ロードバランシングでは、2 つ以上のデバイスが論理的にグループ化され、スループットやその他のトラフィックパラメータは考慮されずに、グループ化されたデバイス間でリモートアクセス VPN セッションが均等に分散されます。
AnyConnect カスタム属性	7.0	任意（Any）	Secure Firewall Management Center は、AnyConnect カスタム属性をサポートし、AnyConnect クライアント機能を設定するためのインフラストラクチャを、それらの機能に対するハードコードサポートを Firewall Threat Defense に追加することなく、提供するようになりました。
ローカルユーザー認証	7.0	任意（Any）	Secure Firewall Management Center Web インターフェイスを使用して Firewall Threat Defense でローカルにユーザーを設定および管理し、プライマリおよびセカンダリのリモートアクセス VPN 認証用にローカルユーザーを設定できるようになりました。
選択的ポリシーの展開	7.0	任意（Any）	展開時に、リモートアクセス VPN およびサイト間 VPN 設定への変更を含めるか除外するかを選択できるようになりました。
AnyConnect モジュール設定のサポート	6.7	任意（Any）	Secure Firewall Management Center は、セキュリティを強化するために AnyConnect モジュールとプロファイルの設定をサポートするようになりました。

機能	Minimum Firewall Management Center	Minimum Firewall Threat Defense	詳細
LDAP 許可のサポート	6.7	任意（Any）	Secure Firewall Management Center を使用して、リモートアクセス VPN の LDAP 認証を設定できます。
リモートアクセス VPN の SAML シングルサインオンサポート	6.7	任意（Any）	SAML 2.0 サーバーをリモートアクセス VPN のシングルサインオン認証サーバーとして設定できます。
AnyConnect 管理 VPN トンネルのサポート	6.7	任意（Any）	Firewall Threat Defense リモートアクセス VPN は、VPN ユーザーが VPN に接続しなくても、企業のエンドポイントの電源がオンになったときにエンドポイントへの VPN 接続を可能にする AnyConnect 管理 VPN トンネルの設定をサポートします。
Datagram Transport Layer Security（DTLS）1.2 のサポート。	6.6	すべて	DTLS 1.2 は、デフォルトの SSL 暗号グループに含まれるようになり、TLS 1.2 とともに構成できます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。