サイト間 VPN トンネル構成認証

サイト間 VPN トンネル構成認証

ASA構成ファイルからのクリアテキスト形式での事前共有キーの取得

ASA では、設定した事前共有キーは暗号化されたハッシュとして保存されます。したがって、*show run* コマンドを使用したときに、実行構成で、事前共有キーがクリアテキストで表示されることはありません。

事前共有キーをクリアテキスト形式で取得するには、次の手順を実行します。

手順

ステップ 1 SSH コンソールから ASA に接続し、*more system:running-config* コマンドを入力します。

このコマンドにより、事前共有キーがクリアテキスト形式で表示されます。

ステップ 2 **tunnel-group** セクションに移動して、すべてのトンネルピアとクリアテキスト形式の各事前共有キー値を確認します。

```
ciscoASA# more system:running-config
!
tunnel-group 1.1.1.1 type ipsec-l2l
tunnel-group 1.1.1.1 ipsec-attributes
pre-shared-key <PSK-in-plaintext> <-----The pre-shared-key is now displayed in clear
text format.
```

ASA 構成ファイルまたは Live Connect ASA からの事前共有キーの自動取得

Firepower 移行ツール 3.0 は、送信元が Live Connect ASA である場合、または **More System: Running Configuration** ファイルがアップロードされている場合は、サイト間 VPN に使用されている事前共有キーの取得を自動化します。

IKEv2 ベースの VPN では、ローカル認証キーとリモート認証キーが同じでない場合はリモート認証キーが取得されます。

からの PKI 証明書のエクスポートと Firewall Management Center へのインポート

Firewall 移行ツール 2.4 では、証明書ベースの VPN の Firewall Management Center への移行がサポートされるようになりました。

ASA では、トラストポイントモデルを使用して、証明書を構成に保存します。トラストポイントは、証明書が保存されるコンテナです。ASA トラストポイントは最大 2 つの証明書を保存できます。

構成ファイルの ASA トラストポイントまたは証明書にはハッシュ値が含まれています。したがって、Firewall Management Center に直接インポートすることはできません。

インポート先の Firewall Management Center で、移行前アクティビティの一環として、トラストポイントまたは VPN 証明書を PKI オブジェクトとして手動で移行します。このアクティビティは、 Firewall 移行ツール を使用した移行を開始する前に実行する必要があります。

手順

ステップ 1 次のコマンドを使用し、CLI を介してインポート元の から PKI 証明書をキーとともに PKCS12 ファイルにエクスポートします。

```
ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>
```

ステップ 2 PKI 証明書を Firewall Management Center にインポートします（**[オブジェクト管理（Object Management）] > [PKI オブジェクト（PKI Objects）]**）。

詳細については、『Firewall Management Center Configuration Guide』[英語] を参照してください。

手動で作成した PKI オブジェクトは、 Firewall 移行ツール の [VPNトンネル（VPN Tunnels）] セクションの [確認と検証（Review and Validate）] ページで使用できます。