AnyConnect VPN の設定

- VPN への接続と接続解除 （1 ページ）
- Windows システムにおける Start Before Login（PLAP）の設定 （9 ページ）
- Trusted Network Detection を使用した接続または接続解除 （10 ページ）
- Always-Onを使用した VPN 接続の必要性 （14 ページ）
- キャプティブ ポータル ホットスポットの検出と修復の使用 （21 ページ）
- L2TP または PPTP を介した Cisco Secure Client の設定 （25 ページ）
- 管理 VPN トンネルの使用 （26 ページ）
- Cisco Secure Client プロキシ接続の設定 （34 ページ）
- VPN トラフィックの選択および除外 （39 ページ）
- VPN 認証の管理 （51 ページ）

VPN への接続と接続解除

AnyConnect VPN 接続オプション

Cisco Secure Client には、自動的に VPN セッションを接続、再接続、または切断するための多数のオプションが用意されています。これらのオプションは、ユーザが VPN に接続するために便利な方法を提供し、同時にネットワーク セキュリティの要件をサポートします。

AnyConnect 接続の開始とリスタート

VPN 接続サーバーの設定を行い、ユーザが手動で接続するセキュア ゲートウェイの名前とアドレスを提供します。

便利な自動 VPN 接続を提供するための Cisco Secure Client 機能を次から選択します。

- ログイン前の Windows VPN 接続の自動開始
- Cisco Secure Client 起動時の VPN 接続の自動開始
- VPN 接続の自動リスタート

また、強力なネットワーク セキュリティを適用したり、ネットワーク アクセスを VPN のみに制限したりするために、次の自動 VPN ポリシー オプションの使用を検討してください。

- Trusted Network Detection について
- Always-Onを使用した VPN 接続の必要性
- キャプティブ ポータル ホットスポットの検出と修復の使用

Cisco Secure Client 接続の再ネゴシエートと維持

アクティビティが発生していない場合でも、Cisco Secure Firewall ASA がユーザーに対して AnyConnect VPN 接続を維持する長さを制限できます。VPN セッションがアイドルになった場合、接続を終了するか、または接続を再ネゴシエートできます。

- キープアライブ：Cisco Secure Firewall ASA はキープアライブメッセージを定期的に送信します。これらのメッセージは、Cisco Secure Firewall ASA によって無視されますが、クライアントと Cisco Secure Firewall ASA の間の、デバイスを使用した接続の維持に役立ちます。

  ASDM または CLI でキープアライブを設定する手順については、『Cisco ASA Series VPN Configuration Guide』[英語] の「*Enable Keepalive*」の項を参照してください。

- デッド ピア検出：Cisco Secure Firewall ASA および Cisco Secure Client クライアントは、「R-U-There」メッセージを送信します。これらのメッセージは、IPsec のキープアライブメッセージよりも少ない頻度で送信されます。Cisco Secure Firewall ASA（ゲートウェイ）および Cisco Secure Client の両方で、DPD メッセージの送信を有効にして、タイムアウト間隔を設定できます。

  - クライアントが Cisco Secure Firewall ASA の DPD メッセージに応答しない場合、ASA はもう 1 回試行してから、セッションを「再開待機」モードに移行します。このモードでは、ユーザはネットワークをローミングしたり、スリープモードに移行してから後で接続を回復したりできます。アイドルタイムアウトが発生する前にユーザーが再接続しなかった場合、Cisco Secure Firewall ASA はトンネルを終了します。推奨されるゲートウェイ DPD 間隔は 300 秒です。

  - Cisco Secure Firewall ASA がクライアントの DPD メッセージに応答しない場合、クライアントはもう 1 回試行してから、トンネルを終了します。推奨されるクライアント DPD 間隔は 30 秒です。

    ASDM 内で DPD を設定する手順については、適切なリリースの『Cisco ASA Series VPN ASDM Configuration Guide』[英語] の「*Configure Dead Peer Detection*」の項を参照してください。

- ベスト プラクティス：

  - クライアント DPD を 30 秒に設定します（[グループ ポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnect 接続（AnyConnect Client）] > [デッド ピア検出（Dead Peer Detection）]）。

- サーバ DPD を 300 秒に設定します（[グループ ポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnect 接続（AnyConnect Client）] > [デッド ピア検出（Dead Peer Detection）]）。
- SSL および IPsec の両方のキー再生成を 1 時間に設定します（[グループ ポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnect 接続（AnyConnect Client）] > [キー再作成（Key Regeneration）]）。

AnyConnect VPN 接続の終了

AnyConnect VPN 接続を終了するには、ユーザーはセキュアゲートウェイに対してエンドポイントを再認証し、新しい VPN 接続を作成する必要があります。

次の接続パラメータは、タイムアウトに基づいて、VPN セッションを終了します。

- 最大接続時間：ユーザの最大接続時間を分単位で設定します。ここで指定した時間が経過すると、システムは接続を終了します。また、無制限の接続時間（デフォルト）を許可することもできます。
- VPN アイドル タイムアウト：セッションが指定した時間非アクティブである場合は、ユーザのセッションを終了します。VPN アイドル タイムアウトを設定しない場合は、デフォルトのアイドル タイムアウトが使用されます。
- デフォルト アイドル タイムアウト：セッションが指定した時間非アクティブである場合は、ユーザのセッションを終了します。デフォルト値は 30 分（1800 秒）です。

これらのパラメータを設定するには、適切なリリースの『Cisco ASA Series VPN ASDM Configuration Guide』の「*Specify a VPN Session Idle Timeout for a Group Policy*」の項を参照してください。

VPN 接続サーバーの設定

Cisco Secure Client VPN サーバーリストは、VPN ユーザーが接続するセキュアゲートウェイを識別するホスト名とホストアドレスのペアで構成されます。ホスト名は、エイリアス、FQDN、または IP アドレスで指定できます。

サーバーリストに追加されたホストは、Cisco Secure Client GUI の [接続先（Connect to）] ドロップダウンリストに表示されます。その後、ユーザはドロップダウン リストから選択して VPN 接続を開始できます。リストの最上位にあるホストはデフォルト サーバで、GUI のドロップダウン リストの先頭に表示されます。ユーザがリストから代替サーバを選択した場合、その選択されたサーバが新しいデフォルト サーバになります。

サーバ リストにサーバを追加すると、その詳細を表示し、サーバ エントリを編集または削除するようになります。サーバ リストにサーバを追加するには、次の手順を実行します。

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [サーバ リスト（Server List）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

ステップ 3 サーバのホスト名およびアドレスを設定します。

a) [ホスト表示名（Host Display Name）]、ホストの参照に使用されるエイリアス、FQDN、または IP アドレスを入力します。名前に「&」または「<」文字を使用しないでください。FQDN または IP アドレスを入力した場合、次の手順で [FQDN] または [IP アドレス（IP Address）] を入力する必要はありません。

IP アドレスを入力する場合、セキュア ゲートウェイのパブリック IPv4 アドレスまたはグローバル IPv6 アドレスを使用します。リンクローカルセキュア ゲートウェイ アドレスの使用はサポートしていません。

b) （任意）[ホスト表示名（Host Display Name）] に入力していない場合、ホストの [FQDN] または [IP アドレス（IP Address）] を入力します。

c) （任意）[ユーザ グループ（User Group）] を指定します。

Cisco Secure Client は、ユーザーグループとともに FQDN または IP アドレスを使用してグループ URL を形成します。

ステップ 4 [バックアップ サーバ リスト（Backup Server List）] に、バックアップ サーバとしてフォールバックするサーバを入力します。名前に「&」または「<」文字を使用しないでください。

（注） 逆の面から述べれば、[サーバ（Server）] メニューの [バックアップ サーバ（Backup Server）] タブは、すべての接続エントリのグローバル項目です。バックアップ サーバの場所に配置したエントリは、ここで、個々のエントリ サーバ リスト エントリとして入力した内容によって上書きされます。この設定は優先され、推奨される方法です。

ステップ 5 （任意）[ロード バランシング サーバ リスト（Load Balancing Server List）] .に、ロード バランシング サーバ を追加します。名前に「&」または「<」文字を使用しないでください。

このサーバ リスト エントリのホストにセキュリティ アプライアンスのロード バランシング クラスタを指定し、かつ Always-On 機能が有効になっている場合は、このリストにクラスタのロード バランシング デバイスを追加します。指定しなかった場合、ロード バランシング クラスタ内にあるバックアップ デバイスへのアクセスは Always-On 機能によりブロックされます。

ステップ 6 クライアントがこの Cisco Secure Firewall ASA に使用する [プライマリ プロトコル（Primary Protocol）] を指定します。

a) SSL（デフォルト）または IPSec を選択します。

IPsec を指定した場合、ユーザ グループは接続プロファイル（トンネル グループ）の正確な名前である必要があります。SSL の場合、ユーザ グループは接続プロファイルの group-url または group-alias です。

b) IPSec を指定した場合は、[標準認証のみ（Standard Authentication Only）] を選択してデフォルトの認証方式（独自の AnyConnect EAP）を無効にし、ドロップダウン リストからいずれかの方式を選択します。

（注） 認証方式を独自の Cisco Secure Client EAP から標準ベースの方式に変更すると、Cisco Secure Firewall ASA でセッションタイムアウト、アイドルタイムアウト、接続解除タイムアウト、スプリットトンネリング、スプリット DNS、MSIE プロキシ設定、およびその他の機能を設定できなくなります。

ステップ 7 （任意）このサーバ用の SCEP を設定します。

a) SCEP CA サーバの URL を指定します。FQDN または IP アドレスを入力します。たとえば、http://ca01.cisco.com などです。

b) [チャレンジ PW のプロンプト（Prompt For Challenge PW）] をオンにして、ユーザが証明書を手動で要求できるようにします。ユーザが [証明書を取得（Get Certificate）] をクリックすると、クライアントではユーザに対してユーザ名および 1 回限定利用のパスワードに関するプロンプトが表示されます。

c) CA の証明書サムプリントを入力します。SHA1 ハッシュまたは MD5 ハッシュを使用します。CA URL およびサムプリントを用意することができるのは CA サーバ管理者です。サムプリントは、発行した証明書の「fingerprint」属性フィールドや「thumbprint」属性フィールドではなく、サーバから直接取得する必要があります。

ステップ 8 [OK] をクリックします。

関連トピック

Cisco Secure Client プロファイルエディタのサーバーリスト
Cisco Secure Client プロファイルエディタのサーバーリストの追加/編集

ログイン前の Windows VPN 接続の自動開始

Start Before Login について

Start Before Login（SBL）と呼ばれるこの機能により、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。

（注） Start Before Login（SBL）および Secure Firewall ポスチャ を使用する場合、SBL は事前ログインであるため、完全な Secure Firewall ポスチャ 機能を実現するには、Secure Firewall ポスチャ 事前展開モジュールをエンドポイントにインストールする必要があります。

SBL がインストールされ、有効になると、[ネットワーク接続（Network Connect）] ボタンは Cisco Secure Client コア VPN および Network Access Manager UI を起動します。

SBL には、Network Access Manager タイルも含まれており、ユーザが設定したホーム ネットワーク プロファイルを使用した接続を可能にします。SBL モードで許可されるネットワーク プロファイルには、非 802.1X 認証モードを採用するすべてのメディア タイプ（オープン WEP、WPA/WPA2 パーソナル、および静的キー（WEP）ネットワークなど）が含まれます。

SBL は Windows システムのみで利用でき、Windows のバージョンによって異なるメカニズムを使用して実装されます。

- Windows では、Pre-Login Access Provider（PLAP）が Cisco Secure Client SBL を実装するために使用されます。

  PLAP では、Ctrl キー、Alt キー、および Del キーを同時に押すとウィンドウが表示され、そこでシステムにログインするか、ウィンドウの右下隅にある [ネットワーク接続（Network Connect）] ボタンでネットワーク接続（PLAP コンポーネント）を起動するかを選択できます。

  PLAP は Windows の 32 ビット版と 64 ビット版をサポートします。

SBL を有効にする理由としては、次のものがあります。

- ユーザのコンピュータに Active Directory インフラストラクチャを導入済みである。
- ネットワークでマッピングされるドライブを使用し、Microsoft Active Directory インフラストラクチャの認証を必要とする。
- コンピュータのキャッシュにクレデンシャルを入れることができない（グループポリシーでキャッシュのクレデンシャル使用が許可されない場合）。このシナリオでは、コンピュータへのアクセスが許可される前にユーザのクレデンシャルが確認されるようにするため、ユーザは社内ネットワーク上のドメイン コントローラと通信できることが必要です。
- ネットワーク リソースから、またはネットワーク リソースへのアクセスを必要とする場所からログイン スクリプトを実行する必要がある。SBL を有効にすると、ユーザは、ローカル インフラストラクチャおよび通常はオフィスにいるときに実行されるログイン スクリプトにアクセスできます。これには、ドメイン ログイン スクリプト、グループポリシー オブジェクト、およびユーザがシステムにログインするときに通常実行されるその他の Active Directory 機能が含まれます。
- インフラストラクチャとの接続が必要な場合があるネットワーキング コンポーネント（MS NAP/CS NAC など）が存在する。

Start Before Login に関する制限事項

- Cisco Secure Client は、高速ユーザー切り替えとの互換性がありません。
- Cisco Secure Client は、サードパーティの Start Before Login アプリケーションでは起動できません。

Start Before Login の設定

ステップ 1 Cisco Secure Client Start Before Login モジュールのインストール。

ステップ 2 Cisco Secure Client VPN プロファイルでの SBL の有効化。

Cisco Secure Client Start Before Login モジュールのインストール

Cisco Secure Clientインストーラは、基盤となるオペレーティングシステムを検出し、システムディレクトリに Cisco Secure Client SBL モジュールから適切な Cisco Secure Client DLL を配置します。Windows デバイスでは、インストーラは、32 ビット版と 64 ビット版のどちらのオペレーティング システムが使用されているかを判別して、該当する PLAP コンポーネント（vpnplap.dll または vpnplap64.dll）をインストールします。

（注） SBLモジュールがインストールされたままCisco Secure Clientをアンインストールすると、SBLモジュールは無効となり、リモートユーザーの画面に表示されなくなります。

SBL モジュールを事前展開するか、SBL モジュールをダウンロードするように ASA を設定することができます。Cisco Secure Client を事前展開する場合は、Start Before Login モジュールよりも先にコア クライアント ソフトウェアをインストールする必要があります。MSI ファイルを使用して AnyConnect VPN および Start Before Login コンポーネントを事前展開する場合は、正しい順序で実行する必要があります。

ステップ 1 ASDM で、**[設定（Configuration）]** > **[リモート アクセス VPN（Remote Access VPN）]** > **[ネットワーク（クライアント）アクセス（Network (Client) Access）]** > **[グループ ポリシー（Group Policies）]** に移動します。

ステップ 2 グループ ポリシーを選択し、新しいグループ ポリシーの [編集（Edit）] または [追加（Add）] をクリックします。

ステップ 3 左側のナビゲーションペインで **[詳細（Advanced）]** > **[AnyConnectクライアント（AnyConnect Client）]** を選択します。

ステップ 4 [ダウンロードするオプションのクライアント モジュール（Optional Client Module for Download）] 設定の [継承（Inherit）] をオフにします。

ステップ 5 ドロップダウン リストから **AnyConnect SBL** モジュールを選択します。

Cisco Secure Client VPN プロファイルでの SBL の有効化

始める前に

- SBLは、呼び出されたときにネットワークに接続されている必要があります。場合によっては、ワイヤレス接続がワイヤレス インフラストラクチャに接続するユーザのクレデンシャルに依存するために、接続できないことがあります。このシナリオでは、ログインのクレデンシャル フェーズよりも SBL モードが優先されるため、接続できません。このような場合に SBL を機能させるには、ログインを通してクレデンシャルをキャッシュするようにワイヤレス接続を設定するか、その他のワイヤレス認証を設定する必要があります。
- Network Access Managerがインストールされている場合、デバイス接続を展開して、適切な接続を確実に使用できるようにする必要があります。

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 1）（Preferences (Part 1)）] を選択します。

ステップ 2 [Start Before Loginの使用（Use Start Before Login）] を選択します。

ステップ 3 （任意）リモート ユーザが SBL を制御できるようにする場合は、[ユーザ制御可（User Controllable）] をオンにします。

（注） SBL を有効にする場合は、その前にユーザがリモート コンピュータをリブートする必要があります。

Start Before Login のトラブルシューティング

ステップ 1 Cisco Secure Client VPN プロファイルが Cisco Secure Firewall ASA にロードされており、展開できるようになっていることを確認します。

ステップ 2 以前のプロファイルを削除します。プロファイルの場所は、この表に示されています。

ステップ 3 Windows の [プログラムの追加と削除（Add/Remove Programs）] を使用して SBL コンポーネントを再インストールします。コンピュータをリブートして、再テストします。

ステップ 4 イベントビューアでユーザーの Cisco Secure Client ログをクリアし、再テストします。

ステップ 5 セキュリティアプライアンスを再度参照して、Cisco Secure Client を再インストールします。

ステップ 6 いったんリブートします。次回リブート時には、Start Before Login プロンプトが表示されます。

ステップ 7 DART バンドルを収集し、Cisco Secure Client 管理者に送付します。

ステップ 8 次のエラーが表示された場合は、ユーザーの Cisco Secure Client VPN プロファイルを削除します。

```
Description: Unable to parse the profile C:\Documents and Settings\All Users\Application Data
\Cisco\Cisco Secure Client\Profile\VABaseProfile.xml. Host data not available.
```

ステップ 9 .tmpl ファイルに戻って、コピーを .xml ファイルとして保存し、その XML ファイルをデフォルト プロファイルとして使用します。

Cisco Secure Client 起動時の VPN 接続の自動開始

[起動時に自動接続（Auto Connect on Start）] とも呼ばれるこの機能は、Cisco Secure Client が開始されると、VPN クライアントプロファイルで指定されたセキュアゲートウェイへの VPN 接続を自動的に確立します。

[起動時に自動接続（Auto Connect on Start）] はデフォルトでは無効であり、ユーザはセキュアゲートウェイを指定または選択する必要があります。

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [起動時に自動接続（Auto Connect on Start）] を選択します。

ステップ 3 （任意）[起動時に自動接続（Auto Connect on Start）] をユーザが制御できるようにするには、[ユーザ制御可（User Controllable）] を選択します。

Windows システムにおける Start Before Login（PLAP）の設定

Start Before Login（SBL）機能によって、ユーザーが Windows にログインする前に VPN 接続が開始されます。これにより、ユーザは自分のコンピュータにログインする前に、企業のインフラストラクチャに接続されます。Windows にインストールできるのは、一度に 1 つの PLAP のみです。

SBL Cisco Secure Client 機能は、Pre-Login Access Provider（PLAP）と呼ばれます。これは、接続可能なクレデンシャル プロバイダーです。この機能を使用すると、プログラマチック ネットワークの管理者は、クレデンシャルの収集やネットワーク リソースへの接続など特定のタスクをログオン前に実行することができます。PLAP では、サポートされている Windows オペレーティング システムすべてに対して SBL 機能を提供します。PLAP は、vpnplap.dll を使用する 32 ビット版のオペレーティング システムと、vpnplap64.dll を使用する 64 ビット版のオペレーティング システムをサポートしています。PLAP 機能は、x86 および x64 をサポートしています。

VPN 接続の自動リスタート

[自動再接続（Auto Reconnect）] が有効（デフォルト）になっている場合、Cisco Secure Client は初期接続に使用したメディアに関係なく、VPNセッションの中断から回復し、セッションを再確立します。たとえば、有線、ワイヤレス、または 3G/4G/5G のセッションを再確立できます。[自動再接続（Auto Reconnect）] が有効になっている場合は、システムの一時停止またはシステムの再開が発生した場合の再接続動作も指定します。システムの一時停止とは、Windows の「休止状態」や macOS または Linux の「スリープ」など、低電力スタンバイのことです。システムの再開とは、システムの一時停止からの回復のことです。

[自動再接続（Auto Reconnect）] を無効にすると、クライアントでは接続解除の原因にかかわらず、再接続が試行されません。この機能のデフォルト設定（有効）を使用することを強く推奨します。この設定を無効にすると、不安定な接続では VPN 接続の中断が発生することがあります。

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [自動再接続（Auto Reconnect）] を選択します。

ステップ 3 自動再接続の動作を選択します。

- [Disconnect On Suspend]（デフォルト）：Cisco Secure Client では、システムの一時停止時に VPN セッションに割り当てられたリソースが解放され、システムのレジューム後も再接続は試行されません。
- [再開後に再接続（Reconnect After Resume）]：クライアントでは、システムが一時停止すると VPN セッションに割り当てられたリソースが保持され、システムの再開後は再接続が試行されます。

Trusted Network Detection を使用した接続または接続解除

Trusted Network Detection について

信頼ネットワーク検出（TND）を使用すると、ユーザーが企業ネットワークの中（信頼ネットワーク）にいる場合は Cisco Secure Client により自動的に VPN 接続が解除され、企業ネットワークの外（非信頼ネットワーク）にいる場合は自動的に VPN 接続が開始されるようにすることができます。

TND を使用している場合でも、ユーザーが手動で VPN 接続を確立することは可能です。信頼ネットワークの中でユーザーが手動で開始した VPN 接続は解除されません。TND で VPN セッションが接続解除されるのは、最初に非信頼ネットワークにいたユーザーが信頼ネットワークに移動した場合だけです。たとえば、ユーザーが自宅で VPN 接続を確立した後で会社に移動すると、この VPN セッションは TND によって接続解除されます。

（注） Network Visibility Module の TND 機能を設定するには、「Network Visibility Module」の章の Network Visibility Module のプロファイルエディタを参照してください。

TND は Cisco Secure Client VPN プロファイルに設定します。Cisco Secure Firewall ASA の設定を変更する必要はありません。Cisco Secure Client が信頼ネットワークと非信頼ネットワークの間の遷移を認識したときに実施するアクションまたはポリシーを指定する必要があります。また、信頼ネットワークおよび信頼サーバーを特定する必要があります。

（注） VPN トンネルが接続された状態で TND ポリシー評価が行われ、ポリシーで名前ベースの信頼できるサーバーが指定されている場合は常に、その名前解決は、VPN ヘッドエンドによってプッシュされる DNS サーバーを使用して、VPN トンネル経由で実行されます。

Trusted Network Detection のガイドライン

- TND 機能は Cisco Secure Client GUI を制御し、接続を自動的に開始するため、GUI を常に実行している必要があります。ユーザが GUI を終了した場合、TND によって VPN 接続が自動的に開始されることはありません。
- さらに Cisco Secure Client - AnyConnect VPN で Start Before Login（SBL）が実行されている場合は、ユーザが信頼できるネットワークの中に移動した時点で、コンピュータ上に表示されている SBL ウィンドウが自動的に閉じます。
- Always-Onが設定されているかどうかにかかわらず、信頼ネットワーク検出は、IPv4 ネットワークおよび IPv6 ネットワーク経由での Cisco Secure Firewall ASA への IPv6 および IPv4 VPN 接続でサポートされています。
- TND ポリシーは、既存の VPN トンネル状態でのみ有効になります。進行中の Cisco Secure Client 接続/再接続の試行中にネットワークまたはインターフェイスの変更が発生した場合（Cisco Secure Client がすでに接続/再接続を試行している間にインターフェイスの変更が発生するデュアルホームシナリオなど）、TND はトリガーされません。複数のインターフェイス（信頼できるインターフェイスと信頼できないインターフェイス）がある場合、Cisco Secure Client のネットワークアクティビティに選択されるインターフェイスはオペレーティングシステムによって異なります。
- ユーザ コンピュータ上に複数のプロファイルがあると、TND 設定が異なっている場合には問題になることがあります。デュアルホームシナリオでエンドポイントを信頼できると見なすには、すべての TND 条件を満たすインターフェイスが少なくとも 1 つ必要です。

  ユーザーが過去に TND 対応のプロファイルを受け取っていた場合、システムをリスタートすると、Cisco Secure Client は最後に接続されたセキュリティアプライアンスへの接続を試みますが、これが目的の動作ではないことがあります。別のセキュリティアプライアンスに接続するには、そのヘッドエンドを手動で接続解除してから、再接続する必要があります。この問題を回避する手段としては、次のような対策が考えられます。

  - 社内ネットワーク上にあるすべての Cisco Secure Firewall ASA にロードされるクライアントプロファイルで、TND を有効にする。
  - すべての Cisco Secure Firewall ASA がリストされた 1 つのプロファイルをホストエントリセクションに作成し、このプロファイルをすべての Cisco Secure Firewall ASA にロードする。
  - 複数の異なるプロファイルが必要ない場合は、すべての Cisco Secure Firewall ASA のプロファイルに同じプロファイル名を使用する。既存のプロファイルは各 Cisco Secure Firewall ASA により上書きされます。

- Linux 上で TND を使用するには、ネットワーク マネージャがインストールされてターゲット（RHEL/Ubuntu）デバイス上で正しく実行されていることと、ネットワーク インターフェイスがネットワーク マネージャによって管理されていることが必要です。

Trusted Network Detection の設定

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [自動 VPN ポリシー（Automatic VPN Policy）] を選択します。

ステップ 3 [信頼されたネットワークポリシー（Trusted Network Policy）] を選択します。

これは、ユーザが社内ネットワーク（信頼ネットワーク）内に存在する場合にクライアントが実行するアクションです。次のオプションがあります。

- [接続解除（Disconnect）]：（デフォルト）クライアントは、信頼ネットワークでVPN接続を終了します。
- [接続（Connect）]：クライアントは、信頼ネットワークで VPN 接続を開始します。
- [何もしない（Do Nothing）]：クライアントは、信頼ネットワークでアクションを実行しません。[信頼されたネットワークポリシー（Trusted Network Policy）] と [信頼されていないネットワークポリシー（Untrusted Network Policy）] の両方を [何もしない（Do Nothing）] に設定すると、Trusted Network Detection（TND）は無効となります。
- [一時停止（Pause）]：ユーザーが信頼ネットワークの外でVPNセッションを確立した後に、信頼済みとして設定されたネットワークに入った場合、Cisco Secure Client は AnyConnect VPN セッションを接続解除するのではなく、一時停止します。ユーザが再び信頼できるネットワークの外に出ると、そのセッションは AnyConnect VPN により再開されます。この機能を使用すると、信頼ネットワークの外へ移動した後に新しいVPNセッションを確立する必要がなくなるため、ユーザにとっては有用です。

ステップ 4 [信頼されていないネットワークポリシー（Untrusted Network Policy）] を選択します。

これは、ユーザが社内ネットワーク外に存在する場合にクライアントが実行するアクションです。次のオプションがあります。

- [接続（Connect）]：非信頼ネットワークが検出されるとクライアントにより VPN 接続が開始されます。
- [何もしない（Do Nothing）]：クライアントは、非信頼ネットワークの検出時にアクションを実行しません。このオプションを指定すると、Always-On VPNが無効になります。[信頼されたネットワークポリシー（Trusted Network Policy）] と [信頼されていないネットワークポリシー（Untrusted Network Policy）] の両方を [何もしない（Do Nothing）] に設定すると、Trusted Network Detection は無効となります。

ステップ 5 [信頼された DNS ドメイン（Trusted DNS Domains）] を指定します。

クライアントが信頼ネットワーク内に存在する場合にネットワーク インターフェイスに割り当てることができるDNSサフィックス（カンマ区切りの文字列）を指定します。split-dnsリストに複数のDNSサフィックスを追加し、Cisco Secure Firewall ASA でデフォルトドメインを指定した場合、複数の DNS サフィックスを割り当てることができます。

Cisco Secure Client は、次の順序で DNS サフィックスのリストを構築します。

- ヘッドエンドから渡されたドメイン。
- ヘッドエンドから渡されたスプリット DNS リスト。
- パブリック インターフェイスの DNS サフィックス（設定されている場合）。設定されていない場合は、プライマリ DNS サフィックスの親サフィックスを伴うプライマリおよび接続固有のサフィックス（対応するボックスが拡張 TCP/IP 設定でオンの場合）。

照合する DNS サフィックス	TrustedDNSDomains に使用する値
example.com（のみ）	*example.com
example.com および vpn.example.com	*.example.com または example.com、vpn.example.com
asa.example.com および vpn.example.com	*.example.com または asa.example.com、vpn.example.com

ステップ 6 [信頼されたDNSサーバー（Trusted DNS Servers）] を指定します。

クライアントが信頼ネットワーク内に存在する場合にネットワーク インターフェイスに割り当てることができるすべての DNS サーバーアドレス（カンマ区切りの文字列）。たとえば、203.0.113.1,2001:DB8::1 です。IPv4 および IPv6 DNS サーバーアドレスでは、ワイルドカード（*）がサポートされています。

DNS で解決できるヘッドエンドサーバーの DNS エントリが必要です。IP アドレスによる接続の場合、mus.cisco.com を解決できる DNS サーバーが必要です。mus.cisco.com が DNS で解決できない場合、キャプティブ ポータルの検出が期待どおりに動作しません。

（注） TrustedDNSDomains、TrustedDNSServers、またはその両方を設定できます。TrustedDNSServers を設定する場合は、DNS サーバーをすべて入力してください。その結果、サイトはすべて信頼ネットワークの一部になります。

アクティブインターフェイスは、VPN プロファイルのすべてのルールが一致した場合に、信頼ネットワークに含まれると見なされます。

ステップ 7 信頼できる URL として追加するホスト URL を指定します。信頼できる証明書を使用してアクセス可能なセキュア Web サーバーが、信頼できるサーバーとして見なされる必要があります。[追加（Add）] をクリックすると、URL が追加され、証明書ハッシュに事前にデータが取り込まれます。ハッシュが見つからない場合は、ユーザに対して証明書ハッシュを手動で入力して [設定（Set）] をクリックするように求めるエラー メッセージが表示されます。

（注） このパラメータを設定できるのは、信頼された DNS ドメインまたは信頼された DNS サーバーを 1 つ以上を定義する場合だけです。信頼された DNS ドメインまたは信頼された DNS サーバーが定義されていない場合、このフィールドは無効になります。

Always-Onを使用した VPN 接続の必要性

Always-On VPN について

Always-On操作により、VPNセッションがアクティブでない限り、コンピュータが信頼ネットワーク上にない場合にはインターネット リソースにアクセスできなくなります。この状況でVPN を常に適用すると、コンピュータがセキュリティに対する脅威から保護されます。

Always-Onが有効になっている場合、ユーザがログインした後、および非信頼ネットワークが検出されたときに、VPN セッションが自動的に確立されます。VPN セッションは、ユーザーがコンピュータからログアウトするか、セッション タイマーまたはアイドル セッション タイマー (Secure Firewall ASA グループポリシーで指定) が期限切れになるまで開いたままになります。セッションがまだ開いている場合は、Cisco Secure Clientは、セッションを再アクティブ化するために、 接続の再確立を継続的に試行します。それ以外の場合は、新しい VPN セッションの確立を継続的に試みます。

VPN プロファイルで Always-On が有効になっている場合、Cisco Secure Clientは他のダウンロードされたすべての Cisco Secure Client プロファイルを削除してエンドポイントを保護し、Cisco Secure Firewall ASA に接続するように設定されているパブリックプロキシを無視します。

Always-On を有効にする場合は、次の Cisco Secure Client オプションも考慮する必要があります。

- [ユーザーに Always-On VPN セッションの接続解除を許可（Allowing the user to Disconnect the VPN session）]：Cisco Secure Client では、ユーザーが Always-On VPN セッションの接続を解除できます。**Allow VPN Disconnect** を有効にすると、Cisco Secure Client では VPN セッションが確立された時点で[接続解除（Disconnect）]ボタンが表示されます。Always-On VPN を有効にすると、プロファイル エディタでは、[接続解除（Disconnect）] ボタンがデフォルトで有効になります。

  [接続解除（Disconnect）]ボタンを押すと、すべてのインターフェイスがロックされます。これにより、データの漏えいを防ぐことができる以外に、VPNセッションの確立には必要のないインターネットアクセスからコンピュータを保護することができます。現在のVPNセッションでパフォーマンスが低下したり、VPNセッションの中断後に再接続で問題が発生したりした場合、Always-On VPN セッションのユーザは [接続解除（Disconnect）] をクリックして代替のセキュア ゲートウェイを選択できます。

- [接続障害ポリシーの設定（Setting a Connect Failure Policy）]：接続障害ポリシーにより、Always-On VPN が有効で、Cisco Secure Client が VPN セッションを確立できない場合に、コンピュータがインターネットにアクセスできるかどうかが決まります。「常時接続の接続障害ポリシーの設定」を参照してください。

- [キャプティブポータルホットスポットの処理（Handling Captive Portal Hotspots）]：「キャプティブ ポータル ホットスポットの検出と修復の使用」を参照してください。

- VPN が切断されている間の特定のホストへのアクセスの許可：[VPNが切断された状態で次のホストへのアクセスを許可する（Allow access with VPN connected）]（特定の Secure

Firewall ポスチャ の導入に必要な場合があります）で使用可能なオプションの設定。[常にオン（Always On）] の間に AnyConnect VPN が切断されたときに、設定されたホストにエンドポイントがアクセスできるようにします。値は、IP アドレス、IP アドレス範囲（CIDR 形式）、または FQDN を指定できるホストのカンマ区切りリストです。最大 500 のホストを指定できます。

SAML 認証を使用するためにこのパラメータを設定するには、外部 SAML ID プロバイダーで Always-On VPN を使用する （16 ページ） を参照してください。

Always-On VPN の制限事項

- [常時オン（Always On）] は Windows および macOS でのみ使用可能です。
- Always-On がオンであっても、ユーザがログオンしていない場合は、AnyConnect VPN は VPN 接続を確立しません。AnyConnect VPN が VPN 接続を確立するのは、ログイン後に限られます。
- Always-On VPN では、プロキシを介した接続はサポートされていません。

Always-On VPN のガイドライン

脅威に対する保護を強化するためにも、Always-On VPN の設定を行う場合は、次のような追加的な保護対策を講じることを推奨します。

- 認証局（CA）からデジタル証明書を購入し、それをセキュア ゲートウェイ上に登録することを強く推奨します。ASDM では、[アイデンティティ証明書（Identity Certificates）] パネル（[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [証明書の管理（Certificate Management）] > [アイデンティティ証明書（Identity Certificates）]）に、公開証明書を容易に登録するための [ASA SSL VPN を Entrust で登録（Enroll ASA SSL VPN with Entrust）] ボタンが用意されています。
- Always-On が設定されたプロファイルをエンドポイントに事前に展開し、事前定義された Cisco Secure Firewall ASA への接続を制限します。事前展開により、不正なサーバへのアクセスを防止することができます。
- ユーザが処理を終了できないように管理者権限を制限します。管理者権限を持つ PC ユーザは、エージェントを停止することにより、Always-Onポリシーを無視することができます。Always-Onの安全性を十分に確保する必要がある場合は、ユーザに対してローカル管理者権限を付与しないでください。
- Windows コンピュータ上の Cisco サブフォルダ（通常は `C:\ProgramData`）へのアクセスを制限します。
- 限定的な権限または標準的な権限を持つユーザは、それぞれのプログラム データ フォルダに対して書き込みアクセスを実行できる場合があります。このアクセスを使用すれば、Cisco Secure Client プロファイルを削除できるため、Always-On 機能を無効にすることができます。

- Windows ユーザのグループ ポリシー オブジェクト（GPO）を事前に展開して、限定的な権限を持つユーザが GUI を終了できないようにします。macOS ユーザに対してもこれに相当するものを事前に展開します。

Always-On VPN の設定

ステップ 1 Always-On を VPN プロファイルに設定する （16 ページ）。

ステップ 2 （任意）サーバ リストへのロードバランシング バックアップ クラスタ メンバーの追加。

ステップ 3 （任意）常時接続 VPN からのユーザの除外。

Always-On を VPN プロファイルに設定する

始める前に

Always-On VPN を使用するには、Cisco Secure Firewall ASA 上に有効な信頼できるサーバー証明書が設定されている必要があります。設定されていない場合、VPN 常時接続は失敗し、その証明書が無効であることを示すイベントがログに記録されます。また、サーバー証明書が厳格な証明書トラスト モードを通過できるようにすると、Always-On VPN プロファイルのダウンロードを防止して不正なサーバーへの VPN 接続をロックできます。

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [自動 VPN ポリシー（Automatic VPN Policy）] を選択します。

ステップ 3 Trusted Network Detection の設定 （12 ページ）。

ステップ 4 [常時接続（Always On）] を選択します。

ステップ 5 （任意）[VPN の接続解除を許可（Allow VPN Disconnect）] を選択または選択解除します。

ステップ 6 （任意）VPN が [常にオン（Always On）] の場合、切断されるときにエンドポイントがアクセスできるホストを定義します。SAML 認証を使用する場合は、外部 SAML ID プロバイダーで Always-On VPN を使用する （16 ページ） を参照してください。

ステップ 7 （任意）接続障害ポリシーの設定。

ステップ 8 （任意）キャプティブ ポータル修復の設定。

外部 SAML ID プロバイダーで Always-On VPN を使用する

[常にオン（Always On）] を有効にして SAML 認証をサポートするには、次の手順に従います。これは、[VPN が切断されている次のホストへのアクセスを許可する（Allow Access to the Following Hosts with VPN Disconnected）] のパラメータの構成に影響します。

ステップ 1 Cisco Secure Client プロファイルエディタ、プリファレンス（Part 2） の [常にオン（Always On）] のパラメータを無効にします。

ステップ 2 結果のプロファイルが展開された後、すべての DNS フローと、SAML 認証中に Cisco Secure Client が使用するブラウザによって生成されたすべての TCP フロー（埋め込みまたはデフォルト）をキャプチャしながら、SAML 認証を実行します。

Windows

- Microsoft ツールの ProcMon を使用して、ブラウザの TCP フローをキャプチャします。
- ProcMon トレースを開始する前に、Cisco Secure Client ブラウザを使用している場合は、プロセス名フィルタ acwebhelper.exe を追加します。既定のブラウザを使用する場合は、デフォルトのブラウザの実行可能ファイルに一致するプロセス名フィルタを追加します。
- ディスプレイフィルタ **udp.port==53 || (tcp.flags.syn == 1 && tcp.flags.ack ==0)** を使用して、Wireshark で DNS トラフィックと TCP フロートラフィックをキャプチャします。

macOS

- ネイティブツール tcpmon を使用して、プロセス名メタデータを使用して関連するネットワークトラフィックをキャプチャします：**sudo tcpdump -n -k NP > /tmp/capture.txt**
- Cisco Secure Client 組み込みブラウザから発信されたパケットの場合、プロセス名フィールドは *(proc com .apple.WebKit:PID1, eproc Cisco AnyConnect:PID2)* と表示されます。

ステップ 3 Cisco Secure Client が SAML 認証に使用するブラウザから発信されたすべての TCP 接続と、そのような TCP 接続に先行し、TCP 接続の宛先 IP アドレスを含む DNS 応答パケットを識別します。

ステップ 4 以前に識別された DNS 応答パケットのクエリ名フィールドから FQDN を抽出し、Cisco Secure Client プロファイルエディタの [設定（Preferences）]（パート 2）の [VPNの切断時に次のホストへのアクセス（Allow Access to the Following Hosts with VPN Disconnected）] の常時オンのパラメータに追加します。

ステップ 5 また、同じ常時オンの設定パラメータに、対応する DNS トラフィックが先行していないブラウザ接続に対応するすべての IP アドレスを追加します（IP アドレスによる接続など）。

ステップ 6 常時オンのプロファイル設定を再度有効にします。

サーバ リストへのロードバランシング バックアップ クラスタ メンバーの追加

Always-On VPN は、AnyConnect VPN セッションのロード バランシングに影響を与えます。Always-On VPN を無効にした状態では、クライアントからロード バランシング クラスタ内のプライマリ デバイスに接続すると、クライアントはプライマリ デバイスから任意のバックアップ クラスタ メンバーにリダイレクションされます。Always-On を有効にすると、クライアント プロファイルのサーバ リスト内にバックアップ クラスタ メンバーのアドレスが指定されていない限り、クライアントがプライマリ デバイスからリダイレクトされることはありません。このため、サーバ リストにはいずれかのバックアップ クラスタ メンバーを必ず追加するようにしてください。

クライアント プロファイルにバックアップ クラスタ メンバーのアドレスを指定する場合は、ASDM を使用してロード バランシング バックアップ サーバ リストを追加します。手順は次のとおりです。

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [サーバ リスト（Server List）] を選択します。

ステップ 2 ロードバランシング クラスタのプライマリ デバイスであるサーバを選択し、[編集（Edit）] をクリックします。

ステップ 3 いずれかのロード バランシング クラスタ メンバーの FQDN または IP アドレスを入力します。

常時接続 VPN からのユーザの除外

Always-Onポリシーに優先して適用される除外規定を設定できます。たとえば、特定のユーザに対して他社とのVPNセッションを確立できるようにしつつ、企業外資産に対してはAlways-On VPN ポリシーを除外するという場合があります。

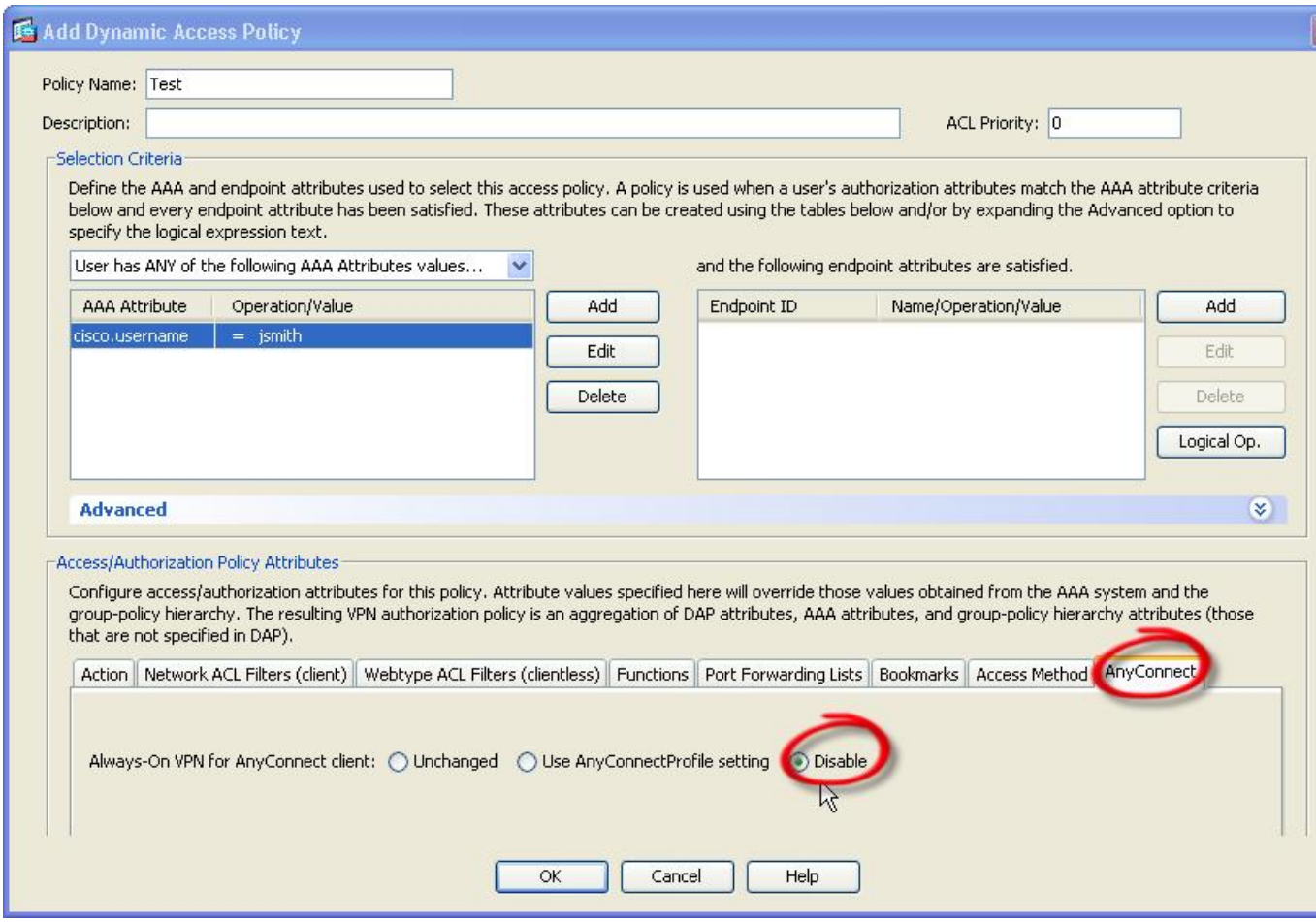
Cisco Secure Firewall ASA のグループポリシーおよびダイナミック アクセス ポリシーで設定された除外規定はAlways-Onポリシーを上書きします。ポリシーの割り当てに使用される一致基準に従って例外を指定します。Cisco Secure Client VPN ポリシーでは Always-On が有効になっているが、ダイナミック アクセス ポリシーまたはグループポリシーでは無効になっている場合、各新規セッションの確立に関するダイナミック アクセス ポリシーまたはグループポリシーが基準と一致すれば、クライアントでは現在以降の VPN セッションに対して無効の設定が保持されます。

この手順では、AAA エンドポイント条件を使用して企業外資産にセッションを照合するダイナミック アクセス ポリシーを設定します。

ステップ 1 [設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [ダイナミック アクセス ポリシー（Dynamic Access Policies）] > [追加（Add）] または [編集（Edit）] を選択します。

ステップ 2 ユーザをAlways-On VPN から除外する条件を設定します。たとえば、[選択基準（Selection Criteria）] 領域を使用して、ユーザのログイン ID に一致する AAA 属性を指定します。

ステップ 3 [ダイナミック アクセス ポリシーの追加（Add Dynamic Access Policy）] ウィンドウまたは [ダイナミック アクセス ポリシーの編集（Edit Dynamic Access Policy）] ウィンドウの下半分にある [AnyConnect] タブをクリックします。



ステップ 4 [AnyConnect クライアントのAlways-On VPN（Always-On VPN for AnyConnect client）] の横にある [無効（Disable）] をクリックします。

常時接続の接続障害ポリシーの設定

接続障害ポリシーについて

接続障害ポリシーは、Always-On VPN が有効で、Cisco Secure Client が VPN セッションを確立できない場合に、コンピュータがインターネットにアクセスできるかどうかを決定します。これは、セキュアゲートウェイに到達不能な場合、またはCisco Secure Clientがキャプティブポータル ホットスポットの存在を検出できない場合に発生する可能性があります。

オープン ポリシーは、最大限のネットワーク アクセスを許可します。これにより、インターネットリソースやその他のローカルネットワークリソースへのアクセスが必要なタスクをユーザが継続して実行できるようにします。

クローズドポリシーは、VPNセッションが確立されるまで、すべてのネットワーク接続を無効にします。Cisco Secure Client では、エンドポイントから、コンピュータが接続を許可されてい

るセキュアゲートウェイ宛以外のトラフィックをすべてブロックするパケットフィルタを有効にすることで、この制限が実現されています。

Cisco Secure Client では、接続障害ポリシーの内容にかかわらず、VPN 接続の確立が継続的に試行されます。

接続障害ポリシーを設定するためのガイドライン

最大限のネットワーク アクセス権を許可するオープン ポリシーを使用する場合は、次の点を考慮してください。

- VPNセッションが確立されるまでセキュリティと保護は提供されません。したがって、エンドポイント デバイスが Web ベースのマルウェアに感染したり、センシティブ データが漏えいしたりする可能性があります。
- [接続解除（Disconnect）] ボタンが有効で、かつユーザが [接続解除（Disconnect）] をクリックした場合は、オープン接続障害ポリシーは適用されません。

VPNセッションが確立されるまですべてのネットワーク接続を無効にする終了ポリシーを使用する場合は、次の点を考慮してください。

- ユーザが VPN の外部へのインターネット アクセスを必要とする場合に、クローズド ポリシーを適用すると、生産性が低下する可能性があります。
- クローズドの目的は、エンドポイントを保護するプライベート ネットワークのリソースが使用できない場合に、ネットワークの脅威から企業資産を保護することです。スプリット トンネリングによって許可されたプリンタやテザー デバイスなどのローカル リソースを除き、すべてのネットワーク アクセスが禁止されるため、エンドポイントは Web ベースのマルウェアとセンシティブ データ漏えいから常に保護されます。
- このオプションは、主にネットワークに常時アクセス可能なことよりも、セキュリティが持続することを重視する組織向きです。
- クローズドポリシーは、特に有効にしない限り、キャプティブ ポータルを修復しません。
- クライアント プロファイルで [最新の VPN ローカル リソースを適用（Apply Last VPN Local Resources）] が有効になっている場合は、直近の VPN セッションにより適用されたローカル リソース ルールを適用できます。たとえば、これらのルールにより、アクティブ シンクやローカル印刷へのアクセスを規定することができます。
- Cisco Secure Client ソフトウェアのアップグレード中、Always-On が有効であると、ネットワークはクローズドポリシーに関係なくブロックが解除され、開かれます。
- クローズド接続ポリシーの展開は、段階的に行うことを強く推奨します。たとえば、最初に接続障害オープンポリシーを使用してAlways-On を展開し、ユーザーを通じて Cisco Secure Client がシームレスに接続できない頻度を調査します。さらに、新機能に関心を持つユーザを対象に、小規模な接続障害クローズドポリシーを試験的に展開しそのフィードバックを依頼します。引き続きフィードバックを依頼しながら試験的なプログラムを徐々に拡大したうえで、全面的な展開を検討します。接続障害クローズドポリシーを展開する場合は必ず、VPN ユーザに対して接続障害クローズド ポリシーのメリットだけでなく、ネットワーク アクセスの制限についても周知してください。

注意 Cisco Secure Client が VPN セッションの確立に失敗した場合は、接続障害クローズドポリシーによりネットワークアクセスは制限されます。接続障害クローズドポリシーは、細心の注意を払って実装してください。

接続障害ポリシーの設定

Always-On 機能を有効にする場合にのみ、接続障害ポリシーを設定します。デフォルトでは、接続障害ポリシーはクローズされており、VPN が到達不能な場合にはインターネットにアクセスできません。この状況でインターネットへのアクセスを許可するには、オープンするように接続障害ポリシーを設定する必要があります。

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [接続エラーポリシー（Connect Failure Policy）] パラメータを次のいずれかに設定します。

- [クローズド（Closed）]：（デフォルト）セキュア ゲートウェイに接続できない場合、ネットワークアクセスが制限されます。
- [オープン（Open）]：クライアントがセキュア ゲートウェイに接続できない場合、ブラウザなどのアプリケーションによるネットワーク アクセスが許可されます。

ステップ 3 クローズド ポリシーを指定した場合は、次の手順を実行します。

a) キャプティブ ポータル修復の設定。

b) ネットワーク アクセスが無効になっている間、最後の VPN セッションのローカル デバイス ルールを保持する場合は、[最新の VPN ローカル リソースを適用（Apply Last VPN Local Resources）] を選択します。

キャプティブポータルホットスポットの検出と修復の使用

キャプティブ ポータルについて

空港、喫茶店、ホテルなど、Wi-Fi や有線アクセスを提供している施設では、アクセスする前に料金を支払ったり、アクセプタブル ユース ポリシーを順守することに同意したりする必要があります。こうした施設では、キャプティブ ポータルと呼ばれる技術を使用することにより、ユーザがブラウザを開いてアクセス条件に同意するまではアプリケーションの接続が行えないようにしています。キャプティブポータルの検出はこの制限を認識することであり、キャ

プティブ ポータル修復はネットワーク アクセスを取得するためにキャプティブ ポータルのホットスポット要件を満たすプロセスです。

キャプティブポータルは、VPN 接続が開始されると Cisco Secure Client によって自動的に検出され、追加設定は必要ありません。また、Cisco Secure Client は、キャプティブポータルの検出中にブラウザの設定を変更せず、キャプティブポータルを自動的に修復しません。修復は、エンドユーザーが実行します。Cisco Secure Client は、現在の設定に応じてキャプティブポータルの検出に対応します。

- Always-On が無効の場合、または Always-On が有効で接続障害ポリシーが開いている場合、各接続試行時に次のメッセージが表示されます。

```
The service provider in your current location is restricting access to the Internet.
 You need to log on with the service provider before you can establish a VPN session.
 You can try this by visiting any website with your browser.
```

  エンドユーザは、ホットスポットプロバイダーの要件を満たすことで、キャプティブ ポータル修復を実行する必要があります。これらの要件には、ネットワークにアクセスするための料金の支払い、アクセプタブル ユース ポリシーへの署名、その両方、またはプロバイダーが定義するその他の要件などがあります。

- Always-On が有効で、接続障害ポリシーが閉じている場合、キャプティブ ポータル修復を明示的に有効にする必要があります。有効の場合、エンドユーザは修復を前述のように実行できます。無効の場合、各接続試行時に次のメッセージが表示され、VPN に接続できません。

```
The service provider in your current location is restricting access to the Internet.
 The Cisco Secure Client protection settings must be lowered for you to log on with
 the service provider. Your current enterprise security policy does not allow this.
```

キャプティブ ポータル修復の設定

Always-On 機能を有効にし、接続障害ポリシーをクローズドに設定する場合にのみ、キャプティブ ポータル修復を設定します。この場合、キャプティブポータルのために VPN に接続できないときは、キャプティブポータル修復を設定すると、Cisco Secure Client は VPN に接続できます。

（注） このプラットフォームでは常時接続がサポートされていないため、キャプティブ ポータルの修復の設定は Linux に適用されません。したがって、プロファイル エディタでの [キャプティブ ポータルの修復を常に許可（Allow Captive Portal Remediation Aloways On）] の設定に関係なく、Linux ユーザはキャプティブ ポータルを修復できます。

接続障害ポリシーがオープンに設定されているか、または Always-On が有効でない場合、ユーザーはネットワークアクセスが制限されないため、Cisco Secure Client VPN プロファイルに特定の設定がなくてもキャプティブポータルを修復できます。

デフォルトでは、セキュリティを最大化するために、常時接続をサポートしているプラットフォーム（Windows と macOS）上ではキャプティブポータルの修復は無効になっています。Cisco Secure Client は、キャプティブポータル修復フェーズ中のデータ漏洩保護機能を提供しません。データ損失保護が必要な場合は、関連するエンドポイントセキュリティ製品を使用する必要があります。

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [キャプティブ ポータルの修復を許可（Allow Captive Portal Remediation）] **.**を選択します。

この設定は、クローズ接続障害ポリシーによるネットワーク アクセス制限を解除します。

ステップ 3 修復タイムアウトを指定します。

Cisco Secure Client がネットワークアクセス制限を解除する時間（分単位）を入力します。ユーザには、キャプティブ ポータルの要件を満たすことができるだけの十分な時間が必要です。

キャプティブポータルの修復の強化（Windows および macOS）

キャプティブポータルの修復が強化され、Cisco Secure Client によって制限されているネットワークアクセス（常時接続などによる）を伴うキャプティブポータルが検出されるたびに、Cisco Secure Client の組み込みブラウザを使用して修復が実行されます。その他のアプリケーションは、Cisco Secure Client ブラウザでのキャプティブポータルの修復が保留中の間、ネットワークアクセスがブロックされたままになります。ユーザーは Cisco Secure Client ブラウザを閉じて、外部ブラウザにフェールオーバーできます（プロファイルで有効になっている場合）。これにより、Cisco Secure Client は通常のキャプティブポータルの修復動作に戻ります。その場合に、次のメッセージが表示されます。

```
Please retry logging on with the service provider to retain access to the Internet, by
visiting any website with your browser.
```

キャプティブポータルが検出されたものの、ネットワークアクセスが Cisco Secure Client によって制限されている場合、Cisco Secure Client ブラウザが自動的に起動し、ユーザーに修復を求める次のメッセージが表示されます。

```
The service provider in your current location is restricting access to the internet. You
 need to log on with the service provider before you establish a VPN session, using the
 Cisco Secure Client browser.
```

キャプティブ ポータルの修復の設定ブラウザのフェールオーバー

キャプティブポータルの修復のために Cisco Secure Client ブラウザが起動するたびに適用されるようにブラウザのフェールオーバーを設定することができます。ブラウザのフェールオーバーを設定することで、ユーザーは Cisco Secure Client ブラウザを閉じた後に外部ブラウザを介してキャプティブポータルを修復できます。

キャプティブポータルの修復のために起動した Cisco Secure Client ブラウザには、サーバーセキュリティ証明書に関して厳密なセキュリティ設定が備わっています。キャプティブ ポータルの修復中は、信頼されていないサーバ証明書は受け入れられません。信頼できないサーバー証明書が検出されると、対応する HTTPS URL が Cisco Secure Client ブラウザによってロードされず、修復プロセスがブロックされる可能性があります。キャプティブ ポータルの修復中に信頼できないサーバ証明書が受け入れられる場合は、キャプティブポータルの修復ブラウザのフェールオーバーを有効にしてユーザがキャプティブ ポータルを修復できるようにする必要があります。有効にすると、ユーザーは Cisco Secure Client ブラウザを閉じ、（Cisco Secure Client は通常のキャプティブポータルの修復動作に戻るため）外部ブラウザを使用して修復を継続することができます。

始める前に

Windows および macOS でサポートされています。

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 エンドユーザーが（Cisco Secure Client ブラウザを閉じた後）キャプティブポータルの修復に外部ブラウザを使用させる場合は、[キャプティブポータルの修復ブラウザのフェールオーバー（Captive Portal Remediation Browser Failover）] をオンにします。デフォルトでは、エンドユーザーは Cisco Secure Client ブラウザを使用してキャプティブポータルの修復のみを行えます。つまり、ユーザーは強化されたキャプティブポータルの修復を無効にすることはできません。

キャプティブ ポータルの検出と修復のトラブルシューティング

次のような状況では、Cisco Secure Client は誤ってキャプティブポータルと見なされる場合があります。

- サーバー名が正しくない証明書（CN）を持った Cisco Secure Firewall ASA に接続しようとしている場合、Cisco Secure Client は、その環境を「キャプティブポータル」環境と見なします。

  これを回避するには、Cisco Secure Firewall ASA 証明書が正しく設定されていることを確認します。証明書の CN 値は、VPN クライアントプロファイルの Cisco Secure Firewall ASA サーバーの名前と一致する必要があります。

- Cisco Secure Firewall ASA の前に別のデバイスがネットワーク上に存在し、そのデバイスが ASA への HTTPS アクセスをブロックして、クライアントによる Cisco Secure Firewall ASA への接続に応答すると、Cisco Secure Client は、その環境を「キャプティブポータル」環境と見なします。これは、ユーザーが内部ネットワークに存在し、ファイアウォールを介して Cisco Secure Firewall ASA に接続している場合に発生する可能性があります。

  企業内から Cisco Secure Firewall ASA へのアクセスを制限する必要がある場合、ASA のアドレスへの HTTP および HTTPS トラフィックが HTTP ステータスを返さないようにファイアウォールを設定します。Cisco Secure Firewall ASA への HTTP/HTTPS アクセスは許可

するか、完全にブロックし、ASA に送信された HTTP/HTTPS 要求が予期しない応答を返さないようにします。

ユーザがキャプティブ ポータル修復ページにアクセスできない場合は、次のことを試すようにユーザに指示してください。

- 修復を実行するためのブラウザを 1 つだけ残し、インスタント メッセージング プログラム、電子メール クライアント、IP フォン クライアントなど、HTTP を使用するその他のアプリケーションをすべて終了します。

  キャプティブ ポータルは、接続の反復試行を無視し、結果的にクライアント側でタイムアウトにすることで、DoS 攻撃を積極的に阻止することができます。HTTP 接続が多数のアプリケーションによって試行された場合、この問題の深刻度は大きくなります。

- ネットワーク インターフェイスを無効にした後、再度有効にします。このアクションにより、キャプティブ ポータルの検出が再試行されます。

- コンピュータを再起動します。

L2TP または PPTP を介した Cisco Secure Client の設定

一部の国の ISP では、Layer 2 Tunneling Protocol（L2TP）や Point-to-Point Tunneling Protocol（PPTP）のサポートが必要です。

セキュアゲートウェイを宛先としたトラフィックを Point-to-Point Tunneling Protocol（PPP）接続上で送信するため、Cisco Secure Client は外部トンネルが生成したポイントツーポイント アダプタを使用します。PPP 接続上で VPN トンネルを確立する場合、クライアントでは Cisco Secure Firewall ASA より先を宛先としてトンネリングされたトラフィックから、この Cisco Secure Firewall ASA を宛先とするトラフィックが除外される必要があります。除外ルートを特定するかどうかや、除外ルートを特定する方法を指定する場合は、Cisco Secure Client プロファイルの [PPP 除外（PPP Exclusion）] 設定を使用します。除外ルートは、セキュアでないルートとして Cisco Secure Client GUI の [ルートの詳細（Route Details）] 画面に表示されます。

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [PPP 除外（PPP Exclusion）] でその方式を選択します。また、このフィールドに対する [ユーザ制御可（User Controllable）] をオンにして、ユーザがこの設定を表示および変更できるようにします。

- [自動（Automatic）]：PPP 除外を有効にします。Cisco Secure Client は、PPP サーバーの IP アドレスを自動的に決定します。

- [オーバーライド（Override）]：[PPP除外サーバーIP（PPP Exclusion Server IP）] フィールドで指定された定義済みのサーバー IP アドレスを使用して PPP 除外を有効にします。[PPP除外サーバーIP（PPP Exclusion Server IP）] フィールドは、このオーバーライド方式にのみ適用され、[自動（Automatic）] オプションで PPP サーバーの IP アドレスを検出できない場合にのみ使用する必要があります。

[PPP除外サーバーIP（PPP Exclusion Server IP）] フィールドで [ユーザ制御可（User Controllable）] をオンにすると、エンドユーザーは preferences.xml ファイルを使用して IP アドレスを手動で更新できます。「ユーザに対する PPP 除外上書きの指示 （26 ページ）」セクションを参照してください。

- [無効（Disabled）]：PPP 除外は適用されません。

ユーザに対する PPP 除外上書きの指示

自動検出が機能しない場合に、PPP 除外フィールドをユーザー設定可能に設定すると、ユーザーはローカルコンピュータ上で Cisco Secure Client プリファレンスファイルを編集することにより、これらの設定を上書きすることができます。

ステップ 1 メモ帳などのエディタを使用して、プリファレンス XML ファイルを開きます。

このファイルは、ユーザのコンピュータ上で次のいずれかのパスにあります。

- Windows：%LOCALAPPDATA%\Cisco\Cisco Secure Client\VPN\preferences.xml 次に例を示します。
- macOS：/Users/username/.vpn/.anyconnect
- Linux：/home/username/.vpn/.anyconnect

ステップ 2 PPPExclusion の詳細を `<ControllablePreferences>` の下に挿入して、Override 値と PPP サーバーの IP アドレスを指定します。アドレスは、完全な形式の IPv4 アドレスにする必要があります。次に例を示します。

```
<AnyConnectPreferences>
<ControllablePreferences>
<PPPExclusion>Override
<PPPExclusionServerIP>192.168.22.44</PPPExclusionServerIP></PPPExclusion>
</ControllablePreferences>
</AnyConnectPreferences>
```

ステップ 3 ファイルを保存します。

ステップ 4 Cisco Secure Client を終了し、リスタートします。

管理 VPN トンネルの使用

管理 VPN トンネルについて

管理 VPN トンネルにより、エンドユーザによって VPN 接続が確立されるときだけでなく、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の接続が確保されます。オフィスネットワークに VPN を介してユーザが頻繁に接続しないデバイスに対しては特に、外出中のオフィスのエンドポイントで Patch Management を行うことができます。この機能には、社内

ネットワークの接続を必要とするエンドポイント OS ログイン スクリプトに対するメリットもあります。

管理 VPN トンネルはエンドユーザに対し透過的であるため、ユーザ アプリケーションによって開始されたネットワーク トラフィックはデフォルトで影響を受けませんが、代わりに管理 VPN トンネルの外部に転送されます。

管理トンネル機能が有効として検出されると、制限付きのユーザアカウント（ciscoacvpnuser）が作成され、最小権限の原則が適用されます。このアカウントは、Cisco Secure Client のアンインストール中、またはインストールのアップグレード中に削除されます。

ログインが低速であるとユーザから報告された場合、管理トンネルが適切に設定されていない可能性があります。「管理 VPN トンネルの設定 （29 ページ）」で、この機能を有効にするのに必要な設定手順について説明します。この設定を行ったにもかかわらず、社内ネットワークへの接続ができない症状が出ている場合は、「管理 VPN トンネル接続問題のトラブルシューティング」を参照してください。

管理 VPN トンネルの互換性と要件

- ASDM 9.0.1（またはそれ以降）および ASDM 7.10.1（またはそれ以降）が必要です。
- ユーザ ログインの前後にユーザによって開始された VPN トンネルが切断されるたびに接続します。

（注） 信頼ネットワーク検出（TND）機能によって信頼ネットワークが検出されるか、Cisco Secure Client ソフトウェアアップデートが進行中の場合、管理 VPN トンネルは確立されません。

- ユーザ ログインの前後にユーザが VPN トンネルを開始するたびに切断します。
- マシン ストア証明書認証のみを使用します。
- ユーザが開始したネットワーク通信に影響しないように（管理 VPN トンネルは、エンドユーザに対して透過的であるため）Split-include トンネリングの設定がデフォルトで必要です。この動作をオーバーライドする場合は、「Tunnel-All 設定をサポートするカスタム属性の設定 （32 ページ）」を参照してください。
- サーバ証明書に対して厳密な証明書のチェックを実行します。サーバー証明書のルート CA 証明書は、マシン証明書ストア（Windows の場合はコンピュータ証明書ストア、macOS の場合はシステム キーチェーンまたはシステム ファイル証明書ストア）に存在する必要があります。
- バックアップ サーバ リストで作業します。
- 現在 Windows および macOS でのみ入手可能です。以降のリリースでは、Linux のサポートが追加されます。

管理 VPN トンネルの非互換性と制限

- 管理 VPN プロファイルはプロキシ設定の値 [ネイティブ（Native）] をサポートしていません。この制限は、管理 VPN トンネルはユーザがログインしていなくても開始できるため、 Windows クライアントにのみ適用されます。 そのため、ユーザ固有のブラウザ プロキシ設定に依存することはできません。
- 管理 VPN プロファイルは、VPN サーバからプッシュされるプライベート プロキシ設定をサポートしません。管理 VPN トンネルはエンド ユーザに対して透過的であることを目的としているため、ユーザ固有の設定またはシステム プロキシ設定は変更されません。
- ユーザの VPN トンネルが非アクティブになるたびに管理 VPN トンネルが確立されるため、Always On 機能と互換性はありません。ただし、すべてのトラフィックをトンネリングするように管理トンネル接続のグループ ポリシーを設定して、ユーザの VPN トンネルが非アクティブの間にトラフィックが物理インターフェイスによってリークされないようにすることができます。「Tunnel-All 設定をサポートするカスタム属性の設定 （32 ページ）」を参照してください。
- キャプティブポータルの修復は、Cisco Secure Client UI が実行中でユーザーがログインしている間、管理 VPN トンネル機能が有効になっていなかったかのようであるときにのみ実行されます。
- 管理 VPN プロファイルの設定は、管理 VPN トンネルがアクティブのときにのみ Cisco Secure Client で適用されます。管理 VPN トンネルが切断されると、ユーザの VPN トンネル プロファイル設定のみが適用されます。このため、管理 VPN トンネルはユーザの VPN トンネル プロファイルの信頼ネットワーク検出（TND）設定（つまり、設定済みの信頼できないネットワーク ポリシーに関係なく TND が無効化されるか、「信頼できないネットワーク」が検出された場合）に従って開始されます。また、管理 VPN プロファイルにおける TND 接続アクションは（管理 VPN トンネルがアクティブである場合にのみに適用）、管理 VPN トンネルがエンド ユーザに対して透過的であるように常にユーザの VPN トンネルに適用されます。ユーザエクスペリエンスに一貫性をもたせるために、ユーザと管理の両方の VPN トンネルプロファイルで同じ TND 設定を使用する必要があります。

管理 VPN プロファイルによって適用される必須設定

特定のプロファイル設定は管理 VPN トンネルがアクティブである間は必須です。有効なプロファイルの設定をサポートするために、対応する UI 制御を無効にすることで、Cisco Secure Client 管理 VPN プロファイル エディタにより必須設定が適用されます。主に、ユーザのインタラクションを排除してトンネルの中断を最小限に抑えるために、管理トンネルの接続中に次の設定値が上書きされます。

- *AllowManualHostInput: false*：管理トンネル (ヘッドレス クライアント) に関連しません。
- *AlwaysOn: false*：管理トンネルが切断されるたびにユーザのトンネル プロファイル設定が適用されるため、関連しません。
- *AutoConnectOnStart: false*：以前に接続されたホストに対する起動時の自動接続用 UI クライアントにのみ関連します。
- *AutomaticCertSelection: true*：証明書の選択ポップアップを回避します。
- *AutoReconnect: true*：ネットワークの変更時に管理トンネルが終了するのを回避します。

- *AutoReconnectBehavior: ReconnectAfterResume*：ネットワークの変更時に管理トンネルの終了を回避します。
- *AutoUpdate: false*：管理トンネル接続中にソフトウェア アップデートは実行されません。
- *BlockUntrustedServers: true*： 信頼できないサーバ証明書のプロンプトを回避します。
- *CertificateStore: MachineStore*：管理トンネル認証はログイン ユーザなしでも成功する必要があります。
- *CertificateStoreOverride: true*：Windows でのマシン証明書認証に必要です。
- *EnableAutomaticServerSelection: false*：管理 VPN プロファイルではホスト エントリは 1 つのみです。
- EnableScripting: false：Cisco Secure Client カスタマイゼーション スクリプト（接続時または切断時に呼び出される）は管理トンネル接続中は実行されません。
- *MinimizeOnConnect:false*：管理トンネル（ヘッドレス クライアント）に関連しません。
- *RetainVPNOnLogoff:true*: 管理トンネルはユーザがログオフしてもアクティブなままである必要があります。
- *ShowPreConnect Message*：管理トンネル（ヘッドレス クライアント）に関連しません。
- *UserEnforcement: AnyUser*：特定のユーザがログインしたときに管理トンネルが切断されないようにします。
- *UseStartBeforeLogon:False*：ユーザ トンネルにのみ適用されます。
- *WindowsVPNEstablishment: AllowRemote* ユーザ：どのユーザ タイプ（ローカルまたはリモート）がログインしても管理トンネルが影響されないようにします。
- [LinuxVPNEstablishment：リモート ユーザを許可（LinuxVPNEstablishment: Allow Remote Users）]：管理トンネルがどのタイプ（ローカル/リモート）のユーザによっても影響されないようにします。

また、Cisco Secure Client では、管理トンネルの接続中は、WindowsLogonEnforcement および SCEP 関連の設定はプロファイル設定として適用されません。

管理 VPN トンネルの設定

ユーザがログインしていなくても管理トンネル接続が発生する場合があるため、マシン ストア証明書認証のみがサポートされます。したがって、少なくとも 1 つの関連するクライアント証明書がクライアント ホストのマシン証明書ストアで使用できる必要があります。

管理 VPN トンネルのトンネル グループの設定

トンネルグループの認証方法は、ASDM で**[設定（Configuration）]>[リモートアクセス（Remote Access）]>[ネットワーク（クライアント）アクセス（Network (Client) Access）]>[AnyConnect 接続プロファイル（AnyConnect Connection Profiles）]>[追加/編集（Add/Edit）]** に移動し、

[証明書のみ（certificate only）] として設定する必要があります。次に、[詳細設定（Advanced）] > [グループ エイリアス/グループ URL（Group Alias/Group URL）] でグループ URL を設定してから、次に 「管理 VPN トンネルのプロファイルの作成 （30 ページ）」 の説明に従って管理 VPN プロファイルで指定します。

このトンネル グループのグループ ポリシーには、トンネル グループで設定されたクライアント アドレスの割り当てを使用するすべての IP プロトコルに対して split include トンネリングが設定されている必要があります（ASDM から [下記のネットワーク リストをトンネル（Tunnel Network List Below）] には **[リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）] > [編集（Edit）] > [詳細設定（Advanced）] > [スプリット トンネリング（Split Tunneling）]を選択）。** > 「Tunnel-All 設定をサポートするカスタム属性の設定 （32 ページ）」 では、その他のスプリット トンネリング設定のサポートを有効にする方法について説明します。両方の IP プロトコルに対するトンネル グループでクライアント アドレスの割り当てが設定されていない場合、[クライアント バイパス プロトコル（Client Bypass Protocol）] を有効にし、クライアント アドレスの割り当てのない IP プロトコルと一致するトラフィックが管理 VPN トンネルで中断されないようにする必要があります。

管理 VPN トンネルのプロファイルの作成

特定のクライアント デバイスには、1 つの管理 VPN プロファイルのみを展開できます。管理 VPN プロファイルは固定名（VpnMgmtTunProfile.xml）で専用ディレクトリ（Windows では %ProgramData%\Cisco\Cisco Secure Client\VPN\Profile\MgmtTun、macOS では /opt/cisco/secureclient/VPN/profile/mgmttun）に格納されます。管理 VPN プロファイルには、「管理 VPN トンネルのトンネル グループの設定 （29 ページ）」 セクションに従って設定されたトンネル グループを指しているゼロまたは 1 つのホスト エントリを使用できます。（トンネル確立中のプロファイルの更新時に）この機能を自動的に無効にするには、管理 VPN プロファイルでゼロのホスト エントリを設定する必要があります。

始める前に

管理 VPN トンネルのトンネル グループの設定 （29 ページ）を完了します。

ステップ 1 **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnectクライアントプロファイル（AnyConnect Client Profile）]** に移動します。

ステップ 2 [追加（Add）] をクリックします。[AnyConnect クライアントプロファイルの追加（Add AnyConnect Client Profiles）] ウィンドウが表示されます。

ステップ 3 プロファイルの使用方法として、 [AnyConnect 管理 VPN プロファイル（AnyConnect Management VPN Profile）] を選択します。[AnyConnect クライアント プロファイルの追加（Add AnyConnect Client Profiles）] 画面でフィールドを読み込む方法の詳細については、『Cisco ASA Series VPN ASDM Configuration Guide』 [英語] の「Configure AnyConnect Client Profiles」セクションを参照してください。

ステップ 4 「管理 VPN トンネルのトンネル グループの設定 （29 ページ）」で作成したグループ ポリシーを選択します。[OK] をクリックして管理 VPN プロファイルを作成してから、[編集（Edit）] をクリックして設定します。以降の更新に対しても同様に行います。

（オプション）すでに設定済みの管理 VPN プロファイルをアップロードする

すでに設定済みの管理 VPN プロファイル（スタンドアロン Cisco Secure Client 管理 VPN プロファイル エディタを使用して編集または作成された、Cisco Secure Client からコピーされた、または別の Cisco Secure Firewall ASA からエクスポートされた）を Cisco Secure Firewall ASA にアップロードする必要がある場合があります。

ステップ 1 ASDM で、[AnyConnect クライアント プロファイル（AnyConnect Client Profile）] ウィンドウから [追加（Add）]、[アップロード（Upload）] をクリックします。.
ファイルのアップロードの接続先の場所を選択するには、 *vpnm* 拡張子付きのプロファイルを選択することを確認します。

ステップ 2 プロファイル名を提供し、プロファイルの使用率のドロップダウン メニューから **AnyConnect 管理 VPN プロファイル**を選択します。

ステップ 3 「管理 VPN トンネルのトンネル グループの設定 （29 ページ）」で作成したグループ ポリシーを選択します。[OK] をクリックし、管理 VPN プロファイルを作成します。

グループ ポリシーへの管理 VPN プロファイルの関連付け

管理トンネル接続に使用するトンネル グループ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。

（注） 同様に、ユーザ トンネル接続に使用する正規のトンネル グループにマッピングされたグループ ポリシーに管理 VPN プロファイルを追加することもできます。ユーザが接続すると、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 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。

また、アウトオブバンドで管理 VPN プロファイルを展開することができます。その場合、VpnMgmtTunProfile.xml という名前が付いていることを確認し、上記の管理 VPN プロファイル ディレクトリにコピーして、Cisco Secure Client エージェント サービスを再起動（またはリブート）します。

始める前に

「管理 VPN トンネルのトンネル グループの設定 （29 ページ）」と「管理 VPN トンネルのプロファイルの作成 （30 ページ）」を完了します。

ステップ 1 ASDM で **[グループポリシー（Group Policy）] > [詳細（Advanced）] > [AnyConnectクライアント（AnyConnect Client）]** に移動します。

ステップ 2 ダウンロードするクライアント プロファイルで、[追加（Add）] をクリックし、「管理 VPN トンネルのプロファイルの作成 （30 ページ）」セクションで作成または更新された管理 VPN プロファイルを選択します。

Tunnel-All 設定をサポートするカスタム属性の設定

管理 VPN トンネルでは、ユーザが開始したネットワーク通信に影響しないように（管理 VPN トンネルは、エンド ユーザに対して透過的であるため）Split-include トンネリングの設定がデフォルトで必要です。この動作は管理トンネル接続で使用されているグループポリシーで次のカスタム属性を設定することによりオーバーライドできます（[CreateCustom 属性 ASDM（CreateCustom Attribute ASDM）] ウィンドウ：**[設定（Configuration）] > [リモートアクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループポリシー（Group Policies）] > [編集（Edit）] > [詳細設定（Advanced）] > [AnyConnect クライアント（AnyConnect Client）] > [カスタム属性（Custom Attributes）] > [追加（Add）]**）。

新しいカスタム属性タイプを **ManagementTunnelAllAllowed** に設定し、対応するカスタム属性を *true* に設定すると、その構成が両方の IP プロトコルに対して tunnel-all、split-exclude、split-include、または bypass のいずれかの場合、Cisco Secure Client は管理トンネル接続を続行します。

管理 VPN プロファイルの更新の制限

管理 VPN プロファイルの更新を新しい AnyConnect ローカル ポリシー ファイル（AnyConnectLocalPolicy.xml）設定を使用した特定の信頼できるサーバリストに制限しても、ユーザが任意のサーバから VPN プロファイルを更新するのを許可することができます。この設定は、[AnyConnect VPN ローカル ポリシー エディタ（AnyConnect VPN Local Policy Editor）] を使用して [任意のサーバからの管理 VPN プロファイル更新を許可（Allow Management VPN Profile Updates From AnyServer）] チェック ボックスをオンにすることで編集できます。

たとえば、管理 VPN プロファイルの更新が VPN サーバー TrustedServer からのみ許可される場合、このチェックボックスはオフになっており、TrustedServer は信頼できるサーバーリストに追加されます。（TrustedServer を該当する VPN プロファイルのサーバ エントリに存在する FQDN または IP アドレスと置き換えてください）。

管理 VPN トンネル接続問題のトラブルシューティング

クライアント ホストがリモートから到達できない場合、さまざまなシナリオが発生して管理 VPN トンネルの切断や確立できない状況の原因となっている可能性があります。次のシナリオでは、Cisco Secure Client GUI と CLI に管理接続状態が統計情報のエントリとして反映されます。

- [切断（無効）（Disconnected (disabled)）]：機能は無効です。
- [切断（信頼ネットワーク）(Disconnected (trusted network)）]：TND が信頼ネットワークを検出したため、管理トンネルは確立されません。
- [切断（アクティブ ユーザ トンネル）（Disconnected (user tunnel active)）]：ユーザ トンネルは現在保留中 です（つまり、管理トンネルを切断しています）。
- [切断（プロセスの起動に失敗）（Disconnected (process launch failed)）]：管理トンネル接続の試行時にプロセスの起動エラーが発生しました。
- [切断（接続に失敗）（Disconnected (connect failed)）]：管理トンネルの確立時に接続障害が発生しました。
- [切断された（無効な VPN 設定）（Disconnected (invalid VPN configuration)）]：管理トンネルの確立時に無効なスプリットトンネリング設定が発生しました。追加情報については、「Tunnel-All 設定をサポートするカスタム属性の設定 （32 ページ）」を参照してください。
- [切断（ソフトウェアアップデートが保留中）（Diconnected (software update pending)）]：Cisco Secure Client ソフトウェアアップデートは現在保留中です（つまり、管理トンネルを切断しています）。
- [切断（Disconnected）]：管理トンネルを確立しようとしているか、その他の理由により確立できませんでした。

管理 VPN トンネル経由の接続の欠落をトラブルシューティングする場合は（クライアント ホストで確立されることを想定）、次を確認します。

- 管理 VPN 接続の状態を Cisco Secure Client UI の [統計出力のエクスポート（Export Stats output）] の [統計（Statistics）] タブをで確認するか、CLI で [接続情報/管理接続状態（Connection Information/Management Connection State）] を確認します。管理接続状態が予期せずに [切断（disconnected）] と表示され、提供された説明が不十分な場合、詳細なトラブルシューティングについて DART ツールを使用した Cisco Secure Client ログをキャプチャします。
- UI の統計行に [管理接続状態：切断（無効）（Management Connection State: Disconnected (disabled)）] と表示される場合、証明書認証で設定されたトンネル グループを指す、1 つのホスト エントリで管理 VPN プロファイルが設定されていることを確認します。関連付けられているグループ ポリシーに 1 つのプロファイル（管理 VPN プロファイル）が設定されている必要があります。

（注） 関連付けられているグループポリシーでバナーを有効にすることはできません。管理のトンネル接続中にユーザのインタラクションはサポートされていません。

- UI の統計行に [管理接続状態：切断（無効）（Management Connection State: Disconnected (disabled)）] と表示される場合、正規のユーザ トンネル接続で使用されるトンネル グルー

プに関連付けられているグループ ポリシー内で管理 VPN プロファイルが設定されていることを確認します。ユーザがそのトンネル グループに接続すると、管理 VPN プロファイルがダウンロードされ、この機能が有効になります。

（注） また、管理 VPN プロファイルをアウト オブ バンドで展開できます。

- UI の統計行に [管理接続状態：切断（接続に失敗）（Management Connection State: Disconnected (connect failed)）] と表示される場合、次に示すように、管理トンネル接続はユーザのインタラクションが必要な場合に常に失敗することに注意してください。
  - サーバー証明書が信頼されない場合。サーバー証明書のルート CA 証明書は、マシン証明書ストア内に存在する必要があります。
  - （マシン ストア証明書に関連する）秘密キーがパスワードで保護されている場合、対応するクライアント証明書は管理トンネル接続で使用できません。秘密キーのパスワードを入力するようユーザにプロンプトを表示できないため、クライアント証明書は使用できません。
  - macOS システム キーチェーン プライベート キーが、Cisco Secure Client エージェント実行可能ファイル（vpnagentd）にプロンプトを表示せずにアクセスを許可するように設定されていない場合、秘密鍵にアクセスするためのクレデンシャルをユーザーに要求することができないため、対応するクライアント証明書は管理トンネル接続では使用できません。
  - グループ ポリシーがバナーを使用して設定されている場合。

Cisco Secure Client プロキシ接続の設定

Cisco Secure Client プロキシ接続について

Cisco Secure Client は、ローカルプロキシ、パブリックプロキシ、プライベートプロキシで VPN セッションをサポートしています。

- ローカル プロキシ接続：

  ローカルプロキシは、Cisco Secure Client と同じ PC 上で動作し、トランスペアレントプロキシとして使用されることもあります。トランスペアレント プロキシ サービスの例として、一部のワイヤレス データ カードによって提供されるアクセラレーション ソフトウェアや、一部のアンチウイルス ソフトウェア（Kaspersky など）に搭載のネットワーク コンポーネントなどがあります。

  ローカルプロキシの使用は、Cisco Secure Client プロファイルで有効または無効にします。「ローカル プロキシ接続の許可」を参照してください。

- パブリック プロキシ接続：

  通常、パブリック プロキシは Web トラフィックの匿名化に使用されます。Windows がパブリック プロキシを使用するように設定されている場合、Cisco Secure Client はその接続を使用します。パブリック プロキシは macOS と Linux でネイティブと上書きの両方をサポートしています。

  パブリックプロキシの設定についてパブリック プロキシ （36 ページ）は、を参照してください。

- プライベート プロキシ接続：

  プライベート プロキシ サーバーは、企業の使用ポリシーに基づいて企業ユーザーが特定の Web サイト（たとえば、アダルト、ギャンブル、ゲームなどのサイト）にアクセスできないようにするために社内ネットワークで使用されます。

  トンネルの確立後にブラウザにプライベート プロキシ設定をダウンロードするようにグループ ポリシーを設定します。VPN セッションが終了すると、設定は元の状態に復元されます。プライベート プロキシ接続の設定 （37 ページ）を参照してください。

（注） プロキシサーバーを経由する Cisco Secure Client SBL 接続は、Windows オペレーティングシステムのバージョン、システム（マシン）の設定、またはその他のサードパーティ プロキシ ソフトウェア機能に依存します。このため、Microsoft または使用するすべてのサードパーティ プロキシ アプリケーションによって提供される、システム全体のプロキシ設定を参照してください。

VPN クライアント プロファイルによるクライアント プロキシの制御

VPN クライアント プロファイルでは、クライアント システムのプロキシ接続をブロックしたり、リダイレクトしたりできます。Windows および Linux の場合、パブリック プロキシ サーバのアドレスを自分で設定したり、ユーザーに設定を許可したりできます。

VPN クライアントプロファイルにプロキシ設定を設定する方法の詳細については、Cisco Secure Client プロファイルエディタ、プリファレンス（Part 2）を参照してください。

クライアントレス サポートのためのプロキシ自動設定ファイルの生成

Cisco Secure Firewall ASA の一部のバージョンでは、Cisco Secure Client セッションの確立後にプロキシサーバーを介したクライアントレス ポータル アクセスをサポートするため、Cisco Secure Client 設定を作成する必要があります。Cisco Secure Client は、プロキシ自動構成（PAC）ファイルを使用して、クライアント側のプロキシ設定を変更して、これを実行できるようにします。Cisco Secure Client は、Secure Firewall ASA がプライベート側のプロキシ設定を指定しない場合にのみ、このファイルを生成します。

Cisco Secure Client プロキシ接続の要件

プロキシ接続の OS サポートは次のようになります。

プロキシ接続タイプ	Windows	macOS	Linux
ローカル プロキシ	○	○（上書きおよびネイティブ）	○
プライベート プロキシ	○（Internet Explorer）	○（システム プロキシ設定として設定）	×
パブリック プロキシ	○（IEおよび上書き）	○（上書きおよびネイティブ	○（上書きおよびネイティブ）

プロキシ接続の制限

- プロキシ経由の接続は、Always-On機能が有効になっている場合にはサポートされません。
- ローカル プロキシへのアクセスを許可するには、VPN クライアント プロファイルが必要です。

ローカル プロキシ接続の許可

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [ローカル プロキシ接続を許可（Allow Local Proxy Connections）] を選択（デフォルト）または選択解除します。ローカル プロキシはデフォルトで無効になっています。

パブリック プロキシ

パブリック プロキシはWindowsおよびLinuxの各プラットフォームでサポートされています。プロキシ サーバは、クライアント プロファイルで設定されるプリファレンスに基づいて選択されます。プロキシオーバーライドの場合、Cisco Secure Client はプロファイルからプロキシサーバーを取得します。リリース 4.1 以降では、Linux および macOS でのネイティブプロキシ構成とともに macOS でのプロキシサポートが追加されました。

Linux では、Cisco Secure Client の実行前にネイティブプロキシ設定がエクスポートされます。設定を変更した場合は、再起動が必要です。

プロキシサーバーの認証には、ユーザー名とパスワードが必要です。Cisco Secure Client は、プロキシサーバーが認証を要求するように構成されている場合、基本認証と NTLM 認証をサポートします。Cisco Secure Clientダイアログは認証プロセスを管理します。プロキシサーバーに対する認証に成功すると、Cisco Secure Client は Cisco Secure Firewall ASA ユーザー名およびパスワードの入力を求めます。

パブリック プロキシ接続の設定（Windows）

Windows でパブリック プロキシ接続を設定するには、次の手順を実行します。

ステップ 1 Internet Explorer またはコントロール パネルから [インターネット オプション（Internet Options）] を開きます。

ステップ 2 [接続（Connections）] タブを選択し、[LAN 設定（LAN Settings）] ボタンをクリックします。

ステップ 3 プロキシ サーバを使用するように LAN を設定し、プロキシ サーバの IP アドレスを入力します。

パブリック プロキシ接続の設定（macOS）

ステップ 1 システム設定に移動し、接続している適切なインターフェイスを選択します。

ステップ 2 [詳細設定（Advanced）] をクリックします。

ステップ 3 新しいウィンドウで [プロキシ（Proxies）] タブを選択します。

ステップ 4 HTTPS プロキシを有効にします。

ステップ 5 右側のパネルの [セキュアプロキシサーバ（Secure Proxy Server）] フィールドに、プロキシ サーバのアドレスを入力します。

パブリック プロキシ接続の設定（Linux）

Linux でパブリック プロキシ接続を設定するには、環境変数を設定します。

プライベート プロキシ接続の設定

ステップ 1 Cisco Secure Firewall ASA グループポリシーにプライベートプロキシ情報を設定します。『Cisco ASA Series VPN CLI or ASDM Configuration Guide』[英語] の「Configuring a Browser Proxy for an Internal Group Policy」の項を参照してください。

（注） macOS 環境では、（VPN 接続時に）Cisco Secure Firewall ASA からプッシュダウンされたプロキシ情報は、端末を開いて **scutil --proxy** を発行するまで、ブラウザに表示されません。

ステップ 2 （任意）ブラウザのプロキシ設定を無視するためのクライアントの設定。

ステップ 3 （任意）Internet Explorer の [接続（Connections）] タブのロックダウン。

次のタスク

（注） プロキシ経由で開始された VPN セッションがアクティブな場合、プロキシ経由のネットワークアクセスは Cisco Secure Client に関連するプロセスのみに制限されます。したがって、HTTP/HTTPS を介して通信するサードパーティ アプリケーションに対応するには、VPN ポリシーのプライベートプロキシ設定を、[プロキシを使用しない（Do not use proxy）] など、[クライアントプロキシ設定を変更しない（Do not modify client proxy settings）] 以外に設定する必要があります。または、VPN プロファイルのプロキシ設定を構成して、VPN 接続の開始時にシステムプロキシ設定を無視することもできます。

ブラウザのプロキシ設定を無視するためのクライアントの設定

Cisco Secure Client プロファイルでは、ユーザーの PC 上で Microsoft Internet Explorer または Safari のプロキシ設定が無視されるようにポリシーを指定できます。これにより、ユーザーは社内ネットワークの外部からトンネルを確立できなくなり、Cisco Secure Client は望ましくないまたは違法なプロキシサーバー経由で接続できなくなります。

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 [プロキシ設定（Proxy Settings）] ドロップダウン リストで、[プロキシを無視（Ignore Proxy）] を選択します。[プロキシを無視（Ignore Proxy）] を選択すると、クライアントはすべてのプロキシ設定を無視します。Cisco Secure Firewall ASA からダウンロードされるプロキシに対してアクションが実行されません。

Internet Explorer の [接続（Connections）] タブのロックダウン

ある条件下では、Cisco Secure Client によって Internet Explorer の [ツール（Tools）] > [インターネット オプション（Internet Options）] > [接続（Connections）] タブが非表示にされます。このタブが表示されている場合、ユーザーはプロキシ情報を設定できます。このタブを非表示にすると、ユーザーが意図的または偶発的にトンネルを迂回することを防止できます。タブのロックダウンは接続解除すると反転され、このタブに適用される管理者定義のポリシーの方が優先されます。このロックダウンは、次のいずれかの条件で行われます。

- Cisco Secure Firewall ASA の設定で、[接続（Connections）] タブのロックダウンが指定されている。
- Cisco Secure Firewall ASA の設定で、プライベート側プロキシが指定されている。
- Windows のグループポリシーにより、以前に [接続（Connections）] タブがロックされている（no lockdown Cisco Secure Firewall ASA グループポリシー設定の上書き）。

グループポリシーで、プロキシのロックダウンを許可する、または許可しないように Cisco Secure Firewall ASA を設定できます。ASDM を使用してこれを設定する手順は次のとおりです。

ステップ 1 ASDM で、**[設定（Configuration）]** > **[リモート アクセス VPN（Remote Access VPN）]** > **[ネットワーク（クライアント）アクセス（Network (Client) Access）]** > **[グループ ポリシー（Group Policies）]** に移動します。

ステップ 2 グループ ポリシーを選択し、新しいグループ ポリシーの [編集（Edit）] または [追加（Add）] をクリックします。

ステップ 3 ナビゲーションペインで、**[詳細（Advanced）]**>**[ブラウザプロキシ（Browser Proxy）]** に移動します。[プロキシ サーバ ポリシー（Proxy Server Policy）] ペインが表示されます。

ステップ 4 **[プロキシ ロックダウン（Proxy Lockdown）]** をクリックして、その他のプロキシ設定を表示します。

ステップ 5 プロキシのロックダウンを有効にして、Cisco Secure Client のセッション中は Internet Explorer の [接続（Connections ）] タブを非表示にするには、[継承（Inherit）] をオフにして [はい（Yes）] を選択します。または、プロキシのロックダウンを無効にして、Cisco Secure Client のセッション中は Internet Explorer の [接続（Connections ）] タブを表示するには、[いいえ（No）] を選択します。

ステップ 6 [OK] をクリックして、プロキシ サーバ ポリシーの変更を保存します。

ステップ 7 [適用（Apply）] をクリックして、グループ ポリシーの変更を保存します。

プロキシ設定の確認

- Windows の場合：次の場所でレジストリのユーザーおよびシステムのプロキシ設定を検索します。

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Connections
```

- macOS の場合：ターミナル ウィンドウを開き、次を入力します。

```
scutil --proxy
```

VPN トラフィックの選択および除外

VPN をバイパスするための IPv4 または IPv6 トラフィックの設定

ASA が IPv6 トラフィックのみを待機している場合は Cisco Secure Client が IPv4 トラフィックをどのように管理するかを設定し、Cisco Secure Firewall ASA がClient Bypass Protocol 設定を使用して IPv4 トラフィックのみを待機している場合は Cisco Secure Client クライアントが IPv6 トラフィックをどのように管理するかを設定できます。

Cisco Secure Clientで Cisco Secure Firewall ASA に VPN 接続をする場合、ASA はクライアントに IPv4、IPv6、または IPv4 および IPv6 両方のアドレスを割り当てる場合があります。

Client Bypass Protocol が IP プロトコルに対して有効であり、かつ、あるアドレスプールがそのプロトコルに対して設定されていない（つまり、そのプロトコルの IP アドレスが Cisco Secure Firewall ASA によってクライアントに割り当てられていない）場合、そのプロトコルを使用する IP トラフィックは VPN トンネルを介して送信されません。これは、トンネル外で送信されます。

クライアント バイパス プロトコルが無効であり、かつ、あるアドレス プールがそのプロトコル用に設定されていない場合、VPN トンネルが確立された後、クライアントではその IP プロトコルのすべてのトラフィックをドロップします。

たとえば、Cisco Secure Firewall ASA が Cisco Secure Client 接続に IPv4 アドレスのみを割り当て、エンドポイントがデュアルスタックされていると想定します。エンドポイントが IPv6 アドレスへの到達を試みた場合、クライアントバイパスプロトコルが無効になっていると、IPv6 トラフィックはドロップされます。クライアントバイパスプロトコルが有効になっていると、IPv6 トラフィックはクライアントからクリア テキストで送信されます。

SSL 接続ではなく IPsec トンネルを確立している場合は、クライアントで IPv6 が有効になっているかどうかが Cisco Secure Firewall ASA に通知されないため、Cisco Secure Firewall ASA は常に Client Bypass Protocol 設定をプッシュダウンします。

Client Bypass Protocol を Cisco Secure Firewall ASA でグループポリシーに設定します。

ステップ 1 ASDM で、**[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）]** に移動します。

ステップ 2 グループ ポリシーを選択し、新しいグループ ポリシーの [編集（Edit）] または [追加（Add）] をクリックします。

ステップ 3 **[詳細（Advanced）] > [AnyConnect]** を選択します。

ステップ 4 デフォルト グループ ポリシー以外のグループ ポリシーの場合、[クライアント バイパス プロトコル（Client Bypass Protocol）] の隣にある [継承（Inherit）] チェックボックスをオフにします。

ステップ 5 次のオプションのいずれかを選択します。

- Cisco Secure Firewall ASA がアドレスを割り当てなかった IP トラフィックをドロップする場合は、[無効（Disable）] をクリックします。
- その IP トラフィックをクリア テキストで送信する場合は、[有効（Enable）] をクリックします。

ステップ 6 [OK] をクリックします。

ステップ 7 [Apply] をクリックします。

ローカル プリンタおよびテザー デバイスをサポートしたクライアント ファイアウォールの設定

『Cisco ASA Series VPN CLI or ASDM Configuration Guide』[英語] の「*Client Firewall with Local Printer and Tethered Device Support*」の項を参照してください。

スプリット トンネリングの設定

スプリット トンネリングは、[ネットワーク（クライアント）アクセス（Network (Client) Access）] グループ ポリシーに設定します。『Cisco ASA Series VPN CLI or ASDM Configuration Guide』[英語] の「*Configure Split Tunneling for AnyConnect Traffic*」の項を参照してください。

ASDM でグループ ポリシーに変更を加えたら、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] > [追加/編集（Add/Edit）] > [グループ ポリシー（Group Policy）] で、グループ ポリシーを接続プロファイルに関連付けてください。

Linux でのネットワーク トラフィックのルーティング

Linux ユーザーが VM インスタンス/Docker コンテナでネットワーク トラフィックをルーティングできるようにするには、新しいカスタム属性を作成して有効にする必要があります。**tunnel-from-any-source** カスタム属性を作成し、*true* に設定すると、Cisco Secure Client は、split-include または split-exclude トンネルモードの任意の送信元アドレスを持つパケットを許可し、VM インスタンスまたは Docker コンテナ内のネットワークアクセスを許可します。

（注） VM インスタンスまたは Docker コンテナで使用されるネットワークは、最初にトンネルから除外する必要があります。

ダイナミック スプリット トンネリングについて

ダイナミック スプリット トンネリングは、ASDM グループポリシー設定で [次のネットワークリストを除外（Exclude Network List Below）] または [次のネットワークリストをトンネリング（Tunnel Network List Below）] オプションを使用して設定されるスタティック スプリット トンネリング オプションを強化するために設計されました。スプリット トンネリングを定義するために通常使用される静的な包含または除外と違い、ダイナミック スプリット トンネリングでの包含または除外は、特定のサービスに関するトラフィックを VPN トンネリングから除外するまたは VPN トンネリングに包含する必要があるシナリオに対応しています。IP プロトコルごとに個別のスプリットトンネリング設定を構成できません。たとえば、IPv4 にダイナミックスプリット包含トンネリング（IPv4 スプリット包含ドメインやダイナミックスプリット包含ドメインなど）を有効にすると、IPv6 にダイナミックスプリット除外トンネリング（IPv6 Tunnel-all やダイナミックスプリット除外ドメインなど）を有効にできません。さらに、拡張

ダイナミック スプリット トンネリングを提供します。ダイナミックスプリット除外ドメインとダイナミックスプリット包含ドメインの両方が拡張ドメイン名の一致に指定されています。

制限は、スタティック スプリット トンネリングからダイナミック スプリット トンネリングまでさまざまです。スタティック スプリット トンネリングの場合、IP プロトコルあたり 2500 ネットワーク/ACE に制限されます。ダイナミック スプリット トンネリングでは、Cisco Secure Client はヘッドエンドによってプッシュされるドメインリストの最初の 20,000 文字によるダイナミック スプリット トンネリング ドメインのみを考慮し、クライアントでの切り捨てによってのみ適用されます。ワイルドカードは使用できません。ダイナミックスプリット除外とダイナミックスプリット包含の両方で、設定されたドメインに加えて、そのサブドメインもすべてトンネルから除外されます（または、ダイナミックスプリット包含に含まれます）。

ダイナミック スプリット除外トンネリング：複数のクラウドベースのサービスが同じ IP プールにホストされており、ユーザの場所またはクラウド上のコンピュータ資源の負荷に応じて異なる IP アドレスへと解決される場合があります。そのようなサービスのうち 1 つだけを VPN トンネルから除外したい場合、管理者が静的な除外を使用してそのためのポリシーを定義するのは、特に ISP NAT、6to4、4to6 などのネットワーク変換スキームも考慮される場合は困難です。ダイナミック スプリット除外トンネリングでは、トンネルの確立後に、ホストの DNS ドメイン名に基づいて動的にスプリット除外トンネリングをプロビジョニングできます。たとえば、VPN 管理者は、実行時に example.com を VPN トンネルから除外するように設定できます。VPN トンネルがアップしているときにアプリケーションが mail.example.com に接続しようとすると、VPN クライアントは、自動的にシステム ルーティング テーブルとフィルタを変更し、トンネル外部への接続を許可します。

拡張ダイナミックスプリット除外トンネリング：ダイナミックスプリット除外トンネリングがダイナミックスプリット除外ドメインとダイナミックスプリット包含ドメインの両方で設定されている場合、VPN トンネルから動的に除外されたトラフィックは少なくとも 1 つのダイナミックスプリット除外ドメインに一致する必要がありますが、ダイナミックスプリット包含ドメインに一致する必要はありません。たとえば、VPN 管理者がダイナミック スプリット除外ドメイン example.com とダイナミック スプリット包含ドメイン mail.example.com を設定した場合、mail.example.com 以外のすべての example.com トラフィックはトンネリングから除外されます。

ダイナミック スプリット包含トンネリング：ダイナミック スプリット包含トンネリングでは、トンネルの確立後に、ホストの DNS ドメイン名に基づいて動的にスプリット包含トンネリングをプロビジョニングできます。たとえば、VPN 管理者は、実行時に domain.com を VPN トンネルに含めるように設定できます。VPN トンネルがアップしているときにアプリケーションが www.domain.com に接続しようとすると、VPN クライアントは、自動的にシステム ルーティング テーブルとフィルタを変更し、VPN トンネル内部での接続を許可します。

拡張ダイナミック スプリット包含トンネリング：ダイナミック スプリット包含トンネリングがダイナミック スプリット包含ドメインとダイナミック スプリット除外ドメインの両方で設定されている場合、VPN トンネルに動的に包含されたトラフィックは少なくとも 1 つのダイナミック スプリット包含ドメインに一致する必要がありますが、ダイナミック スプリット除外ドメインに一致する必要はありません。たとえば、VPN 管理者が domain.com をスプリット包含ドメインとして、www.domain.com をスプリット除外ドメインとして設定した場合、www.domain.com 以外のすべての domain.com トラフィックがトンネリングされます。

（注） ダイナミック スプリット トンネリングは、Linux またはモバイルプラットフォームではサポートされていません。

スタティック スプリット トンネリングとダイナミック スプリット トンネリングの相互運用性

静的な除外と動的な除外は共存可能です。スタティック スプリット トンネリングはトンネルの確立時に適用され、ダイナミック スプリット トンネリングは、トンネルが接続済みとなっているときにドメインへのトラフィックが発生すると適用されます。

ダイナミック スプリット除外トンネリング

ダイナミック スプリット除外トンネリングは、「tunnel all」、「split include」、および「split exclude」トンネリングに適用されます。

- すべてのネットワークをトンネリングする：VPN トンネルからの除外は、すべて動的です。
- 特定のネットワークを除外する：事前設定された静的な除外に動的な除外が追加されます。
- 特定のネットワークを包含する：除外されるホスト名の IP アドレスのうち、スプリットを含むネットワークと重複する場合のみ、動的な除外が適用されます。それ以外の場合、トラフィックは VPN トンネルからすでに除外されているため、動的な除外は行われません。

拡張ダイナミック スプリット除外トンネリングは、「tunnel all」および「split exclude」トンネリングに適用されます。ダイナミック スプリット除外ドメインとダイナミック スプリット包含ドメインの両方、およびスプリット包含トンネリングが設定されている場合、その結果の設定は拡張ダイナミック スプリット包含トンネリングになります。

ダイナミック スプリット包含トンネリング

ダイナミック スプリット包含トンネリングは、スプリット包含設定にのみ適用されます。

拡張ダイナミック スプリット包含トンネリングは、スプリット包含設定にのみ適用されます。

（注） Umbrella ローミング セキュリティによる保護は、スタティックまたはダイナミック スプリット トンネリングのいずれかが有効になっていると、アクティブになります。Cisco Umbrella クラウドリゾルバは、到達可能であり、かつ、VPN トンネルによるプローブが可能である場合を除き、VPN トンネルから静的に包含または除外することが必要となる場合があります。

スプリット トンネリング設定をともなう重複シナリオの結果

動的な包含または除外の対象は、まだ包含または除外されていない IP アドレスのみです。静的トンネリングおよび何らかの形式の動的トンネリングの両方が適用されており、新たな包含または除外を強制する必要がある場合、すでに適用された包含または除外との衝突が発生する可能性があります。動的な除外（除外されるドメイン名と一致する DNS 応答の一部となっているすべての IP アドレスが対象）が実行される場合、除外において考慮されるのは、まだ除外されていないアドレスのみです。同様に、動的な包含（包含されるドメイン名と一致する DNS 応答の一部となっているすべての IP アドレスが対象）が実行される場合、包含において考慮されるのは、まだ包含されていないアドレスのみです。

静的なパブリック ルート（セキュア ゲートウェイ ルートなどのスプリット除外ルートやクリティカル ルートなど）は、ダイナミック スプリット包含ルートよりも優先されます。そのため、動的な包含の少なくとも 1 つの IP アドレスが静的なパブリック ルートと一致する場合、動的な包含は強制されません。

同様に、静的スプリット包含ルートはダイナミック スプリット除外ルートよりも優先されます。そのため、動的な除外の少なくとも 1 つの IP アドレスが静的スプリット包含ルートと一致する場合、動的な除外は強制されません。

ダイナミック スプリット トンネリングの使用状況の通知

VPN トンネルの接続中は、ダイナミック スプリット トンネリングに何が設定されているかをいくつかの方法で確認できます。

- [統計（Statistics）] タブ：Cisco Secure Firewall ASA グループポリシーで設定されている VPN トンネルから除外された、または VPN トンネルに包含されたドメイン名を含むダイナミックトンネル除外およびダイナミックトンネル包含が表示されます。
- [エクスポート統計（Export Stats）]：VPN トンネリングから除外された、または VPN トンネリングに包含されたドメイン名と、IPv4 と IPv6 の両方のトンネル モードを含むファイルが生成されます。ダイナミック ルートもエクスポートされた統計に含まれます。
- [ルートの詳細（Route Details）] タブ：除外または包含された各 IP アドレスに対応するホスト名を持つ IPv4 および IPv6 ダイナミック スプリット除外および包含ルートが表示されます。

（注） Cisco Secure Client UI には、AnyConnect VPN が実現する保護されたルートまたは保護されていないルートが、IP プロトコルにつき最大 200 個表示されます。ルートの数が 200 を超えると、切り捨てが発生します。すべてのルートを表示するには、Windows では **route print** を実行し、Linux または macOS では **netstat -rn** を実行します。

- VPN の設定ログ メッセージ：VPN トンネルから除外された、または VPN トンネルに包含されたドメインの数が示されます。

ダイナミック スプリット除外トンネリングの設定

始める前に

ダイナミック スプリット トンネリングについて （41 ページ） を参照してください。

ダイナミック スプリット トンネリングでは、トンネルの確立後に、DNS ドメイン名に基づいて動的にスプリット除外トンネリングを行うことができます。ダイナミック スプリット トンネリングを設定するには、Cisco Secure Firewall ASA 上でカスタム属性を作成し、グループポリシーに追加します。GUI の手順については、『Cisco ASA Series VPN ASDM Configuration Guide』[英語] の「*Configure Dynamic Split Tunneling*」を参照してください。

ステップ 1 次のコマンドを使用して、WebVPN コンテキストでカスタム属性タイプを定義します。

```
anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude domains
```

ステップ 2 VPN トンネル外部のクライアントによるアクセスが必要な各クラウド/Web サービスについて、属性名を定義します。たとえば、Google Web サービスに関する DNS ドメイン名のリストとして、Google_domains を追加します。この属性値には、VPN トンネルから除外するドメイン名のリストが含まれており、例として次のようにカンマ区切り値（CSV）形式にする必要があります。

```
anyconnect-custom-data dynamic-split-exclude-domains example_service_domains example1.com, example2.com
```

ステップ 3 次のコマンドを使用して、以前に定義されているカスタム属性を特定のポリシー グループに追加します。これは、group-policy 属性のコンテキストで実行されます。

```
anyconnect-custom dynamic-split-exclude-domains value example_service_domains
```

拡張ダイナミック スプリット除外トンネリングの設定

始める前に

ダイナミック スプリット トンネリングについて （41 ページ） を参照してください。

ダイナミック スプリット除外トンネリングがダイナミック スプリット除外ドメインとダイナミック スプリット包含ドメインの両方で設定されている場合、拡張ドメイン名照合がサポートされています。拡張ダイナミックスプリット除外トンネリングを設定するには、Cisco Secure Firewall ASA 上で 2 つのカスタム属性を作成し、グループポリシーに追加します。GUI の手順については、『Cisco ASA Series VPN ASDM Configuration Guide』[英語] の「*Configure Dynamic Split Tunneling*」を参照してください。

ステップ 1 次のコマンドを使用して、WebVPN コンテキストでカスタム属性タイプを定義します。

```
anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude domains
```

ステップ 2 VPN トンネル外部のクライアントによるアクセスが必要な各クラウド/Web サービスについて、属性名を定義します。たとえば、example.com がダイナミック スプリット除外ドメインで、www.example.com がダイナミック スプリット包含ドメインである場合、examples.com へのすべてのトラフィックは www.example.com

を除いて除外されます。この属性値には、VPN トンネルから除外する（またはしない）ドメイン名のリストが含まれており、例として次のようにカンマ区切り値（CSV）形式にする必要があります。

```
anyconnect-custom-data dynamic-split-exclude-domains example_service_domains example1.com, example2.com
anyconnect-custom-data dynamic-split-include-domains example_service_domains_tunneled www.example1.com,
 www.example2.com
```

ステップ 3 次のコマンドを使用して、以前に定義されているカスタム属性を特定のポリシー グループに追加します。これは、group-policy 属性のコンテキストで実行されます。

```
anyconnect-custom dynamic-split-exclude-domains value
example_service_domains
anyconnect-custom dynamic-split-include-domains value
example_service_domains_tunneled
```

ダイナミック スプリット包含トンネリングの設定

始める前に

ダイナミック スプリット トンネリングについて （41 ページ） を参照してください。

ダイナミック スプリット トンネリングでは、トンネルの確立後に、ホストの DNS ドメイン名に基づいて動的にスプリット包含トンネリングをプロビジョニングできます。ダイナミック スプリット トンネリングを設定するには、Cisco Secure Firewall ASA 上でカスタム属性を作成し、グループポリシーに追加します。GUI の手順については、『Cisco ASA Series VPN ASDM Configuration Guide』[英語] の「*Configure Dynamic Split Tunneling*」を参照してください。

ステップ 1 次のコマンドを使用して、WebVPN コンテキストでカスタム属性タイプを定義します。

```
anyconnect-custom-attr dynamic-split-include-domains description dynamic split include domains
```

ステップ 2 VPN トンネルによるクライアント アクセスが必要な各クラウド/Web サービスについて、カスタム属性名を定義します。この属性値には、VPN トンネルに包含するドメイン名のリストが含まれており、例として次のようにカンマ区切り値（CSV）形式にする必要があります。

```
anyconnect-custom-data dynamic-split-include-domains corporate_service_domains domain1.com, domain2.com
```

（注） カスタム属性は 421 文字以内である必要があります。制限を超えると、動的に包含されたドメインのリスト（CSV 形式）を 小さな値に分割する必要がある場合があります。

ステップ 3 次のコマンドを使用して、以前に定義されているカスタム属性を特定のポリシー グループに追加します。これは、group-policy 属性のコンテキストで実行されます。

```
anyconnect-custom dynamic-split-include-domains value
corporate_service_domains
```

拡張ダイナミック スプリット包含トンネリングの設定

始める前に

ダイナミック スプリット トンネリングについて （41 ページ） を参照してください。

ダイナミック スプリット包含トンネリングがダイナミック スプリット包含ドメインとダイナミック スプリット除外ドメインの両方で設定されている場合、拡張ドメイン名照合がサポートされています。拡張ダイナミックスプリット包含トンネリングを設定するには、Cisco Secure Firewall ASA 上で 2 つのカスタム属性を作成し、グループポリシーに追加します。GUI の手順については、『Cisco ASA Series VPN ASDM Configuration Guide』[英語] の「*Configure Dynamic Split Tunneling*」を参照してください。

ステップ 1 次のコマンドを使用して、WebVPN コンテキストでカスタム属性タイプを定義します。

```
anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude domains
```

ステップ 2 VPN トンネルからのクライアント アクセスが必要な各クラウド/Web サービスについて、カスタム属性名を定義します。たとえば、domain.com がダイナミック スプリット包含ドメインであり、www.domain.com がダイナミック スプリット除外ドメインである場合、domain.com へのすべてのトラフィックは www.domain.com を除いて包含されます。属性値には、VPN トンネルに包含する（またはしない）ドメイン名のリストが含まれており、例として次のようにカンマ区切り値（CSV）形式にする必要があります。

```
anyconnect-custom-data dynamic-split-include-domains corporate_service_domains domain1.com, domain2.com
anyconnect-custom-data dynamic-split-include-domains corporate_service_domains_excluded
www.domain1.com, www.domain2.com
```

ステップ 3 次のコマンドを使用して、以前に定義されているカスタム属性を特定のポリシー グループに追加します。これは、group-policy 属性のコンテキストで実行されます。

```
anyconnect-custom dynamic-split-include-domains value
corporate_service_domains
anyconnect-custom dynamic-split-exclude-domains value
corporate_service_domains_excluded
```

スプリット DNS

スプリット DNS は、スプリット包含とスプリット除外の両方のトンネリング構成でサポートされます。

スプリット包含トンネリングのスプリット DNS が [ネットワーク（クライアント）アクセス（Network (Client) Access）] グループポリシーに設定されている場合、Cisco Secure Client は、特定の DNS クエリを VPN DNS サーバー（同様にグループポリシーに設定）にトンネルします。他のすべての DNS クエリは、VPN トンネルの外部でパブリック DNS サーバに送信されます。

スプリット除外トンネリングのスプリット DNS が設定されている場合、特定の DNS クエリは VPN トンネルの外部でパブリック DNS サーバに送信されます。他のすべての DNS クエリは、VPN DNS サーバにトンネルされます。

スプリットトンネリング構成でスプリット DNS が有効になっていない場合、DNS クエリがトンネル経由でルーティングされるのは、グループポリシーで [トンネル経由ですべての DNS ルックアップを送信する（Send All DNS lookups through tunnel）] が設定されている場合のみです。それ以外の場合は、トンネルの外部でルーティングされる可能性もあります。

スプリット DNS の要件

スプリット DNS は、Windows と macOS プラットフォームでサポートされています。

- Linux では限定的なサポートが提供されます。具体的には、トンネル DNS 要求のみがスプリット DNS ポリシーの対象となります。そのため、トンネルの外部に送信される一部の DNS 要求は、スプリット DNS ポリシーに準拠しない可能性があります。

macOS の場合、Cisco Secure Client は、次のいずれかの条件を満たす場合のみ、ある IP プロトコルのトゥルースプリット DNS を使用できます。

- グループ ポリシーで、スプリット DNS が 1 つの IP プロトコル（IPv4 など）に設定されており、クライアント バイパス プロトコルがもう片方の IP プロトコル（IPv6 など）に設定されている（後者の IP プロトコルにはアドレス プールは設定されていない）。
- スプリット DNS が両方の IP プロトコルに設定されている。

一方の IP プロトコルにスプリット包含のスプリット DNS が設定され、もう一方のプロトコルにスプリット除外のスプリット DNS が設定されている場合、スプリット包含のスプリット DNS が優先されるため、Cisco Secure Client はスプリット除外のスプリット DNS 設定を無視します。

スプリット DNS は、名前解決のためにネイティブ/OS DNS クライアントに依存する一般的なアプリケーション（ブラウザやメールアプリケーションなど）にのみ関連します。サポートされないアプリケーションとしては、dig や nslookup など、カスタムのリゾルバを使用するツールが挙げられます。

スプリット包含トンネリングのスプリット DNS の設定

グループポリシーにスプリット包含トンネリングのスプリット DNS を設定するには、次の手順を実行します。

ステップ 1 少なくとも 1 つの DNS サーバを設定します。

『Cisco ASA Series VPN CLI or ASDM Configuration Guide』[英語] の「*Configure Server Attributes for an Internal Group Policy*」の項を参照してください。

指定したプライベート DNS サーバが、クライアント プラットフォームに設定されている DNS サーバとオーバーラップしていないことを確認します。重複していると、名前解決が正しく動作しない可能性があります。

ステップ 2 Split-Include トンネリングを設定します。

[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループ ポリシー（Group Policies）] > [詳細（Advanced）] > [スプリット トンネリング（Split Tunneling）]ペインで、[次のトンネル ネットワーク リスト（Tunnel Network List Below）] を選択し、[ネットワーク リスト（Network List）] にトンネルするアドレスを指定します。

ステップ 3 [設定（Configuration）]>[リモートアクセスVPN（Remote Access VPN）]>[ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループポリシー（Group Policies）] > [詳細（Advanced）] > [スプリットトンネリング（Split Tunneling）]ペインで、[トンネルですべてのDNSルックアップを送信する（Send All DNS lookups through tunnel）] をオフにし、クエリがトンネルされるドメインの名前を [DNS名（DNS Names）] に指定します。

次のタスク

ASDM でグループ ポリシーに変更を加えたら、[設定（Configuration）] > [リモート アクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] > [追加/編集（Add/Edit）] > [グループ ポリシー（Group Policy）] で、グループ ポリシーを接続プロファイルに関連付けてください。

スプリット除外トンネリングのスプリット DNS の設定

グループポリシーにスプリット除外トンネリングのスプリット DNS を設定するには、次の手順を実行します。

ステップ 1 ASDM で、[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [詳細（Advanced）] > [AnyConnectカスタム属性（AnyConnect Custom Attributes）] に移動して新しいカスタム属性タイプを設定します。[追加（Add）] を選択し、[カスタム属性の作成（Create Custom Attribute）] ペインで次の設定を行います。

a) 新しいタイプとして **split-dns-exclude-domains** と入力します。
b) 必要に応じて、説明を入力します。

ステップ 2 作成したタイプの新しいカスタム属性名を設定するには、[追加（Add）] を選択し、[カスタム属性名の作成（Create Custom Attribute Name）] ペインで次のように設定します。

a) タイプとして **split-dns-exclude-domains** を選択します。
b) 名前を入力します。
c) 値には、クエリをトンネリングしないドメイン名のカンマ区切りリストを入力します。
クライアントは、300 個までそのようなドメインを受け入れます。ワイルドカードは使用できません。

ステップ 3 [追加（Add）] を選択し、[カスタム属性の作成（Create Custom Attribute）] ペインで次の設定を行います。

a) [属性タイプ（Attribute Type）] フィールドで、ステップ 1 で作成したタイプを選択します。
b) [値（Value）] フィールドで、ステップ 2 で作成した名前を選択します。

ステップ 4 少なくとも 1 つの VPN DNS サーバを設定します。

『Cisco ASA Series VPN CLI or ASDM Configuration Guide』[英語] の「*Configure Server Attributes for an Internal Group Policy*」の項を参照してください。

指定したプライベート DNS サーバが、クライアント プラットフォームに設定されている DNS サーバとオーバーラップしていないことを確認します。重複していると、名前解決が正しく動作しない可能性があります。

ステップ 5 スプリット除外トンネリングまたはダイナミックスプリット除外トンネリングを設定します。

[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループポリシー（Group Policies）] > [詳細（Advanced）] > [スプリットトンネリング（Split Tunneling）] ペインで、[次のネットワークリストを除外（Exclude Network List Below）] ポリシーを選択し、[ネットワークリスト（Network List）] に除外するアドレスを指定します。

詳細については、ダイナミック スプリット除外トンネリングの設定 （45 ページ）を参照してください。スプリット包含トンネリングを使用したダイナミックスプリット除外の構成はサポートされていません。

ステップ 6 [設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [グループポリシー（Group Policies）] > [詳細（Advanced）] > [スプリットトンネリング（Split Tunneling）] ペインで、[トンネルですべてのDNSルックアップを送信する（Send All DNS lookups through tunnel）] をオフにします。

次のタスク

ASDM でグループポリシーに変更を加えたら、**[設定（Configuration）] > [リモートアクセス VPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect接続プロファイル（AnyConnect Connection Profiles）] > [追加/編集（Add/Edit）] > [グループポリシー（Group Policy）]** で、グループポリシーを接続プロファイルに関連付けてください。

Cisco Secure Client ログを使用したスプリット DNS の確認

スプリット DNS が有効であることを確認するには、Cisco Secure Client のログで、「Received VPN Session Configuration Settings」が含まれたエントリを検索します。IPv4 と IPv6 のスプリット DNS 用に別々のログ エントリがあります。

- スプリット DNS 除外の場合
  - IPv4 split DNS: 5 excluded domains
  - IPv6 split DNS: 5 excluded domains
- スプリット DNS 包含の場合
  - IPv4 split DNS: 5 included domains
  - IPv6 split DNS: 5 included domains

VPN 認証の管理

重要なセキュリティ上の考慮事項

セキュアゲートウェイ上での自己署名証明書の使用はお勧めしません。

- 理由は、ユーザーが誤って不正なサーバー上の証明書を信頼するようにブラウザを設定する可能性があるため、また、
- ユーザがセキュアゲートウェイに接続する際に、セキュリティ警告に応答する手間がかかるためです。

Cisco Secure Client クライアントに対する厳格な証明書トラストを有効にすることを強くお勧めします。[厳格な証明書トラスト（Strict Certificate Trust）] を設定するには、ローカルポリシー設定の「ローカルポリシーパラメータと値」セクションを参照してください。

サポートされるセキュリティタイプ

Cisco Secure Client は、サーバー証明書の検証とクライアント証明書の認証の両方で RSA 証明書と ECDSA 証明書をサポートしています。

- **RSA 証明書**

  Cisco Secure Client は、次のプロパティを持つ RSA 証明書をサポートします。

  - 2048、4096、または 8192 ビットのキー長
  - ハッシュアルゴリズム MD5 *、SHA1、SHA256、SHA384、または SHA512

    * Cisco Secure Client が FIPS モードで動作している場合、MD5 ハッシュを使用する RSA 証明書はサポートされません。

- **ECDSA 証明書**

  Cisco Secure Client は、次のプロパティを持つ ECDSA 証明書をサポートします。

  - 256、384、または 521 ビットのキー長。これらは、それぞれ NIST P-256、P-384、および P-521 楕円曲線に対応します。

- **EdDSA 証明書**

  Cisco Secure Client は、Windows および macOS オペレーティングシステムに基づいて、デジタル証明書により、信頼を確立して署名操作を実行します。これらのオペレーティングシステムでは EdDSA 証明書がまだサポートされていないため、Cisco Secure Client でもサポートできません。

サーバ証明書処理の設定

サーバ証明書の確認

- 証明書は上記の最小キーサイズを満たし、サポートタイプ（RSA または ECDSA）のいずれかである必要があります。
- （Windows のみ）SSL 接続と IPsec VPN 接続の両方で、証明書失効リスト（CRL）チェックを実行するオプションがあります。プロファイルエディタで有効にすると、Cisco Secure Client はチェーン内のすべての証明書を対象とした最新の CRL を取得します。AnyConnect は次に、当該証明書がこれらの信頼できなくなった失効証明書に含まれているかどうかを確認します。認証局によって失効された証明書であることが判明すると、AnyConnect は接続しません。詳細は、ローカルポリシー設定を参照してください。
- サーバー証明書が設定された Cisco Secure Firewall ASA にユーザーが接続する場合、信頼チェーン（ルートや中間など）に問題があっても、その証明書を信頼し、インポートするためのチェックボックスは表示されます。証明書にそれ以外の問題がある場合、そのチェックボックスは表示されません。
- FQDN によって実行される SSL 接続では、FQDN を使用した初期検証に失敗した場合、名前検証のために FQDN が IP アドレスに解決されず、セカンダリ サーバの証明書検証が行われません。
- 検証が実行される日時（オペレーティングシステムによって報告される日時）は、証明書の有効開始日より後、かつ有効終了日より前でなければなりません。
- 推奨されませんが、サーバ証明書は、キー使用法（KU）または拡張キー使用法（EKU）を受け入れる必要はありません。ただし、フィールドが存在する場合（最も一般的）、次の条件が適用されます。

  SSL と IPsec（RSA 証明書と ECDSA 証明書の両方）の場合、KU フィールドには DigitalSignature を含める必要があります。RSA 証明書の場合、KU には KeyEncipherment または KeyAgreement も含まれている必要があります。

  IPsec VPN の場合、すべての EKU フィールドに ServerAuth または IkeIntermediate が含まれている必要があります。
- IPsec および SSL 接続は、サーバ証明書で名前の検証を実行します。IPsec および SSL 名前検証のために次のルールが適用されます。
  - Subject Alternative Name 拡張子が関連する属性に含まれる場合、名前検証は Subject Alternative Name に対してのみ実行されます。関連する属性には、すべての証明書の DNS Name 属性や、接続が IP アドレスに対して実行される場合は、IP アドレスの属性などが含まれます。
  - Subject Alternative Name 拡張子がない場合、または、あっても関連する属性が含まれていない場合、名前検証は、証明書の Subject で見つかった Common Name 属性に対して実行されます。

- 証明書が名前検証の目的でワイルドカードを使用する場合、そのワイルドカードは最初（左端）のサブドメインのみに含まれなければならず、他に追加する場合はサブドメインの最後（右端）の文字でなければなりません。このルールに準拠していないワイルドカードのエントリは、名前検証の目的では無視されます。

- macOS の場合、期限切れの証明書は、キーチェーンアクセスで [有効期限の切れた証明書を表示（Show Expired Certificates）] が設定されている場合にのみ表示されます。期限切れの証明書は、ユーザーの混乱を招く可能性があるため、デフォルトでは表示されません。

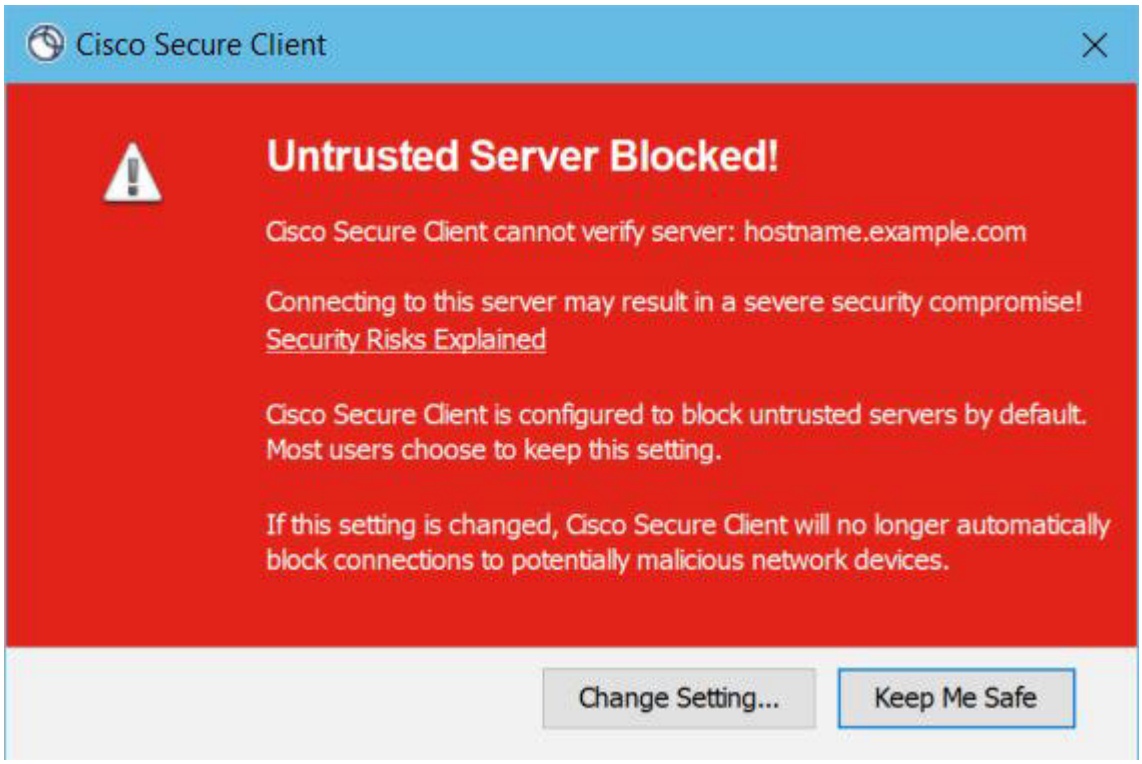
無効なサーバ証明書の処理

非信頼ネットワーク上のモバイル ユーザを狙った攻撃の増加に対応して、シスコは重大なセキュリティ違反を防ぐため、クライアントのセキュリティ保護を強化しました。デフォルトのクライアントの動作は、中間者攻撃に対する追加の防御レイヤを提供するように変更されました。

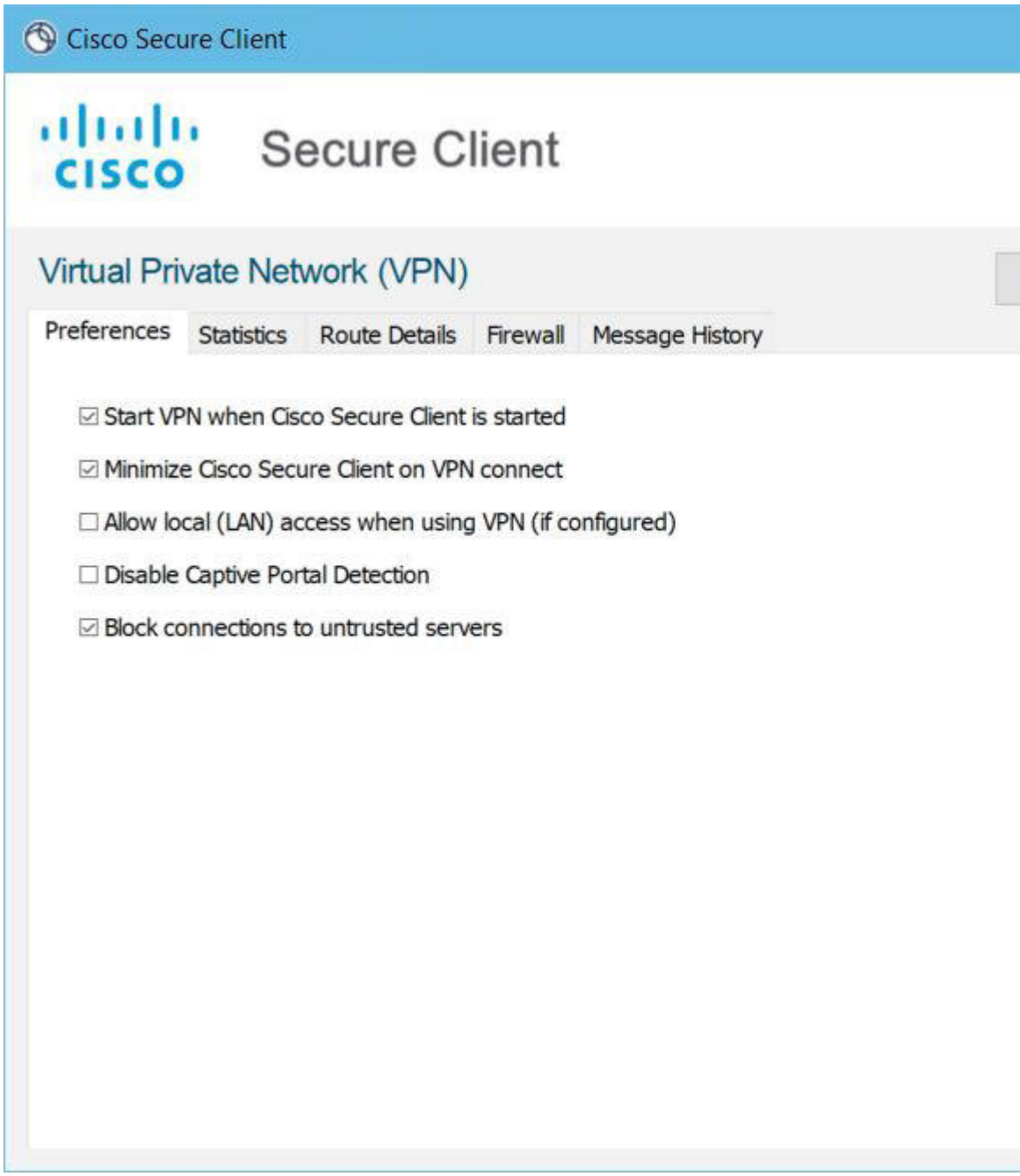
ユーザ対話

ユーザがセキュア ゲートウェイに接続しようとしたときに証明書エラーがある場合（期限切れ、無効な日付、キーの誤用、またはCNの不一致による）、[設定の変更（Change Settings）] および [安全を確保（Keep Me Safe）] ボタンを含む赤色のダイアログがユーザに表示されます。

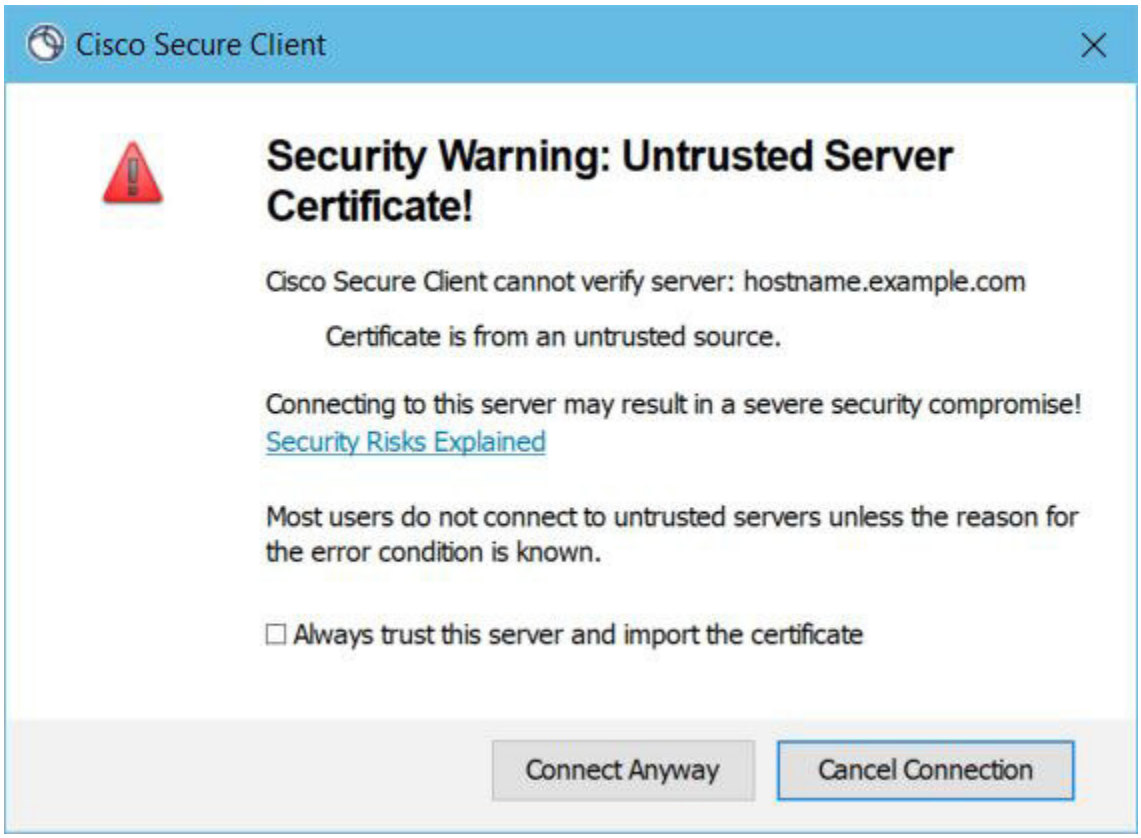
（注） Linux のダイアログは、このマニュアルに示すものと異なる場合があります。



- [安全を確保（Keep Me Safe）] をクリックすると、接続が解除されます。
- [設定の変更（Change Settings）] をクリックすると、Cisco Secure Client の [詳細（Advanced）] > [VPN] > [設定（Preferences）] ダイアログが開きます。ここで、ユーザーは非信頼サーバーへの接続を有効にできます。現在の接続の試行がキャンセルされます。



ユーザーが、[信頼されていないサーバーへの接続をブロック（Block connections to untrusted servers）] をオフにして、証明書に関する問題が CA が信頼できないことのみである場合、次回ユーザーがこのセキュアゲートウェイに接続しようとするときは、ユーザーに証明書ブロック エラーのダイアログは表示されません。



ユーザが [常にこの VPN サーバを信頼し、証明書をインポートする（Always trust this VPN server and import the certificate）] をオンにしている場合、このセキュア ゲートウェイへの今後の接続時に、ユーザの続行を確認するプロンプトは表示されません。

（注） ユーザーが、Cisco Secure Client の [詳細（Advanced）] > [VPN] > [設定（Preferences）] で [信頼されていないサーバーへの接続をブロック（Block connections to untrusted servers）] をオンにしている場合、または、ユーザーの設定が注意事項と制約事項の項で説明されているモードのリストのいずれかの条件と一致する場合、Cisco Secure Client は、プロファイルエディタの [厳格な証明書トラスト（Strict Certificate Trust）] オプションが有効になっているかどうかに関係なく、無効なサーバー証明書と信頼できないサーバーへの接続を拒否します。

改善されたセキュリティ動作

クライアントが無効なサーバ証明書を受け入れると、その証明書はクライアントの証明書ストアに保存されます。以前は、証明書のサムプリントだけが保存されました。ユーザが無効なサーバ証明書を常に信頼してインポートすることを選択した場合のみ、無効な証明書が保存されることに注意してください。

エンドユーザの安全性が自動的に損なわれる管理上の優先操作はありません。先行するセキュリティ上の判断をエンド ユーザから完全に排除するには、ユーザのローカル ポリシー ファイルで [厳格な証明書トラスト（Strict Certificate Trust）] を有効にします。[厳格な証明書トラス

ト（Strict Certificate Trust）] が有効である場合、ユーザにはエラー メッセージが表示され、接続が失敗します。ユーザ プロンプトは表示されません。

ローカルポリシーファイルでの厳格な証明書トラストの有効化については、ローカルポリシー設定 を参照してください。

注意事項と制約事項

無効なサーバ証明書は、次の場合に拒否されます。

- Cisco Secure Client プロファイルで [常時接続（Always On）] が有効になっており、適用されたグループポリシーまたは DAP によりオフにされていない。
- クライアントに、厳格な証明書トラストが有効なローカル ポリシーがある。
- Cisco Secure Client で Start Before Login が設定されている。
- マシン証明書ストアからのクライアント証明書が認証に使用されている。

Certificate-Only 認証の設定

ユーザー名とパスワードを使用して Cisco Secure Firewall ASA でユーザーを認証するか、デジタル証明書で認証するか（または、その両方を使用するか）を指定する必要があります。証明書のみの認証を設定すると、ユーザはデジタル証明書で接続でき、ユーザ ID とパスワードを入力する必要がなくなります。

複数のグループを使用する環境で証明書のみの認証をサポートする場合は、複数のグループ URL をプロビジョニングします。各グループ URL には、さまざまなクライアント プロファイルとともに、グループ固有の証明書マップを作成するためのカスタマイズ済みデータの一部が含まれます。たとえば、Cisco Secure Firewall ASA に開発部の Department_OU 値をプロビジョニングし、このプロセスによる証明書が Cisco Secure Firewall ASA に提供されたときに、このグループにユーザーを配置するようにできます。

（注） セキュア ゲートウェイに対してクライアントを認証するために使用される証明書は有効であり、（CA によって署名された）信頼できるものである必要があります。自己署名されたクライアント証明書は受け入れられません。

ステップ 1 **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect接続プロファイル（AnyConnect Connection Profiles）]** を選択します。接続プロファイルを選択し、[編集（Edit）] をクリックします。[AnyConnect 接続プロファイルの編集（Edit AnyConnect Connection Profile）] ウィンドウが開きます。

ステップ 2 選択されていない場合は、ウィンドウの左ペインにあるナビゲーション ツリーの [基本（Basic）] ノードをクリックします。ウィンドウの右ペインにある [認証（Authentication）] 領域で、[証明書（Certificate）] 方式を有効にします。

ステップ 3 [OK] をクリックし、変更を適用します。

証明書登録の設定

Cisco Secure Clientは、Simple Certificate Enrollment Protocol（SCEP）を使用して、クライアント認証の一部として証明書をプロビジョニングおよび更新します。SCEP を使用した証明書の登録は、Cisco Secure Firewall ASA への Cisco Secure Client IPsec および SSL VPN 接続で次のようにサポートされます。

- SCEP プロキシ：Cisco Secure Firewall ASA はクライアントと認証局（CA）間の SCEP 要求と応答のプロキシとして機能します。
  - クライアントが CA に直接アクセスしないため、CA は、Cisco Secure Client ではなく Cisco Secure Firewall ASA にアクセスできる必要があります。
  - 登録は、クライアントにより常に自動的に開始されます。ユーザーの介入は必要ありません。

関連トピック

Cisco Secure Client プロファイルエディタの [証明書の登録（Certificate Enrollment）]

SCEP プロキシの登録と動作

次の手順では、Cisco Secure Client および Cisco Secure Firewall ASA が SCEP プロキシ用に設定されている場合に、証明書が取得され、証明書ベースの接続が確立された方法について説明します。

1. ユーザーは、証明書と AAA 認証の両方用に設定された接続プロファイルを使用して、Cisco Secure Firewall ASA ヘッドエンドに接続します。Cisco Secure Firewall ASA は、クライアントからの認証用に証明書と AAA クレデンシャルを要求します。
2. ユーザーが AAA クレデンシャルを入力しますが、有効な証明書は使用可能ではありません。この状況は、入力された AAA クレデンシャルを使用してトンネルが確立された後で、クライアントが自動 SCEP 登録要求を送信するトリガーになります。
3. Cisco Secure Firewall ASA が CA に対して登録要求を転送し、CA の応答をクライアントに返します。
4. SCEP 登録が成功すると、クライアントにユーザーに対する（設定可能な）メッセージが表示され、現行のセッションが接続解除されます。ユーザーは、証明書認証を使用して、Cisco Secure Firewall ASA トンネルグループに接続できます。

   SCEP 登録に失敗した場合、クライアントにユーザーに対する（設定可能な）メッセージが表示され、現行のセッションが接続解除されます。ユーザーは自分の管理者に連絡する必要があります。

他の SCEP プロキシの動作上の考慮事項：

- そうするように設定されている場合、ユーザーが介入することなく、期限切れになる前に証明書がクライアントにより自動的に更新されます。
- SCEP プロキシ登録は、SSL と IPSec トンネルの両方の証明書認証に SSL を使用します。

認証局の要件

- IOS CS、Windows Server 2003 CA、および Windows Server 2008 CA を含め、すべての SCEP 準拠 CA がサポートされています。
- CA は自動付与モードである必要があります。証明書のポーリングはサポートされません。
- 一部の CA について、セキュリティを強化するために、電子メールで登録パスワードをユーザに送信するように設定できます。CA パスワードは、ユーザを識別するための認証局に送信されるチャレンジ パスワードまたはトークンです。このパスワードはその後、Cisco Secure Client プロファイルで設定できます。これは、CA が証明書を付与する前に確認する、SCEP 要求の一部になります。

証明書登録のガイドライン

- Cisco Secure Firewall ASA ロードバランシングは、SCEP 登録でサポートされます。
- Cisco Secure Firewall ASA は、クライアントから受信した要求を記録しますが、登録が失敗した理由は表示しません。接続の問題は、CA またはクライアントでデバッグされる必要があります。
- 証明書のみの認証および Cisco Secure Firewall ASA での証明書マッピング：

  複数のグループを使用する環境で証明書のみの認証をサポートする場合は、複数のグループ URL をプロビジョニングします。各グループ URL には、さまざまなクライアント プロファイルとともに、グループ固有の証明書マップを作成するためのカスタマイズ済みデータの一部が含まれます。たとえば、Cisco Secure Firewall ASA に開発部の Department_OU 値をプロビジョニングし、このプロセスによる証明書が Cisco Secure Firewall ASA に提供されたときに、このトンネルグループにユーザーを配置するようにできます。
- ポリシーを適用するための登録接続の特定：

  Cisco Secure Firewall ASA で、登録接続を捕捉し、選択された DAP レコードの適切なポリシーを適用するために、aaa.cisco.sceprequired 属性が使用されます。
- Windows 証明書の警告：

  Windows クライアントが最初に認証局から証明書を取得しようとした際に、警告される可能性があります。プロンプトが表示されたら、[はい（Yes）] をクリックしてください。これにより、ルート証明書をインポートできます。クライアント証明書との接続に影響しません。

SCEP プロキシ証明書登録の設定

SCEP プロキシ登録用 VPN クライアント プロファイルの設定

ステップ 1 VPN プロファイル エディタを開き、ナビゲーション ペインから [証明書の登録（Certificate Enrollment）] を選択します。

ステップ 2 [証明書の登録（Certificate Enrollment）] を選択します。

ステップ 3 登録証明書で、要求する [証明書の内容（Certificate Contents）] を設定します。証明書フィールドの定義については、「AnyConnect プロファイル エディタの [証明書の登録（Certificate Enrollment）]」を参照してください。

（注）
- %machineid% を使用した場合は、デスクトップクライアントに Secure Firewall ポスチャ がロードされます。
- モバイル クライアントの場合、証明書フィールドのうち少なくとも 1 つを指定する必要があります。

SCEP プロキシ登録をサポートするための Cisco Secure Firewall ASA の設定

SCEP プロキシのため、1 つの Cisco Secure Firewall ASA 接続プロファイルは、証明書登録および認証された VPN 接続をサポートします。

ステップ 1 グループ ポリシー（例：cert_group）を作成します。次のフィールドを設定します。

- [一般（General）] で、[SCEP フォワーディング URL（SCEP Forwarding URL）] に CA への URL を入力します。
- [詳細（Advanced）] > [Cisco Secure Client クライアント（AnyConnect Client）] ペインで、[ダウンロードするクライアントプロファイルの継承（Inherit for Client Profiles to Download）] をオフにし、SCEP プロキシ用に設定されたクライアントプロファイルを指定します。たとえば、ac_vpn_scep_proxy クライアント プロファイルを指定します。

ステップ 2 証明書の登録および接続を認証した証明書（例：cert_tunnel）用の接続プロファイルを作成します。

- [認証（Authentication）]：Both（AAA および Certificate）。
- デフォルトのグループ ポリシー：cert_group。
- [詳細（Advanced）]>[一般（General）] で、[この接続プロファイルへの SCEP 登録を有効にする（Enable SCEP Enrollment for this Connction Profile）] をオンにします。
- [詳細（Advanced）] > [グループエイリアス/グループ URL（GroupAlias/Group URL）] で、この接続プロファイルのグループ（cert_group）が含まれるグループ URL を作成します。

SCEP 用の Windows 2012 Server の認証局の設定

認証局ソフトウェアが Windows 2012 サーバーで実行されている場合、Cisco Secure Client で SCEP がサポートされるように次のいずれかの設定変更を行う必要があります。

認証局での SCEP パスワードの無効化

次の手順は、クライアントが SCEP 登録の前にアウトオブバンドパスワードを提供せずに済むように、SCEP チャレンジ パスワードを無効にする方法について説明します。

ステップ 1 認証局サーバで、レジストリ エディタを起動します。これを行うには、**[スタート（Start）]>[ファイル名を指定して実行（Run）]** を選択し、**regedit** と入力して [OK] をクリックします。

ステップ 2 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword に移動します。

EnforcePassword キーが存在しない場合は、新しいキーとして作成します。

ステップ 3 EnforcePassword を編集し、「0」に設定します。存在しない場合は、REG-DWORD として作成します。

ステップ 4 regedit を終了し、認証局サーバをリブートします。

認証局での SCEP テンプレートの設定

以下の手順では、証明書のテンプレートを作成する方法、およびこれをデフォルト SCEP テンプレートとして割り当てる方法について説明します。

ステップ 1 サーバ マネージャを起動します。これは、[スタート（Start）] > [管理ツール（Admin Tools）] > [サーバ マネージャー（Server Manager）] を選択することで実行できます。

ステップ 2 [役割（Roles）] > [証明書サービス（Certificate Services）]（または [Active Directory 証明書サービス（AD Certificate Services）]）を展開します。

ステップ 3 CA の名前 > [証明書テンプレート（Certificate Templates）] に移動します。

ステップ 4 [証明書テンプレート（Certificate Templates）] > [管理（Manage）] を右クリックします。

ステップ 5 [証明書テンプレート コンソール（Cert Templates Console）] から、ユーザ テンプレートを右クリックして [複製（Duplicate）] を選択します。

ステップ 6 新しいテンプレートの [Windows Server 2012] バージョンを選択して、[OK] をクリックします。

ステップ 7 テンプレートの表示名を、NDES IPsec SSL など、具体的な説明に変更します。

ステップ 8 サイトの有効期間を調整します。ほとんどのサイトでは、証明書の期限切れを避けるために 3 年以上を選択します。

ステップ 9 [暗号化（Cryptography）] タブで、展開の最小キー サイズを設定します。

ステップ 10 [サブジェクト名（Subject Name）] タブで、[要求に含まれる（Supply in Request）] を選択します。

ステップ 11 [拡張機能（Extensions）] タブで、[アプリケーションのポリシー（Application Policies）] に少なくとも次が含まれるように設定します。

- クライアント認証

- IP セキュリティ末端システム
- IP セキュリティ IKE 中間
- IP セキュリティ トンネル終端
- IP セキュリティ ユーザ

これらの値は、SSL または IPSec に有効です。

ステップ 12 [適用（Apply）] をクリックして、次に [OK] をクリックして新しいテンプレートを保存します。

ステップ 13 サーバ マネージャから [証明書サービス（Certificate Services）] に移動して CA の名前を選択し、[証明書テンプレート（Certificate Templates）] を右クリックします。[新規（New ）] > [発行する証明書テンプレート（Certificate Template to Issue）] を選択し、作成した新しいテンプレートを選択します（この例では NDES-IPSec-SSL）。次に、[OK] をクリックします。

ステップ 14 レジストリを編集します。これは、[スタート（Start）] > [ファイル名を指定して実行（Run）] で regedit と入力し、[OK] をクリックすることで実行できます。

ステップ 15 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP に移動します。

ステップ 16 次の 3 つのキーの値を、NDES-IPSec-SSL に設定します。

- EncryptionTemplate
- GeneralPurposeTemplate
- SignatureTemplate

ステップ 17 [保存（Save）] をクリックして、認証局サーバをリブートします。

証明書失効通知の設定

認証証明書が間もなく期限切れになることをユーザーに警告するよう Cisco Secure Client を設定します。[証明書の有効期限のしきい値（Certificate Expiration Threshold）] 設定では、証明書の有効期限までの日数を指定します。Cisco Secure Client は、しきい値を使用して、証明書の有効期限が切れることをユーザーに警告するタイミングを決定します。証明書が実際に期限切れになるか、新しい証明書が取得されるまで、Cisco Secure Client は接続するたびにユーザーに警告します。

（注） RADIUS 登録では、[証明書失効しきい値（Certificate Expiration Threshold）] 機能は使用できません。

ステップ 1 Cisco Secure Client プロファイルエディタの VPN を開き、ナビゲーションウィンドウから [証明書の登録（Certificate Enrollment）] を選択します。

ステップ 2 [証明書の登録（Certificate Enrollment）] を選択します。

ステップ 3 [証明書失効しきい値（Certificate Expiration Threshold）] を指定します。

このしきい値は、証明書の有効期限までの日数です。Cisco Secure Client が証明書の失効が近づいていることをユーザーに対して何日前に警告するかを決定します。

デフォルトは 0（警告は表示しない）です。範囲は 0 ～ 180 日です。

ステップ 4 [OK] をクリックします。

証明書選択の設定

次の手順では、クライアントシステムで証明書を検索する方法および証明書を選択する方法を設定する、Cisco Secure Client プロファイル内のすべての場所を示します。いずれの手順も必須ではなく、条件を指定しなかった場合、Cisco Secure Client はデフォルトのキー照合を使用します。

Windows では、Cisco Secure Client はブラウザの証明書ストアを読み取ります。Linux の場合、プライバシー強化メール（PEM）形式のファイル ストアを作成する必要があります。macOS の場合、プライバシー強化メール（PEM）形式のファイル ストアまたはキーチェーンを使用できます。

ステップ 1 Windows および macOS の場合：使用する証明書ストアの設定 （63 ページ）

VPN クライアント プロファイルに Cisco Secure Client で使用される証明書ストアを指定します。

ステップ 2 Windows のみ：Windows ユーザに認証証明書の選択を求めるプロンプトの表示 （66 ページ）

ユーザーに対して有効な証明書のリストを表示し、セッションの認証に使用する証明書をユーザーが選択できるように Cisco Secure Client を設定します。

ステップ 3 macOS および Linux 環境の場合： macOS および Linux での PEM 証明書ストアの作成 （67 ページ）

ステップ 4 macOS および Linux 環境の場合：VPN ローカル ポリシー プロファイルで除外する証明書ストアを選択します。

ステップ 5 証明書照合の設定 （67 ページ）

ストアの証明書を検索する場合に、Cisco Secure Client が照合を試みるキーを設定します。キー（拡張キー）を指定し、カスタム拡張キーを追加できます。また、Cisco Secure Client が照合する識別名に演算子の値のパターンを指定できます。

使用する証明書ストアの設定

Windows、macOS、および Linux では、Cisco Secure Client が VPN クライアントプロファイルで使用するための別の証明書ストアが提供されます。1 つまたは複数の証明書認証の組み合わせが可能で、複数の証明書認証の選択肢のうち特定の VPN 接続において許容されるものをクライアントに指定するようにセキュア ゲートウェイを設定できます。たとえば、macOS では、

ローカルポリシーファイルで ExcludePemFileCertStore を *true* に設定（Cisco Secure Client がネイティブキーチェーン証明書ストアのみを使用するよう強制）し、プロファイルベースの証明書ストアを [ログイン（Login）] に設定（Cisco Secure Client が、ユーザー PEM ファイルストアに加え、ユーザーログインキーチェーンやダイナミック スマートカード キーチェーンなどの証明書ストアのみを使用するよう強制）すると、その組み合わせによるフィルタリングにより、Cisco Secure Client は、厳格にユーザー ログイン キーチェーン証明書ストアを使用するようになります。

Windows では、コンピュータ上で管理者権限を持つユーザは、両方の証明書ストアにアクセスできます。管理者権限を持たないユーザがアクセスできるのは、ユーザ証明書ストアのみです。通常、Windows ユーザには管理者権限がありません。[Windows証明書ストアの上書き（Windows Certificate Store Override）] を選択すると、ユーザーに管理者権限がない場合でも、Cisco Secure Client はマシンストアにアクセスできます。

（注） マシン ストアのアクセス制御は、Windows のバージョンとセキュリティ設定によって異なる場合があります。このため、ユーザは管理者権限を持つ場合にも、マシン ストアの証明書を使用できない可能性があります。この場合、[証明書ストアの上書き（Certificate Store Override）] を選択してマシン ストアへのアクセスを許可します。

次の表で、検索対象の [証明書ストア（Certificate Store）] および [Windows証明書ストアの上書き（Windows Certificate Store Override）] のオン/オフに基づいて Cisco Secure Client がクライアントで証明書を検索する方法について説明します。

証明書ストアの設定	証明書ストアの上書きの設定	**Cisco Secure Client 検索戦略**
[すべて（All）]（Windows 用）	false	Cisco Secure Client は、すべての証明書ストアを検索します。ユーザーに管理者権限がない場合、Cisco Secure Client は、マシンストアにアクセスできません。 この設定は、デフォルトです。この設定は、ほとんどの状況に適しています。変更が必要となる特別な理由またはシナリオ要件がある場合を除いて、この設定は変更しないでください。
[すべて（All）]（Windows 用）	true	Cisco Secure Client は、すべての証明書ストアを検索します。ユーザーに管理者権限がない場合、Cisco Secure Client は、マシンストアにアクセスできます。
[マシン（Machine）]（Windows 用）	true	Cisco Secure Client は、マシン証明書ストアのみを検索します。ユーザーに管理者権限がない場合、Cisco Secure Client は、マシンストアにアクセスできます。
[ユーザー（User）]（Windows 用）	適用なし	Cisco Secure Client は、ユーザー証明書ストア内のみ検索します。管理者権限のないユーザがこの証明書ストアにアクセスできるため、証明書ストアの上書きは適用されません。

証明書ストアの設定	証明書ストアの上書きの設定	Cisco Secure Client 検索戦略
[すべて（All）]（macOS 用）	適用なし	Cisco Secure Client は、利用可能なすべての macOS キーチェーンおよびファイルストアからの証明書を使用します。
[システム（System）]（macOS 用）	適用なし	Cisco Secure Client は、macOS システムキーチェーンおよびシステムファイル/PEM ストアからの証明書のみを使用します。
[ログイン（Log in）]（macOS 用）	適用なし	Cisco Secure Client は、ユーザーファイル/PEM ストアに加え、macOS ログインキーチェーンおよびダイナミック スマートカード キーチェーンからの証明書のみを使用します。
[すべて（All）]（Linux 用）	適用なし	Cisco Secure Client は、システムとユーザーの両方の PEM ファイルストア、およびユーザー Firefox NSS ストアのクライアント証明書を使用します。
[マシン（Machine）]（Linux 用）	適用なし	Cisco Secure Client は、システム PEM ファイルストアのクライアント証明書のみを使用します。
[ユーザ（User）]（Linux 用）	適用なし	Cisco Secure Client は、ユーザー PEM ファイルストア、およびユーザー Firefox NSS ストアのクライアント証明書のみを使用します。

複数証明書認証の使用

始める前に

- デスクトッププラットフォーム（Windows、macOS、Linux）でのみサポートされます。
- VPN プロファイルで AutomaticCertSelection を有効にしている必要があります。
- VPNプロファイルで設定した証明書照合設定によって、複数証明書認証で使用できる証明書が制限されます。

（注） SCEP はサポートされていません。

ステップ 1 [証明書ストア（Certificate Store）] を設定します。

- Windows プラットフォームで、1 マシンおよび 1 ユーザ証明書の場合は、VPN プロファイルで [すべて（All）] に設定し、ステップ 2 の説明に従って CertficateStoreOverride を有効にします。

- Windows プラットフォームで、2 ユーザ証明書の場合は、VPN プロファイルで [すべて（All）] または [ユーザ/ログイン（User/Login）] に設定しますが、ステップ 2 の説明に従って CertificateStoreOverride はそのままにします。

ステップ 2 ユーザーに管理者権限がない場合に Cisco Secure Client にマシン証明書ストアの検索を許可するには、 を選択します。

基本的な証明書認証の使用

ステップ 1 [証明書ストア（Certificate Store）] を設定します。

- [すべて（All）] :（デフォルト）すべての証明書ストアを使用して証明書を検索するよう Cisco Secure Client に指示します。
- [マシン/システム（Machine/System）] : 証明書ルックアップをローカルマシン/システムレベルの証明書ストアに制限するように Cisco Secure Client クライアントに指示します。
- [ユーザー/ログイン（User/Login）] : 証明書ルックアップをローカルユーザー証明書ストアに制限するように Cisco Secure Client に指示します。

ステップ 2 ユーザーに管理者権限がない場合に Cisco Secure Client にマシン証明書ストアの検索を許可するには、 を選択します。

Windows ユーザに認証証明書の選択を求めるプロンプトの表示

ユーザーに対して有効な証明書のリストを表示し、セッションの認証に使用する証明書をユーザーが選択できるように Cisco Secure Client を設定できます。期限切れの証明書は必ずしも無効として見なされるわけではありません。たとえば SCEP を使用している場合、サーバが新しい証明書をクライアントに発行することがあります。期限切れの証明書を削除すると、クライアントがまったく接続できなくなることがあります。この場合、手動による介入とアウトオブバンド証明書配布が必要になります。Cisco Secure Client では、設定されている証明書一致ルールに基づき、セキュリティ関連プロパティ（キーの使用状況、キーのタイプと強度など）に基づいて、クライアント証明書が制限されるだけです。この設定は Windows でのみ使用できます。デフォルトでは、ユーザによる証明書の選択は無効です。

ステップ 1 Cisco Secure Client プロファイルエディタを開き、ナビゲーションウィンドウから VPN [プリファレンス（Part 2）（Preferences (Part 2)）] を選択します。

ステップ 2 証明書の選択を有効にするには、[証明書選択を無効にする（Disable Certificate Selection）] チェックボックスをオフにします。

ステップ 3 **[詳細（Advanced）]** > **[VPN]** > **[プリファレンス（Preferences）]** ペインでユーザが自動証明書の選択のオン/オフを切り替えられるようにする場合を除き、[ユーザ制御可（User Controllable）] チェックボックスをオフにします。

macOS および Linux での PEM 証明書ストアの作成

Cisco Secure Client は、プライバシー強化メール（PEM）形式のファイルストアからの証明書の取得をサポートします。Cisco Secure Client はリモートコンピューターのファイルシステムから PEM 形式の証明書ファイルを読み取り、検証して署名します。

始める前に

あらゆる条件下でクライアントが適切な証明書を取得するためには、ファイルが次の要件を満たしている必要があります。

- すべての証明書ファイルは、拡張子が .pem または .crt で終わっていること。
- すべての秘密キー ファイルは、拡張子 .key で終わっていること。
- クライアント証明書と、それに対応する秘密キーのファイル名が同じであること 例：client.pem と client.key。

ヒント PEM ファイルのコピーを保持する代わりに、PEM ファイルへのソフト リンクを使用できます。

PEM ファイル証明書ストアを作成する場合は、次に示すパスとフォルダを作成します。これらのフォルダに、適切な証明書を配置してください。

PEM ファイル証明書ストアのフォルダ	保存される証明書のタイプ
~/.cisco/certificates/ca （注） .cisco/ はホームディレクトリにあります。	信頼できる CA とルート証明書
~/.cisco/certificates/client	クライアント証明書
~/.cisco/certificates/client/private	秘密キー

マシン証明書は、ルート ディレクトリ以外は PEM ファイル証明書と同じです。マシン証明書の場合は、~/.cisco を /opt/.cisco に置き換えてください。それ以外の場合は、リストされているパス、フォルダ、および証明書の種類が適用されます。また、Cisco Secure Client はシステム CA 証明書の場所（/etc/ssl/certs）を使用してサーバー証明書を検証します。

証明書照合の設定

Cisco Secure Client では、特定のキーのセットに一致するこれらの証明書に証明書の検索を限定できます。証明書照合は、**[証明書照合（Certificate Matching）]** ペインの Cisco Secure Client VPN プロファイルで設定できるグローバル基準です。基準は次のとおりです。

- [キーの使用状況（Key Usage）]

- [拡張キーの使用状況（Extended Key Usage）]
- [識別名（Distinguished Name）]

関連トピック

Cisco Secure Client プロファイルエディタの証明書照合

キーの使用状況の設定

[キーの使用状況（Key Usage）] キーを選択すると、Cisco Secure Client で使用できる証明書が、選択したキーの少なくとも 1 つを持つ証明書に制限されます。サポート対象のセットは、VPN クライアント プロファイルの [キーの使用状況（Key Usage）] リストに一覧表示されており、次が含まれています。

- DECIPHER_ONLY
- ENCIPHER_ONLY
- CRL_SIGN
- KEY_CERT_SIGN
- KEY_AGREEMENT
- DATA_ENCIPHERMENT
- KEY_ENCIPHERMENT
- NON_REPUDIATION
- DIGITAL_SIGNATURE

1 つ以上の基準が指定されている場合、証明書が一致すると見なされるには、少なくとも 1 つの基準が一致している必要があります。

拡張キーの使用状況の設定

[拡張キーの使用状況（Extended Key Usage）] キーを選択すると、Cisco Secure Client で使用できる証明書がこれらのキーを持つ証明書に限定されます。次の表は、既知の制約のセットと、それに対応するオブジェクト ID（OID）をリストにまとめたものです。

制約	OID
ServerAuth	1.3.6.1.5.5.7.3.1
ClientAuth	1.3.6.1.5.5.7.3.2
CodeSign	1.3.6.1.5.5.7.3.3
EmailProtect	1.3.6.1.5.5.7.3.4
IPSecEndSystem	1.3.6.1.5.5.7.3.5
IPSecTunnel	1.3.6.1.5.5.7.3.6
IPSecUser	1.3.6.1.5.5.7.3.7

制約	OID
TimeStamp	1.3.6.1.5.5.7.3.8
OCSPSign	1.3.6.1.5.5.7.3.9
DVCS	1.3.6.1.5.5.7.3.10
IKE Intermediate	1.3.6.1.5.5.8.2.2

カスタム拡張照合キーの設定

その他の OID（本書の例で使用している 1.3.6.1.5.5.7.3.11 など）はすべて、「カスタム」と見なされます。管理者は、既知のセットの中に必要な OID がない場合、独自の OID を追加できます。

証明書識別名の設定

[識別名（Distinguished Name）] の表には、クライアントが使用できる証明書を指定の条件に一致する証明書に限定する証明書 ID、および一致条件が含まれています。条件をリストに追加したり、追加した条件の内容と照合するための値またはワイルドカードを設定したりするには、[追加（Add）] ボタンをクリックします。

ID	説明
CN	SubjectCommonName
SN	SubjectSurName
GN	SubjectGivenName
N	SubjectUnstructName
I	SubjectInitials
GENQ	SubjectGenQualifier
DNQ	SubjectDnQualifier
C	SubjectCountry
L	SubjectCity
SP	SubjectState
ST	SubjectState
O	SubjectCompany
OU	SubjectDept
T	SubjectTitle
EA	SubjectEmailAddr

ID	説明
DC	DomainComponent
ISSUER-CN	IssuerCommonName
ISSUER-SN	IssuerSurName
ISSUER-GN	IssuerGivenName
ISSUER-N	IssuerUnstructName
ISSUER-I	IssuerInitials
ISSUER-GENQ	IssuerGenQualifier
ISSUER-DNQ	IssuerDnQualifier
ISSUER-C	IssuerCountry
ISSUER-L	IssuerCity
ISSUER-SP	IssuerState
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
ISSUER-EA	IssuerEmailAddr
ISSUER-DC	IssuerDomainComponent

[識別名（Distinguished Name）] には、0 個以上の一致基準を含めることができます。証明書が一致すると見なされるには、指定されているすべての基準に一致している必要があります。[識別名（Distinguished Name）] の一致では、証明書に指定の文字列が含まれている必要があるかどうか、および文字列にワイルドカードを許可するかどうかを指定します。

SAML を使用した VPN 認証

最初のセッション認証に Cisco Secure Firewall ASA リリース 9.7.1 以降と統合された SAML 2.0 を使用できます。組み込みブラウザとの SAML 統合が拡張され、これが以前のリリースからのネイティブ（外部）ブラウザ統合に置き換わりました。SAML 認証用に設定されたトンネルグループに接続するときに、Cisco Secure Client は組み込みブラウザウィンドウを開いて認証プロセスを完了します。SAML 試行のたびに新しいブラウザセッションが使用され、ブラウザセッションは Cisco Secure Client に固有のものとなります（セッション状態は、他のどのブラウザとも共有されません）。各 SAML 認証試行はセッション状態なしで始まりますが、試行間で永続クッキーが保持されます。

Cisco Secure Firewall ASA リリース 9.17.1（以降）/ASDM リリース 7.17.1（以降）では、Cisco Secure Client を使用した VPN SAML 外部ブラウザのサポートが追加されました。Cisco Secure Client 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、Web 認証の実行時に Cisco Secure Client が組み込みブラウザではなくローカルブラウザを使用することを選択できます。この機能により、Cisco Secure Client は WebAuthN およびその他の SAML ベースの Web 認証オプション（シングルサインオン、生体認証、または組み込みブラウザでは利用できないその他の拡張方法など）をサポートします。SAML 外部ブラウザを使用するには、『Cisco ASA Series VPN CLI Configuration Guide, 9.17』[英語] の「*Configure Default OS Browser for SAML Authentication*」セクションで説明されている設定を実行する必要があります。

プラットフォーム固有の要件

組み込みブラウザで SAML を使用するためには、次のシステム要件を満たす必要があります。

- Windows：Windows 7（またはそれ以降）、Internet Explorer 11（またはそれ以降）
- macOS：macOS 10.10（またはそれ以降）（Cisco Secure Client は、macOS 10.11 以降を公式にサポートしています）
- Linux：WebKitGTK+ 2.1x（それ以降）、Red Hat 7.4（それ以降）および Ubuntu 16.04（それ以降）の公式パッケージ

アップグレード プロセス

ネイティブ（外部）ブラウザ搭載の Cisco Secure Client SAML 2.0 は、Secure Firewall ASA リリース 9.7.x、9.8.x、および 9.9.1 で使用できます。ブラウザが組み込まれた拡張 Cisco Secure Client バージョンは、Secure Firewall ASA 9.7.1.24（またはそれ以降）、9.8.2.28（またはそれ以降）、または 9.9.2.1（またはそれ以降）で使用できます。

組み込みブラウザ SAML 統合を備えたヘッドエンドまたはクライアント デバイスをアップグレードまたは展開するときには、次のシナリオに注意してください。

- Cisco Secure Client を最初に展開した場合は、他に何も操作しなくても、ネイティブ（外部）ブラウザと組み込みブラウザの両方の SAML 統合が想定どおりに機能します。Cisco Secure Client を最初に導入した場合でも、既存または更新された Secure Firewall ASA バージョンがサポートされます。
- 更新された Cisco Secure Firewall ASA バージョン（組み込みブラウザ SAML 統合を含む）を最初に展開する場合は、Cisco Secure Firewall ASA を順にアップグレードする必要があります。デフォルトでは、更新された Cisco Secure Firewall ASA リリースは、以前のリリースのネイティブ（外部）ブラウザ SAML 統合との下位互換性がありません。認証後に既存の Cisco Secure Client クライアントのアップグレードが発生し、このアップグレードを行うためには、トンネルグループ設定で **saml external-browser** コマンドを有効にする必要があります。

SAML を使用する場合は、次の注意事項に従ってください。

- 常時接続 VPN が有効になっている場合は、外部 SAML ID プロバイダーで Always-On VPN を使用する （16 ページ） を参照してください。
- 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。
- （モバイルのみ）単一ログアウトはサポートされていません。
- Web ブラウザに確立された SAML 認証は Cisco 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、Cisco 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 Cisco 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、Secure Firewall ASA 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。
- SAML IdP *NameID* 属性は、ユーザのユーザ名を特定し、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。
- ユーザが SAML 経由で VPN セッションを確立するたびにアイデンティティ プロバイダー（IdP）による再認証を行う場合は、Cisco Secure Client プロファイルエディタ、プリファレンス（Part 1）で [自動再接続（Auto Reconnect）] を *ReconnectAfterResume* に設定する必要があります。
- 組み込みブラウザ搭載の Cisco Secure Client は VPN 試行のたびに新しいブラウザ セッションを使用するため、IDP が HTTP セッションクッキーを使用してログオン状態を追跡している場合には、毎回ユーザーの再認証が必要になります。この場合、**[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [クライアントレスSSL VPNアクセス（Clientless SSL VPN Access）] > [詳細（Advanced）] [シングルサインオンサーバー（Single Sign On Servers）]** > の [強制再認証（Force Re-Authentication）] は、Cisco Secure Client が開始した SAML 認証には影響しません。

SAML の設定の詳細については、最新のリリース（9.7 以降）の『Cisco ASA Series VPN CLI or ASDM Configuration Guide』[英語] を参照してください。

SDI トークン（SoftID）統合を使用した VPN 認証

Cisco Secure Client は、Windows x86（32 ビット）および x64（64 ビット）で動作する RSA SecurID クライアント ソフトウェア バージョン 1.1 以降のサポートを統合します。

RSA SecurID ソフトウェア オーセンティケータは、企業の資産へのセキュアなアクセスのために必要となる管理項目数を減らします。リモート デバイスに常駐する RSA SecurID Software Token は、1 回限定で使用可能なパスコードを 60 秒ごとにランダムに生成します。SDI は Security Dynamics 社製テクノロジーの略称で、ハードウェアとソフトウェアの両方のトークンを使用する、この 1 回限定利用のパスワード生成テクノロジーを意味します。

通常、ユーザーはツールトレイの [Cisco Secure Client] アイコンをクリックし、接続する接続プロファイルを選択してから、認証ダイアログボックスに適切なクレデンシャルを入力すること

で Cisco Secure Client に接続します。ログイン（チャレンジ）ダイアログボックスは、ユーザが属するトンネル グループに設定されている認証タイプと一致しています。ログイン ダイアログボックスの入力フィールドには、どのような種類の入力が認証に必要か明確に示されます。

SDI 認証では、リモート ユーザは Cisco Secure Client ソフトウェア インターフェイスに個人識別番号（PIN）を入力して RSA SecurID パスコードを受け取ります。セキュアなアプリケーションにパスコードを入力すると、RSA Authentication Manager がこのパスコードを確認してユーザにアクセスを許可します。

RSA SecurID ハードウェアまたはソフトウェアのトークンを使用するユーザには、パスコードまたは PIN、PIN、パスコードのいずれかを入力する入力フィールドが表示されます。ダイアログボックス下部のステータス行には、さらにこの点に関連する情報が表示されます。ユーザーは、ソフトウェアトークンの PIN またはパスコードを Cisco Secure Client ユーザーインターフェイスに直接入力します。

最初に表示されるログインダイアログボックスの外観は、セキュア ゲートウェイの設定によって異なります。セキュア ゲートウェイには、メインのログイン ページ、メインのインデックス URL、トンネル グループのログイン ページ、またはトンネル グループの URL（URL/トンネル グループ）からアクセスできます。メインのログインページからセキュアゲートウェイにアクセスするには、[ネットワーク（クライアント）アクセス（Network (Client) Access）] の [AnyConnect 接続プロファイル（AnyConnect Connection Profiles）] ページで [ユーザーに接続の選択を許可する（Allow user to select connection）] チェックボックスをオンにする必要があります。いずれの方法でも、セキュア ゲートウェイはクライアントにログイン ページを送信します。メインのログイン ページにはドロップダウン リストがあり、ここからトンネル グループを選択します。トンネルグループ ログイン ページにはこの表示はありません。トンネルグループは URL で指定されるためです。

メインのログイン ページ（接続プロファイルまたはトンネル グループのドロップダウン リストを表示）の場合、デフォルト トンネル グループの認証タイプによって、パスワードの入力フィールド ラベルの初期設定が決まります。たとえば、デフォルト トンネル グループが SDI 認証を使用する場合、フィールドラベルは [パスコード（Passcode）] になります。一方で、デフォルト トンネル グループが NTLM 認証を使用する場合、フィールド ラベルは [パスワード（Password）] になります。リリース 2.1 以降では、異なるトンネル グループをユーザが選択しても、フィールドラベルが動的に更新されることはありません。トンネルグループのログイン ページでは、フィールド ラベルはトンネルグループの要件に一致します。

クライアントは、パスワード入力フィールドへの RSA SecurID Software Token の PIN の入力をサポートします。RSA SecurID Software Token ソフトウェアがインストールされており、トンネルグループ認証タイプが SDI の場合、フィールド ラベルは [パスコード（Passcode）] となり、ステータス バーには、「ユーザ名およびパスコードまたはソフトウェア トークンPINを入力してください（Enter a username and passcode or software token PIN）」と表示されます。PIN を使用すると、同じトンネル グループおよびユーザ名で行う次回のログインからは、フィールド ラベルが [PIN] になります。クライアントは、入力された PIN を使用して RSA SecurID Software Token DLL からパスコードを取得します。認証が成功するたびにクライアントはトンネル グループ、ユーザ名、認証タイプを保存し、保存されたトンネル グループが新たにデフォルトのトンネル グループとなります。

Cisco Secure Client では、すべての SDI 認証でパスコードを使用できます。パスワード入力ラベルが [PIN] の場合でも、ユーザはステータス バーの指示どおりにパスコードを入力することができます。クライアントは、セキュア ゲートウェイにパスコードをそのまま送信します。パスコードを使用すると、同じトンネル グループおよびユーザ名で行う次回のログインからは、ラベルが [パスコード（Passcode）] のフィールドが表示されます。

RSASecureIDIntegration プロファイル設定は、次の 3 つの値のいずれかになります。

- Automatic：クライアントはまず 1 つの方式を試行し、それが失敗したら別の方式を試行します。デフォルトでは、ユーザ入力がトークン パスコード（HardwareToken）として処理され、これが失敗したら、ユーザ入力がソフトウェア トークン PIN（SoftwareToken）として処理されます。認証が成功すると、成功した方式が新しい SDI トークン タイプとして設定され、ユーザ プリファレンス ファイルにキャッシュされます。SDI トークン タイプは、次回の認証試行でいずれの方式が最初に試行されるかを定義します。通常、現行の認証試行には、最後に成功した認証試行で使用されたトークンと同じものが使用されます。ただし、ユーザ名またはグループの選択を変更した場合は、入力フィールドラベルに示されている、デフォルトの方式が最初に試行される状態に戻ります。

（注） SDI トークン タイプは、設定が自動の場合のみ、意味を持ちます。認証モードが自動以外の場合は、SKI トークン タイプのログを無視できます。HardwareToken がデフォルトの場合、次のトークン モードはトリガーされません。

- SoftwareToken：クライアントは、ユーザー入力を常にソフトウェア トークン PIN として解釈し、入力フィールドラベルは [PIN:] になります。
- HardwareToken：クライアントは、ユーザー入力を常にトークンパスコードとして解釈し、入力フィールドラベルは [Passcode:] になります。

（注） Cisco Secure Client では、RSA Software Token クライアント ソフトウェアにインポートした複数のトークンからの、トークンの選択はサポートされていません。その代わりに、クライアントは RSA SecurID Software Token GUI を介してデフォルト選択のトークンを使用します。

SDI 認証交換のカテゴリ

すべての SDI 認証交換は次のいずれかのカテゴリに分類されます。

- 通常の SDI 認証ログイン
- 新規ユーザー モード
- 新規 PIN モード
- PIN クリア モード

• 次のトークン コード モード

通常の SDI 認証ログイン

通常ログイン チャレンジは、常に最初のチャレンジです。SDI 認証ユーザーは、ユーザー名およびトークン パスコード（ソフトウェア トークンの場合は PIN）を、ユーザー名とパスコードまたは PIN フィールドにそれぞれ指定する必要があります。クライアントはユーザーの入力に応じてセキュア ゲートウェイ（中央サイトのデバイス）に情報を返し、セキュア ゲートウェイはこの認証を認証サーバ（SDI または RADIUS プロキシ経由の SDI）で確認します。

認証サーバーが認証要求を受け入れた場合、セキュア ゲートウェイは認証が成功したページをクライアントに送信します。これで認証交換が完了します。

パスコードが拒否された場合は認証は失敗し、セキュア ゲートウェイは、エラー メッセージとともに新しいログイン チャレンジ ページを送信します。SDI サーバーでパスコード失敗しきい値に達した場合、SDI サーバーはトークンを次のトークンコードモードに配置します。

新規ユーザー モード、PIN クリア モード、および新規 PIN モード

PIN のクリアは、ネットワーク管理者だけの権限で、SDI サーバーでのみ実行できます。

新規ユーザーモード、PIN クリア モード、新規 PIN モードでは、Cisco Secure Client は、後の「next passcode」ログインチャレンジで使用するために、ユーザー作成 PIN またはシステムが割り当てた PIN をキャッシュに入れます。

PIN クリア モードと新規ユーザー モードは、リモート ユーザーから見ると違いがなく、また、セキュア ゲートウェイでの処理も同じです。いずれの場合も、リモート ユーザーは新しい PIN を入力するか、SDI サーバーから割り当てられる新しい PIN を受け入れる必要があります。唯一の相違点は、最初のチャレンジでのユーザーの応答です。

新規 PIN モードでは、通常のチャレンジと同様に、既存の PIN を使用してパスコードが生成されます。PIN クリア モードでは、ユーザーがトークン コードだけを入力するハードウェア トークンとして PIN が使用されることはありません。RSA ソフトウェア トークンのパスコードを生成するために 0 が 8 つ並ぶ PIN（00000000）が使用されます。いずれの場合も、SDI サーバー管理者は、使用すべき PIN 値（ある場合）をユーザーに通知する必要があります。

新規ユーザーを SDI サーバーに追加すると、既存ユーザーの PIN をクリアする場合と同じ結果になります。いずれの場合も、ユーザーは新しい PIN を指定するか、SDI サーバーから割り当てられる新しい PIN を受け入れる必要があります。これらのモードでは、ユーザーはハードウェア トークンとして、RSA デバイスのトークン コードのみ入力します。いずれの場合も、SDI サーバー管理者は、使用すべき PIN 値（ある場合）をユーザーに通知する必要があります。

新規 PIN の作成

現行の PIN がない場合、システム設定に応じて、次の条件のいずれかを満たすことが、SDI サーバーによって要求されます。

• システムがユーザーに新規 PIN を割り当てる必要がある（デフォルト）。

- ユーザーは新規 PIN を作成する必要がある。
- ユーザーは、PIN を作成するか、システムの割り当てを受け入れるかを選択できる。

PIN をリモートユーザー自身で作成する方法とシステムで割り当てる方法を選択できるように SDI サーバーを設定している場合、ログイン画面にはオプションを示すドロップダウン リストが表示されます。ステータス行にプロンプト メッセージが表示されます。

システムが割り当てる PIN の場合、ユーザーがログインページで入力したパスコードを SDI サーバーが受け入れると、セキュアゲートウェイはシステムが割り当てた PIN をクライアントに送信します。クライアントは、ユーザーが新規 PIN を確認したことを示す応答をセキュアゲートウェイに返し、システムは「next passcode」チャレンジに進みます。

ユーザーが新しく PIN を作成するように選択した場合、Cisco Secure Client にこの PIN を入力するためのダイアログボックスが表示されます。PIN は 4 ～ 8 桁の長さの数値にする必要があります。PIN は一種のパスワードであるため、ユーザーがこの入力フィールドに入力する内容はアスタリスクで表示されます。

RADIUS プロキシを使用する場合、PIN の確認は、最初のダイアログボックスの次に表示される、別のチャレンジで行われます。クライアントは新しい PIN をセキュアゲートウェイに送信し、セキュアゲートウェイは「next passcode」チャレンジに進みます。

「next passcode」チャレンジと「next Token Code」チャレンジ

「next passcode」チャレンジでは、クライアントが新規 PIN の作成または割り当て時にキャッシュに入れられた PIN 値を使用して RSA SecurID Software Token DLL から次のパスコードを取得し、ユーザーにプロンプト表示せずにこれをセキュア ゲートウェイに返します。同様に、ソフトウェア トークン用の「next Token Code」チャレンジでは、クライアントは RSA SecurID Software Token DLL から次のトークン コードを取得します。

ネイティブ SDI と RADIUS SDI の比較

ネットワーク管理者は、SDI 認証を可能にするセキュア ゲートウェイを次のいずれかのモードで設定することができます。

- ネイティブ SDI：SDI サーバと直接通信して SDI 認証を処理できるセキュア ゲートウェイのネイティブ機能です。
- RADIUS SDI：RADIUS SDI プロキシを使用して SDI サーバと通信することで SDI 認証を行うセキュア ゲートウェイのプロセスです。

リモート ユーザからは、ネイティブ SDI と RADIUS SDI は同一です。SDI メッセージは SDI サーバー上で設定が可能なため、これには、Cisco Secure Firewall ASA 上のメッセージ テキストは、SDI サーバー上のメッセージテキストに一致する必要があります。一致しない場合、リモート クライアント ユーザーに表示されるプロンプトが、認証中に必要なアクションに対して適切でない場合があり、Cisco Secure Client が応答できずに認証に失敗することがあります。

RADIUS SDI チャレンジは、少数の例外はありますが、基本的にはミラー ネイティブの SDI 交換です。両者とも最終的には SDI サーバと通信するため、クライアントからの必要な情報と要求される情報の順序は同じです。

認証の間に、RADIUS サーバーは Cisco Secure Firewall ASA にアクセス チャレンジ メッセージを提示します。これらのチャレンジ メッセージ内に、SDI サーバからのテキストを含む応答メッセージがあります。このメッセージテキストは、Cisco Secure Firewall ASA が SDI サーバーと直接通信している場合と RADIUS プロキシを経由して通信している場合とで異なります。そのため、Cisco Secure Client にネイティブ SDI サーバとして認識させるために、Cisco Secure Firewall ASA は RADIUS サーバーからのメッセージを解釈する必要があります。

また、SDI メッセージは SDI サーバーで設定可能であるため、Cisco Secure Firewall ASA のメッセージテキストの全体または一部が、SDI サーバーのメッセージテキストと一致する必要があります。一致しない場合、リモート クライアント ユーザーに表示されるプロンプトが、認証中に必要なアクションに対して適切でない場合があり、Cisco Secure Client が応答できずに認証に失敗することがあります。

RADIUS/SDI メッセージをサポートするための Cisco Secure Firewall ASA の設定

SDI 固有の RADIUS 応答メッセージを解釈し、適切なアクションを Cisco Secure Client ユーザーに求めるように Cisco Secure Firewall ASA を設定するには、SDI サーバーとの直接通信をシミュレートする方法で RADIUS 応答メッセージを転送するように接続プロファイル（トンネルグループ）を設定する必要があります。SDI サーバーに認証されるユーザーは、この接続プロファイルを介して接続する必要があります。

ステップ 1 **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [ネットワーク（クライアント）アクセス（Network (Client) Access）] > [AnyConnect接続プロファイル（AnyConnect Connection Profiles）]** を選択します。

ステップ 2 SDI 固有の RADIUS 応答メッセージを解釈するために設定する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 3 [AnyConnect 接続プロファイルの編集（Edit AnyConnect Connection Profile）] ウィンドウで、左側のナビゲーション ペインにある [詳細（Advanced）] ノードを展開して、[グループ エイリアス/グループ URL（Group Alias / Group URL）] を選択します。

ステップ 4 [ログイン画面への SecurID メッセージの表示を有効にする（Enable the display of SecurID messages on the login screen）] をオンにします。

ステップ 5 [OK] をクリックします。

ステップ 6 **[設定（Configuration）] > [リモートアクセスVPN（Remote Access VPN）] > [AAA/ローカルユーザ（AAA/Local Users）] > [AAAサーバグループ（AAA Server Groups）]** を選択します。

ステップ 7 [追加（Add）] をクリックして、AAA サーバ グループを追加します。

ステップ 8 [AAA サーバ グループの編集（Edit AAA Server Group）] ダイアログで AAA サーバ グループを設定して、[OK] をクリックします。

ステップ 9 [AAA サーバ グループ（AAA Server Groups）] 領域で作成した AAA サーバ グループを選択し、[選択したグループ内のサーバ（Servers in the Selected Group）] 領域で [追加（Add）] をクリックします。

ステップ 10 [SDI メッセージ（SDI Messages）] 領域で [メッセージ テーブル（Message Table）] 領域を展開します。メッセージテキスト フィールドをダブルクリックするとメッセージを編集できます。RADIUS サーバーから送信されたメッセージとテキストの一部または全体が一致するように、RADIUS 応答メッセージテキストを Cisco Secure Firewall ASA で設定します。

次の表に、メッセージコード、デフォルトのRADIUS応答メッセージテキスト、および各メッセージの機能を示します。

（注） Cisco Secure Firewall ASA が使用するデフォルトのメッセージテキストは、Cisco Secure Access Control Server（ACS）で使用されるデフォルトのメッセージテキストです。Cisco Secure ACS を使用していて、デフォルトのメッセージテキストを使用している場合、Cisco Secure Firewall ASA でメッセージテキストを設定する必要はありません。

セキュリティ アプライアンスは、テーブルでの出現順に文字列を検索するため、メッセージテキスト用に使用する文字列が別の文字列のサブセットでないことを確認する必要があります。たとえば、「new PIN」が new-pin-sup と next-ccode-and-reauth の両方に対するデフォルトのメッセージ テキストのサブセットであるとします。new-pin-sup を「new PIN」として設定した場合、セキュリティ アプライアンスは RADIUS サーバから「new PIN with the next card code」を受信すると、next-ccode-and-reauth コードではなく new-pin-sup コードとテキストを照合します。

メッセージコード	デフォルトの RADIUS 応答メッセージ テキスト	機能
next-code	Enter Next PASSCODE	ユーザは PIN を入力せずに次のトークンコードを入力する必要があることを示します。
new-pin-sup	Please remember your new PIN	新しいシステムの PIN が提供されており、ユーザにその PIN を表示することを示します。
new-pin-meth	Do you want to enter your own pin	新しい PIN の作成にどの新しい PIN 方式を使用するかをユーザに尋ねます。
new-pin-req	Enter your new Alpha-Numerical PIN	ユーザ生成の PIN を入力することを要求することを示します。
new-pin-reenter	Reenter PIN:	ユーザーが提供した PIN の確認のために Cisco Secure Firewall ASA が内部的に使用します。ユーザにプロンプトを表示せずに、クライアントが PIN を確認します。
new-pin-sys-ok	New PIN Accepted	ユーザが提供した PIN が受け入れられたことを示します。
next-ccode-and-reauth	new PIN with the next card code	PIN操作後、次のトークンコードを待ってから、認証のために新しい PIN と次のトークンコードの両方を入力する必要があることをユーザに示します。
ready-for-sys- pin	ACCEPT A SYSTEM GENERATED PIN	ユーザーがシステム生成の PIN に対する準備ができていることを示すために Cisco Secure Firewall ASA が内部的に使用します。

ステップ 11　[OK]、[適用（Apply）]、[保存（Save）] の順にクリックします。

証明書のピン留めについて

Cisco Secure Client の証明書のピン留めは、サーバー証明書チェーンが実際に接続しているサーバーから来たものであるか検出するのに役立ちます。この機能は VPN プロファイル設定に基づくもので、Cisco Secure Client サーバー証明書検証ポリシーへの追加機能です。Cisco Secure Client のローカルポリシーファイルでの厳格な証明書トラストの設定は、証明書のピン留めチェックに影響しません。ピンは、VPNプロファイルで、グローバルにまたはホストごとに設定できます。プライマリ ホストについて設定されたピンは、サーバ リスト内のバックアップ ホストに対しても有効です。証明書のピン留めチェックを実行するプリファレンスをユーザが制御することはできません。ピン検証が失敗すると、VPN 接続が終了します。

（注）　Cisco Secure Client は、プリファレンスが有効になっており、接続サーバーの VPN プロファイルにピンがあるときのみ、ピン検証を実行します。

プリファレンスの有効化とグローバルおよびホストごとの証明書ピンの設定は、VPNプロファイル エディタ（Cisco Secure Client プロファイルエディタの証明書ピン）で行うことができます。

証明書のピン留めを設定および維持するにあたっては、注意が必要です。プリファレンスを設定するときは、次の推奨事項を考慮してください。

- ルート証明書および/または中間証明書をピン留めする。理由は、これらはオペレーティング システムにおいて CA ベンダーによって十分に管理されているためです。
- CA が侵害された場合のバックアップとなるよう、別の CA からの複数のルート証明書および/または中間証明書をピン留めする。
- CA の移行が容易になるよう、複数のルート証明書および/または中間証明書をピン留めする。
- リーフ証明書がピン留めされている場合は、証明書の更新時に公開キーを保持するため、同一の証明書署名要求を使用する。
- サーバ リスト内のすべての接続ホストをピン留めする。

グローバル ピンとホストごとのピン

証明書ピンは、グローバルまたはホストごとに設定できます。大部分の接続ホストに対して有効なピンは、グローバル ピンとして設定されます。ルート証明書、中間証明機関の証明書、およびワイルドカード リーフ証明書は、VPN プロファイルのグローバル ピンの下に設定することを推奨します。1 つの接続ホストに対してのみ有効なピンは、ホストごとのピンと見なされます。リーフ証明書、自己署名の証明書は、VPNプロファイルのホストごとのピンの下に設定することを推奨します。

（注） Cisco Secure Client は、ピン検証において、対応する接続サーバーのグローバルピンおよびホストごとのピンをチェックします。

（注） 複数の VPN プロファイルにまたがるグローバル ピンは、マージされません。ピンは、VPN 接続のためのファイル接続サーバから厳格に考慮されます。

（注） ホストごとの証明書のピン留めができるのは、[グローバル ピン（Global Pins）] セクションで証明書ピン留めのプリファレンスが有効になっている場合のみです。

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。