リモート アクセス IPSec VPN

リモート アクセス IPSec VPN の概要

リモート アクセス VPN を使用すると、TCP/IP ネットワーク上のセキュアな接続を介して、ユーザーを中央サイトに接続することができます。Internet Security Association and Key Management Protocol は IKE とも呼ばれ、リモート PC の IPsec クライアントと ASA で、IPsec セキュリティアソシエーションの構築方法を一致させるためのネゴシエーションプロトコルです。各 ISAKMP ネゴシエーションは、フェーズ 1 とフェーズ 2 と呼ばれる 2 つの部分に分かれます。

フェーズ 1 は、以後の ISAKMP ネゴシエーション メッセージを保護する最初のトンネルを作成します。フェーズ 2 は、セキュアな接続を移動するデータを保護するトンネルを作成します。

ISAKMP ネゴシエーションの条件を設定するには、ISAKMP ポリシーを作成します。ここでは、次の項目について説明します。

- ピアの ID を確認する認証方式。
- データを保護し、プライバシーを守る暗号化方式。
- 送信者を特定し、搬送中にメッセージが変更されていないことを保証する Hashed Message Authentication Code（HMAC）方式。

- 暗号キーのサイズを設定する Diffie-Hellman グループ。
- 暗号キーを置き換える前に、ASA がその暗号キーを使用する時間の上限。

トランスフォーム セットは、暗号化方式と認証方式を組み合わせたものです。特定のデータ フローを保護する場合、ピアは、ISAKMP との IPsec セキュリティ アソシエーションのネゴシエート中に、特定のトランスフォーム セットを使用することに同意します。トランスフォーム セットは、両方のピアで同じである必要があります。

トランスフォーム セットにより、関連付けられたクリプト マップ エントリで指定された ACL のデータ フローが保護されます。ASA 設定でトランスフォーム セットを作成して、クリプト マップまたはダイナミック クリプト マップ エントリでトランスフォーム セットの最大数 11 を指定できます。有効な暗号化方式と認証方式をリストしたテーブルなど、さらに詳細な情報については、IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルの作成 （7 ページ）を参照してください。

セキュアクライアントに IPv4 アドレスと IPv6 アドレスの一方または両方を割り当てるように ASA を設定できます。そのように設定するには、ASA 上で内部アドレスプールを作成するか、ASA 上のローカルユーザーに専用アドレスを割り当てます。

エンドポイントに両方のタイプのアドレスを割り当てるには、エンドポイントのオペレーティング システムの中でデュアル スタック プロトコルが実装されている必要があります。どちらのシナリオでも、IPv6 アドレス プールは残っていないが IPv4 アドレスが使用できる場合や、IPv4 アドレス プールは残っていないが IPv6 アドレスが使用できる場合は、接続は行われます。ただし、クライアントには通知されないので、管理者は ASA ログで詳細を確認する必要があります。

クライアントへの IPv6 アドレスの割り当ては、SSL プロトコルに対してサポートされます。

Mobike およびリモート アクセス VPN について

モバイル IKEv2（mobike）は、モバイル デバイスのローミングをサポートするために ASA RA VPN を拡張します。このサポートは、デバイスが現在の接続ポイントから別のポイントに移動するときに、モバイル デバイスの IKE/IPSEC セキュリティ アソシエーション（SA）のエンドポイント IP アドレスが削除されるのではなく更新できることを意味します。

Mobike はバージョン 9.8(1) 以降は ASA でデフォルトにより利用可能です。つまり、Mobike は「常にオン」になります。Mobike は、クライアントがそれを提案し、ASA が受け入れるときにだけ、各 SA に対して有効になります。このネゴシエーションは、IKE_AUTH 交換の一部として行われます。

mobike サポートが有効な状態で SA が確立された後、クライアントはいつでもアドレスを変更して、新しいアドレスを示す UPDATE_SA_ADDRESS ペイロードを含む情報交換を使用して ASA に通知できます。ASA はこのメッセージを処理し、新しいクライアント IP アドレスで SA を更新します。

（注） `show crypto ikev2 sa detail` コマンドを使用して、現在のすべての SA で mobike が有効になっているかどうかを判別できます。

現在の Mobike の実装では、次の機能がサポートされています。

- IPv4 アドレスのみ
- NAT マッピングの変更
- オプションのリターン ルータビリティ チェックによるパス接続と停止検出
- アクティブ/スタンバイ フェールオーバー
- VPN ロード バランシング

RRC（リターン ルータビリティ チェック）機能が有効になっている場合、モバイル クライアントにRRCメッセージが送信され、SAが更新される前に新しいIPアドレスが確認されます。

Cisco Secure Client の AnyConnect VPN モジュールのライセンス要件

（注） この機能は、ペイロード暗号化機能のないモデルでは使用できません。

Secure Firewall ASA ヘッドエンドから Cisco Secure Client（AnyConnect を含む）を展開し、VPN および Secure Firewall ポスチャまたは HostScan モジュールを使用する場合は、Advantage または Premier ライセンスが必要です。トライアルライセンスも使用できます。『Cisco Secure Client 発注ガイド』を参照してください。モデルごとの最大値については、「Cisco ASA Series Feature Licenses」を参照してください。

リモート アクセス IPsec VPN の制限

- ファイアウォール モード ガイドライン：ルーテッド ファイアウォール モードでのみサポートされます。トランスペアレント モードはサポートされていません。
- フェールオーバー ガイドライン IPsec-VPN セッションは、アクティブ/スタンバイ フェールオーバー コンフィギュレーションでのみ複製されます。アクティブ/アクティブ フェールオーバー コンフィギュレーションはサポートされません。
- HA 同期中は設定の変更がブロックされます。この間にユーザーがログインしようとすると、ファイアウォールでの DACL ルールのインストールが失敗する可能性があります。HA 同期が完了すると、ユーザーは正常にログインできます。

- ASA は、サードパーティ製クライアントが Null ユーザー エージェントを送信した場合、リモート アクセス VPN セッションを受け入れません。
- 複数の、頻繁に変更される IP アドレスに解決されるドメインに対して完全修飾ドメイン名（FQDN）アクセス制御リスト（ACL）を使用すると、リモート アクセス VPN 環境でのDHCPアドレスの解決に影響を与える可能性があります。この問題は、外部DHCPサーバーが構成され、ネットワークアドレス変換（NAT）のトランザクション コミットが有効になっている場合に発生する可能性があります。
- Advanced Endpoint Assessment を使用したポスチャ アセスメントでは、SSL 接続の syslog メッセージが生成される場合がありますが、それらは VPN ログオンまたはログオフ イベントと関連付けられません。
- ASA では EAP 方式を終了させないため、ローカル認証はできません。

  ASA は、EAP をパススルーとしてのみサポートし、クライアントの EAP 認証には VPN クライアントの証明書認証を必要とします。リモート認証方式として EAP を構成する場合は、VPNクライアントの証明書認証を構成してください。EAP、PSK、証明書などの複数のリモート認証方式がEAPとともに設定されている場合でも、エラーが表示されます。

リモート アクセス IPsec VPN の設定

このセクションでは、リモート アクセス VPN の設定方法について説明します。

インターフェイスの設定

ASAには、少なくとも2つのインターフェイスがあり、これらをここでは外部および内部と言います。一般に、外部インターフェイスはパブリックインターネットに接続されます。一方、内部インターフェイスはプライベートネットワークに接続され、一般のアクセスから保護されます。

最初に、ASA の 2 つのインターフェイスを設定し、イネーブルにします。次に、名前、IP アドレス、およびサブネット マスクを割り当てます。オプションで、セキュリティ レベル、速度、およびセキュリティ アプライアンスでの二重操作を設定します。

手順

ステップ 1 グローバル構成モードからインターフェイス構成モードに入ります。

interface {*interface*}

例：

```
hostname(config)# interface ethernet0
hostname(config-if)#
```

ステップ 2 インターフェイスに IP アドレスとサブネット マスクを設定します。

ip address *ip_address* [*mask*] [*standby ip_address*]

例：

```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
```

ステップ 3 インターフェイスの名前（最大 48 文字）を指定します。この名前は、設定した後での変更はできません。

nameif *name*

例：

```
hostname(config-if)# nameif outside
hostname(config-if)#
```

ステップ 4 インターフェイスを有効にします。デフォルトでは、インターフェイスは無効です。

例：

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

ISAKMPポリシーの設定と外部インターフェイスでのISAKMPのイネーブル化

手順

ステップ 1 IKEv1 ネゴシエーション中に使用する認証方式とパラメータのセットを指定します。

Priorityは、インターネットキー交換（IKE）ポリシーを一意に識別し、ポリシーにプライオリティを割り当てます。1～65,534 の整数を使用します。1はプライオリティが最も高く、65,534 が最も低くなります。

その後に続く手順では、プライオリティは 1 に設定されます。

ステップ 2 IKE ポリシー内で使用する暗号化方式を指定します。

crypto ikev1 policy *priority* **encryption**{**aes-192** | **aes-256** | | }

例：

ステップ 3 IKE ポリシーのハッシュ アルゴリズムを指定します（HMAC バリアントとも呼ばれます）。

crypto ikev1 policy *priority* **hash** { | **sha**}

例：

```
hostname(config)# crypto ikev1 policy 1 hash sha
hostname(config)#
```

ステップ 4 IKE ポリシーの Diffie-Hellman グループ（IPsec クライアントと ASA が共有秘密キーを確立できる暗号化プロトコル）を指定します。

crypto ikev1 policy *priority* **group** {**14** | | | **19** | **20** | 21}

例：

```
hostname(config)#crypto ikev1 policy 1 group 14
hostname(config)#
```

ステップ 5 暗号キーのライフタイム（各セキュリティアソシエーションが存在し続ける有効期限までの秒数）を指定します。

crypto ikev1 policy *priority* **lifetime** {*seconds*}

限定されたライフタイムの範囲は、120 ～ 2147483647 秒です。 無制限のライフタイムの場合は、0 秒を使用します。

例：

```
hostname(config)# crypto ikev1 policy 1 lifetime 43200
hostname(config)#
```

ステップ 6 outside というインターフェイス上の ISAKMP を有効にします。

crypto ikev1 enable *interface-name*

例：

```
hostname(config)# crypto ikev1 enable outside
hostname(config)#
```

ステップ 7 変更を構成に保存します。

write memory

アドレス プールの設定

ASA では、ユーザーに IP アドレスを割り当てる方式が必要です。この項では、例としてアドレス プールを使用します。

手順

IP アドレスの範囲を使用してアドレス プールを作成します。ASA は、このアドレス プールのアドレスをクライアントに割り当てます。

ip local pool *poolname first-address—last-address* [**mask** *mask*]

アドレス マスクはオプションです。ただし、VPN クライアントに割り当てられた IP アドレスが非標準のネットワークに属し、デフォルトのマスクを使用するとデータが誤ってルーティングされる可能性があるときは、マスク値を指定する必要があります。典型的な例が、IP ローカル プールに 10.10.10.0/255.255.255.0 アドレスが含まれている場合で、これはデフォルトではクラス A ネットワークです。これによって、VPN クライアントがさまざまなインターフェイスで 10 のネットワーク内の異なるサブネットにアクセスする必要がある場合、ルーティングの問題が生じる可能性があります。

例：

```
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)#
```

ユーザーの追加

手順

ユーザー、パスワード、およびそのユーザーの特権レベルを作成します。

username *name* {**nopassword** | **password** *password* [**mschap** | **encrypted** | **nt-encrypted**]} [**privilege** *priv_level*]

例：

```
Hostname(config)# username testuser password 12345678
```

IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルの作成

この項では、トランスフォーム セット（IKEv1）およびプロポーザル（IKEv2）を設定する方法について説明します。トランスフォームセットは、暗号化方式と認証方式を組み合わせたものです。

次の手順では、IKEv1 および IKEv2 プロポーザルを作成する方法を示します。

手順

ステップ 1 データ整合性を確保するために使用される IPsec IKEv1 暗号化とハッシュ アルゴリズムを指定する IKEv1 トランスフォーム セットを設定します。

crypto ipsec ikev1 transform-set *transform-set-name encryption-method* [*authentication*]

encryption には、次のいずれかの値を指定します。

- esp-aes：128 ビット キーで AES を使用する場合。

- esp-aes-192：192 ビット キーで AES を使用する場合。
- esp-aes-256：256 ビット キーで AES を使用する場合。
- esp-null：暗号化を使用しない場合。

authentication には、次のいずれかの値を指定します。

- esp-md5-hmac：ハッシュ アルゴリズムとして MD5/HMAC-128 を使用する場合。
- esp-sha-hmac：ハッシュ アルゴリズムとして SHA/HMAC-160 を使用する場合。
- esp-none：HMAC 認証を使用しない場合。

例：

AES を使用して IKEv1 トランスフォームセットを設定するには、次のようにします。

```
hostname(config)# crypto ipsec transform set FirstSet esp-aes esp-sha-hmac
```

ステップ 2 IKEv2 プロポーザル セットを設定し、使用される IPsec IKEv2 プロトコル、暗号化、および整合性アルゴリズムを指定します。

esp は、カプセル化セキュリティ ペイロード（ESP）IPsec プロトコルを指定します（現在、唯一サポートされている IPsec のプロトコルです）。

crypto ipsec ikev2 ipsec-proposal *proposal_name*

protocol {**esp**} {**encryption** { | | **aes** | **aes-192** | **aes-256** | } | **integrity** { | **sha-1**}

encryption には、次のいずれかの値を指定します。

- aes：ESP に 128 ビットキー暗号化で AES（デフォルト）を使用する場合。
- aes-192：ESP に 192 ビット キー暗号化で AES を使用する場合。
- aes-256：ESP に 256 ビット キー暗号化で AES を使用する場合。

integrity には、次のいずれかの値を指定します。

- sha-1（デフォルト）は、ESP の整合性保護のために米国連邦情報処理標準（FIPS）で定義されたセキュア ハッシュ アルゴリズム（SHA）SHA-1 を指定します。

IKEv2 プロポーザルの設定手順

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure_proposal

hostname(config-ipsec-proposal)# protocol esp encryption aes intergrity sha-1
```

トンネル グループの定義

トンネル グループは、トンネル接続ポリシーのコレクションです。AAA サーバーを識別するトンネル グループを設定し、接続パラメータを指定し、デフォルトのグループ ポリシーを定義します。ASA は、トンネル グループを内部的に保存します。

ASA システムには、2 つのデフォルト トンネル グループがあります。1 つはデフォルトのリモート アクセス トンネル グループである DefaultRAGroup で、もう 1 つはデフォルトの LAN-to-LAN トンネル グループである DefaultL2Lgroup です。これらのグループは変更できますが、削除はできません。トンネル ネゴシエーションで識別された特定のトンネル グループがない場合は、ASA は、これらのグループを使用して、リモート アクセスおよび LAN-to-LAN トンネル グループのデフォルト トンネル パラメータを設定します。

手順

ステップ 1 IPsec リモート アクセス トンネル グループ（接続プロファイルとも呼ばれます）を作成します。

tunnel-group *name* **type** *type*

例：

```
hostname(config)# tunnel-group testgroup type ipsec-ra
hostname(config)#
```

ステップ 2 トンネル グループ一般属性モードに入ります。このモードでは、認証方式を入力できます。

tunnel-group *name* **general-attributes**

例：

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)#
```

ステップ 3 トンネル グループに使用するアドレス プールを指定します。

address-pool [*(interface name)*] *address_pool1* [*...address_pool6*]

例：

```
hostname(config-general)# address-pool testpool
```

ステップ 4 トンネル グループ IPsec 属性モードに入ります。このモードでは、IKEv1 接続のための IPsec 固有の属性を入力できます。

tunnel-group *name* **ipsec-attributes**

例：

```
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-tunnel-ipsec)#
```

ステップ 5 （任意） 事前共有キー（IKEv1 のみ）を設定します。キーには、1 ～ 128 文字の英数字文字列を指定できます。

適応型セキュリティ アプライアンスとクライアントのキーは同じである必要があります。事前共有キーのサイズが異なる Cisco VPN Client が接続しようとすると、ピアの認証に失敗したことを示すエラー メッセージがクライアントによってログに記録されます。

ikev1 pre-shared-key *key*

例：

```
hostname(config-tunnel-ipsec)# pre-shared-key 44kkaol59636jnfx
```

ダイナミック クリプト マップの作成

ダイナミック クリプトマップは、すべてのパラメータが設定されているわけではないポリシー テンプレートを定義します。これにより、ASA は、リモート アクセス クライアントなどの IP アドレスが不明なピアからの接続を受信することができます。

ダイナミック クリプト マップのエントリは、接続のトランスフォーム セットを指定します。また、逆ルーティングもイネーブルにできます。これにより、ASA は接続されたクライアントのルーティング情報を取得し、それを RIP または OSPF 経由でアドバタイズします。

手順

ステップ 1 ダイナミック クリプトマップを作成し、マップの IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルを指定します。

- IKEv1 の場合は、このコマンドを使用します。

  crypto dynamic-map *dynamic-map-name seq-num* **set ikev1 transform-set** *transform-set-name*

- IKEv2 の場合は、このコマンドを使用します。

  crypto dynamic-map *dynamic-map-name seq-num* **set ikev2 ipsec-proposal** *proposal-name*

例：

```
hostname(config)# crypto dynamic-map dyn1 1 set ikev1 transform-set FirstSet
hostname(config)#
```

```
hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal secure_proposal
hostname(config)#
```

ステップ 2 （オプション）このクリプト マップ エントリに基づく接続に対して逆ルート インジェクションを有効にします。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse-route**

例：

```
hostname(config)# crypto dynamic-map dyn1 1 set reverse route
hostname(config)#
```

ダイナミック クリプト マップを使用するためのクリプト マップ エントリの作成

クリプトマップエントリを作成します。これにより、ASAは、ダイナミック クリプト マップを使用して IPsec セキュリティ アソシエーションのパラメータを設定することができます。

このコマンドに関する次の例では、クリプトマップ名はmymap、シーケンス番号は1、ダイナミック クリプト マップ名は dyn1 です。この名前は、ダイナミック クリプト マップの作成のトピックで作成したものです。

手順

ステップ 1 ダイナミック クリプト マップを使用するクリプト マップ エントリを作成します。

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

例：

```
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
```

ステップ 2 クリプト マップを外部インターフェイスに適用します。

crypto map *map-name* **interface** *interface-name*

例：

```
hostname(config)# crypto map mymap interface outside
```

ステップ 3 変更を構成に保存します。

write memory

マルチコンテキストモードでの IPSec IKEv2 リモートアクセス VPN の設定

リモート アクセス IPsec VPN の設定の詳細については、次の項を参照してください。

- インターフェイスの設定 （4 ページ）
- アドレス プールの設定 （6 ページ）
- ユーザーの追加 （7 ページ）

ポスト量子事前共有キーを使用した VPN 認証

新しいキーであるポスト量子事前共有キー（PPK）と事前共有キー（PSK）を使用して IKEv2 を構成し、量子コンピュータ攻撃から Secure Client と ASA 間の IPsec 通信を保護することができます。セキュアな IPsec 接続のために、クライアントおよび ASA で一致する PPK と PSK のセットを設定する必要があります。Secure Client と ASA は、PPK と PSK を使用して、ネットワークトラフィックの暗号化と復号のキーを取得します。

PPK は、バイナリ フォーマットで暗号学的に生成されます。ASA および Secure Client の設定では、バイナリ PPK を 256 ビットの、64 文字の 16 進文字列に変換する必要があります。

VPN 認証にポスト量子事前共有キーを使用するための前提条件

- ライセンス：ASA には高度暗号化ライセンスが必要です。
- サポートされるバージョン
  - ASA バージョン 9.18.1 以降。
  - Secure Client バージョン 5.1.8.x 以降。
- アドレス プール、IKEv2 プロポーザル、クリプト マップなど、リモート アクセス IPsec/IKEv2 VPN 接続用に ASA の他のすべてのパラメータを構成します。
- バイナリ PPK を生成します。
- バイナリ PPK を 256 ビットの、64 文字の 16 進文字列に変換します。
- クライアント マシンの Windows Credential Manager（WCM）で、Secure Client の PPK と 2 つの PSK の両方を構成します。「Windows Credential Manager でのポスト量子事前共有キーと事前共有キーの構成 （14 ページ）」を参照してください。
- Secure Client の VPN プロファイルで PPK 属性を構成します。「ポスト量子事前共有キー属性を使用した Secure Client の VPN プロファイルの設定 （15 ページ）」を参照してください。
- PPK と PPK ID の値が ASA と Secure Client で同じであることを確認します。

VPN 認証でのポスト量子事前共有キーの使用に関するガイドラインと制限事項

ガイドライン

- 管理者は、各クライアントデバイスへの PPK と PSK の生成、品質、および配布を保証する必要があります。

制限事項

- PSK および PPK を使用する IKEv2 のみがサポートされます。
- Secure Client については、Windows のみをサポートします。
- クライアントは、WCM に 1 つの ASA のログイン情報のみを保存できます。

VPN 認証にポスト量子事前共有キーを使用するためのワークフロー

表 *1: VPN* 認証にポスト量子事前共有キーを使用するためのワークフロー

ステップ	アクション	詳細情報
1	バイナリ PPK を生成し、256 ビットの、64 文字の 16 進文字列に変換します。	-
2	Windows Credential Manager（WCM）で PPK と PSK を構成します。	Windows Credential Manager でのポスト量子事前共有キーと事前共有キーの構成 （14 ページ）
3	PPK パラメータを使用して Secure Client VPN プロファイルを構成します。	ポスト量子事前共有キー属性を使用した Secure Client の VPN プロファイルの設定 （15 ページ）
4	ASA トンネルグループを構成します。	ポスト量子事前共有キーを使用した ASA での VPN 認証の構成 （16 ページ）
5	ユーザーは、ASA に接続するために Secure Client にログインします。	-
6	Secure Client は VPN プロファイルの PPK_ID を使用して、WCM から PPK と 2 つの PSK を取得します。	-

ステップ	アクション	詳細情報
7	Secure Client は、ASA トンネルグループのパラメータを使用して、WCM 内の PPK および PSK パラメータを確認します。	-
8	Secure Client と ASA の PPK と PSK が一致する場合、Secure Client は ASA との VPN 接続を確立します。 PPK と PSK が一致しない場合、ASA との VPN 接続は失敗します。	-

Windows Credential Manager でのポスト量子事前共有キーと事前共有キーの構成

PPK、ローカル PSK、およびリモート PSK に別々のクレデンシャルエントリを構成する必要があります。

始める前に

必ずVPN 認証にポスト量子事前共有キーを使用するための前提条件 （12 ページ）およびVPN 認証でのポスト量子事前共有キーの使用に関するガイドラインと制限事項 （13 ページ）を確認してください。

手順

ステップ 1 Windows クライアントマシンで、**[コントロールパネル（Control Panel）] > [ユーザーアカウント（User Accounts）] > [資格情報の管理（Credential Manager）]**を選択します。

ステップ 2 **[Windows 資格情報（Windows Credentials）]** タブをクリックします。

ステップ 3 **[汎用資格情報の追加（Add a Generic Credential）] を**クリックします。

ステップ 4 **[インターネットまたはネットワークのアドレス（Internet or network address）]** フィールドで、次のいずれかの値を指定します。

- PPK の場合は、値を **AC/PPK/<HostAddress>** と指定します（ポスト量子事前共有キー）。これは WCM に 64 桁の 16 進数で格納され、クライアントがバイナリに変換してから、IKEv2 の暗号化および復号キーの導出にこのキーを含めます。
- ローカル PSK の場合、値を **AC/PSK_Local/<HostAddress>** と指定します（クライアントの PSK）。
- リモート PSK の場合、値を **AC/PSK_Remote/<HostAddress>** と指定します（ASA の PSK）。

ステップ 5 Secure Client では使用しないため、**[ユーザー名（User name）]** フィールドでは値を **[n/a]**として指定します。

ステップ 6 **[パスワード（Password）]** フィールドで、次のいずれかの値を指定します。

- PPK の場合は、256 ビットの、64 文字の 16 進数文字列です。
- ローカルおよびリモート PSK の場合、トンネルグループエイリアスを指定する文字列を指定します。

ステップ 7 [OK] をクリックします。

クライアントと ASA が適切に構成されている場合、クライアントは VPN プロファイルの PPK_ID を使用して、WCM から PPK と 2 つの PSK を取得します。Secure Client は上記の PPK および PSK の値を使用し、PPK をバイナリに変換し、PPK および PSK の値を ASA 設定と照合して、VPN 認証を実行します。これら 3 つのキーが認証資格情報であるため、VPN 接続を確立するために他の入力は必要ありません。

ポスト量子事前共有キー属性を使用した Secure Client の VPN プロファイルの設定

VPN プロファイルの **HostEntry** パラメータには、Secure Client の PPK パラメータを構成するための次のような新しいフィールドがあります：

- **IKEIdentity**：ピア ASA を識別するための文字列を指定します。この文字列は、ASA のトンネル グループ名と一致している必要があります。
- **PPK_ID**：PPK を識別する一意の文字列を指定します。この値は、ASA の PPK ID と一致している必要があります。
- **PPK_mandatory**：VPN 接続に PPK が必須の場合、値を true に指定します。この値を構成しない場合、PPK の設定はオプションになります。

例

VPN プロファイルの HostEntry の例を次に示します：

```
<HostEntry>
<HostName> ASAv_PPK</HostName>
<HostAddress>192.168.1.2</HostAddress>
<UserGroup>IPSec_Profile</UserGroup>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true</StandardAuthenticationOnly>
 <IKEIdentity>secure_client_PPK</IKEIdentity>
 <PPK_ID>PPKID_test</PPK_ID>
</PrimaryProtocol>
</HostEntry>
```

ポスト量子事前共有キーを使用した ASA での VPN 認証の構成

ASA のトンネル グループでは、VPN 接続のグループ ポリシーが識別されます。トンネル グループ ポリシーを構成し、PPK および PSK を使用して VPN 認証を有効にすることができます。

始める前に

必ずVPN 認証にポスト量子事前共有キーを使用するための前提条件 （12 ページ）およびVPN 認証でのポスト量子事前共有キーの使用に関するガイドラインと制限事項 （13 ページ）を確認してください。

手順

ステップ 1 トンネル グループの IPsec 属性を構成します。

tunnel-group *name* **ipsec-attributes**

例：

```
hostname(config)# tunnel-group secure_client_PPK ipsec-attributes
hostname(config-tunnel-ipsec)#
```

ステップ 2 クライアントの PSK を構成します。

ikev2 remote-authentication pre-shared-key *key*

例：

```
hostname(config-tunnel-ipsec)#ikev2 remote-authentication pre-shared-key *****
```

ステップ 3 ASA の PSK を構成します。

ikev2 local-authentication pre-shared-key *key*

例：

```
hostname(config-tunnel-ipsec)#ikev2 local-authentication pre-shared-key *****
```

ステップ 4 クライアントの PPK を構成します。

ikev2 remote-authentication post-quantum-key *key* **identifier** *id* mandatory

- key：PPK キーを指定します。
- ID：PPK を識別する一意の文字列を指定します。この値は、Secure Client の VPN プロファイルの PPK ID と一致している必要があります。
- mandatory：VPN 接続に PPK が必須かどうかを指定します。mandatory を指定しない場合、PPK の構成はオプションになります。

例：

```
hostname(config-tunnel-ipsec)#ikev2 remote-authentication post-quantum-key  *****
 identifier PPKID_test mandatory
```

次に、PPK と PSK を使用した ASA トンネル グループ構成のスニペットの例を示します。

例

```
tunnel-group secure_client_PPK ipsec-attributes
       ikev2 remote-authentication pre-shared-key *****
       ikev2 local-authentication pre-shared-key *****
       ikev2 remote-authentication post-quantum-key ***** identity PPKID_test mandatory
```

次の点に注意してください。

- トンネル グループ名は、VPN プロファイルの IKEIdentity 文字列と一致している必要があります。
- トンネル グループ構成の PPK ID は、VPN プロファイルの PPK_ID と一致している必要があります。

その他の参考資料

- RFC 8784
- Cisco Secure Client（AnyConnect を含む）リリース 5 管理者ガイド

リモート アクセス IPsec VPN の設定例

次の例は、リモート アクセス IPsec/IKEv1 VPN を設定する方法を示しています。

```
hostname(config)# crypto ikev1 policy 10
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption aes-256
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config)# crypto ikev1 enable outside
hostname(config)# ip local pool POOL 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev1 transform set AES256-SHA
esp-aes-256 esp-sha-hmac
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# address-pool POOL
hostname(config)# tunnel-group RAVPN ipsec-attributes
hostname(config-ipsec)# ikev1 pre-shared-key ravpnkey
hostname(config)# crypto dynamic-map DYNMAP 1 set ikev1
transform-set AES256-SHA
hostname(config)# crypto dynamic-map DYNMAP 1 set reverse-route
hostname(config)# crypto map CMAP 1 ipsec-isakmp dynamic DYNMAP
hostname(config)# crypto map CMAP interface outside
```

次の例は、リモート アクセス IPsec/IKEv2 VPN を設定する方法を示しています。

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)# integrity sha512
hostname(config-ikev2-policy)# prf sha512
hostname(config)# crypto ikev2 enable outside
hostname(config)# ip local pool POOL 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev2 ipsec-proposal  AES256-SHA512
hostname(config-ipsec-proposal)# protocol esp encryption  aes-256
hostname(config-ipsec-proposal)# protocol esp integrity sha-512
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# address-pool POOL
hostname(config)# tunnel-group RAVPN ipsec-attributes
hostname(config-tunnel-ipsec)# ikev2 local-authentication
pre-shared-key localravpnkey
hostname(config-tunnel-ipsec)# ikev2 remote-authentication
pre-shared-key remoteravpnkey
hostname(config)# crypto dynamic-map DYNMAP 1 set ikev2
ipsec-proposal AES256-SHA512
hostname(config)# crypto dynamic-map DYNMAP 1 set reverse-route
hostname(config)# crypto map CMAP 1 ipsec-isakmp dynamic DYNMAP
hostname(config)# crypto map CMAP interface outside
```

マルチコンテキストモードでの標準ベース IPSec IKEv2 リモートアクセス VPN の設定例

次の例は、マルチコンテキスト モードで標準ベース リモート アクセス IPsec/IKEv2 VPN 用の ASA を構成する方法を示しています。この例では、システム コンテキストおよびユーザー コンテキストの設定について、それぞれ情報を提供します。

システム コンテキストの設定：

```
class default
  limit-resource All 0
  limit-resource Mac-addresses 65536
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
  limit-resource VPN AnyConnect 4.0%

hostname(config)#context CTX2
hostname(config-ctx)#member default   ===============> License allotment for contexts
using class
hostname(config-ctx)#allocate-interface Ethernet1/1.200
hostname(config-ctx)#allocate-interface Ethernet1/3.100
hostname(config-ctx)#config-url disk0:/CTX2.cfg
```

ユーザー コンテキストの設定：

```
hostname/CTX2(config)#ip local pool CTX2-pool 1.1.2.1-1.1.2.250 mask 255.255.255.0
hostname/CTX2(config)#aaa-server ISE protocol radius
hostname/CTX2(config)#aaa-server ISE (inside) host 10.10.190.100
hostname/CTX2(config-aaa-server-host)#key *****
hostname/CTX2(config-aaa-server-host)#exit
hostname/CTX2(config)#


hostname/CTX2(config)#group-policy GroupPolicy_CTX2-IKEv2 internal
hostname/CTX2(config)#group-policy GroupPolicy_CTX2-IKEv2 attributes
hostname/CTX2(config-group-policy)#vpn-tunnel-protocol ikev2
hostname/CTX2(config-group-policy)#exit
hostname/CTX2(config)#


hostname/CTX2(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
hostname/CTX2(config)#crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
hostname/CTX2(config)#crypto map outside_map interface outside
```

デフォルトでは、標準ベース クライアントからの IPSec/IKEv2 リモート アクセス接続は、トンネル グループ DefaultRAGroup に分類されます。

```
hostname/CTX2(config)#tunnel-group DefaultRAGroup type remote-access
hostname/CTX2(config)#tunnel-group DefaultRAGroup general-attributes
hostname/CTX2(config-tunnel-general)#default-group-policy GroupPolicy_CTX2-IKEv2
hostname/CTX2(config-tunnel-general)#address-pool CTX2-pool
hostname/CTX2(config-tunnel-general)#authentication-server-group ISE
hostname/CTX2(config-tunnel-general)#exit
hostname/CTX2(config)#

hostname/CTX2(config)#tunnel-group DefaultRAGroup ipsec-attributes
hostname/CTX2(config-tunnel-ipsec)#ikev2 remote-authentication eap query-identity
hostname/CTX2(config-tunnel-ipsec)#ikev2 local-authentication certificate ASDM_TrustPoint0
hostname/CTX2(config-tunnel-ipsec)#exit
hostname/CTX2(config)#
```

マルチコンテキスト モードでの セキュアクライアント IPSec IKEv2 リモートアクセス VPN の構成例

次の例は、マルチコンテキスト モードでセキュアクライアント リモートアクセス IPsec/IKEv2 VPN 用の ASA を構成する方法を示しています。この例では、システム コンテキストおよびユーザー コンテキストの設定について、それぞれ情報を提供します。

システム コンテキストの設定：

```
class default
    limit-resource All 0
    limit-resource Mac-addresses 65536
    limit-resource ASDM 5
    limit-resource SSH 5
    limit-resource Telnet 5
    limit-resource VPN AnyConnect 4.0%
```

```
hostname(config)#context CTX3
hostname(config-ctx)#member default   ===============> License allotment for contexts
using class
hostname(config-ctx)#allocate-interface Ethernet1/1.200
hostname(config-ctx)#allocate-interface Ethernet1/3.100
hostname(config-ctx)#config-url disk0:/CTX3.cfg
```

各コンテキストの仮想ファイルシステムの作成では、イメージ、プロファイルなどのセキュアクライアント ファイルを使用できます。

```
hostname(config-ctx)#storage-url shared disk0:/shared disk0
```

ユーザー コンテキストの設定：

```
hostname/CTX3(config)#ip local pool ctx3-pool 1.1.3.1-1.1.3.250 mask 255.255.255.0
hostname/CTX3(config)#webvpn
hostname/CTX3(config-webvpn)#enable outside
hostname/CTX3(config-webvpn)# anyconnect image
disk0:/anyconnect-win-4.6.00010-webdeploy-k9.pkg 1
hostname/CTX3(config-webvpn)#anyconnect profiles IKEv2-ctx1 disk0:/ikev2-ctx1.xml
hostname/CTX3(config-webvpn)#anyconnect enable
hostname/CTX3(config-webvpn)#tunnel-group-list enable


hostname/CTX3(config)#username cisco password *****
hostname/CTX3(config)#ssl trust-point ASDM_TrustPoint0 outside
hostname/CTX3(config)#group-policy GroupPolicy_CTX3-IKEv2 internal
hostname/CTX3(config)#group-policy GroupPolicy_CTX3-IKEv2 attributes


hostname/CTX3(config-group-policy)#vpn-tunnel-protocol ikev2 ssl-client
hostname/CTX3(config-group-policy)#dns-server value 10.3.5.6
hostname/CTX3(config-group-policy)#wins-server none
hostname/CTX3(config-group-policy)#default-domain none
hostname/CTX3(config-group-policy)#webvpn
hostname/CTX3(config-group-webvpn)#anyconnect profiles value IKEv2-ctx1 type user
```

次の例では、クライアントサービスを有効にするために、**crypto ikev2 enable outside client-services** コマンドを使用しています。

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

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

```
hostname/CTX3(config)#crypto ikev2 enable outside client-services port 443
hostname/CTX3(config)#crypto ikev2 remote-access trustpoint ASDM_TrustPoint0
hostname/CTX3(config)#crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
hostname/CTX3(config)#crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
hostname/CTX3(config)#crypto map outside_map interface outside
```

```
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 type remote-access
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 general-attributes
hostname/CTX3(config-tunnel-general)#default-group-policy GroupPolicy_CTX3-IKEv2
hostname/CTX3(config-tunnel-general)#address-pool ctx3-pool
hostname/CTX3(config)#tunnel-group CTX3-IKEv2 webvpn-attributes
hostname/CTX3(config-tunnel-webvpn)#group-alias CTX3-IKEv2 enable
```

リモート アクセス VPN の機能履歴

機能名	リリース	機能情報
IPsec IKEv1 および SSL のリモート アクセス VPN	7.0	リモート アクセス VPN を使用すると、インターネットなどの TCP/IP ネットワーク上のセキュアな接続を介して、ユーザーを中央サイトに接続することができます。
IPsec IKEv2 のリモート アクセス VPN	8.4(1)	セキュアクライアント の IPsec IKEv2 サポートが追加されました。
リモート アクセス VPN の自動 mobike サポート。	9.8(1)	IPsec IKEv2 RA VPN に対するモバイル IKE（mobike）のサポートが追加されました。Mobike は常にオンになっています。 IKEv2 RA VPN 接続のための mobike 通信時のリターン ルータビリティ チェックを有効にできるよう、`ikev2 mobike-rrc` コマンドが追加されました。
マルチコンテキスト モードでの IPsec IKEv2 のリモート アクセス VPN	9.9(2)	セキュアクライアント やサードパーティ製標準ベース IPSec IKEv2 VPN クライアントがマルチコンテキストモードで稼働する ASA へのリモートアクセス VPN セッションを確立できるように ASA を設定することをサポートします。 認証ペイロードに署名する `ikev2 rsa-sig-hash sha1` コマンドが追加されました。
認証ペイロードに署名するための SHA-1 ハッシュアルゴリズムを使用した RSA	9.12(1)	サードパーティの標準ベースの IPSec IKEv2 VPN クライアントを使用して、ASA へのリモートアクセス VPN セッションを確立する際の、SHA-1 ハッシュアルゴリズムによる認証ペイロードの署名をサポート。

機能名	リリース	機能情報
IKE/IPsec 暗号化および整合性/PRF 暗号の廃止 DH グループ 14 での IKEv1 のサポート	9.13(1)	次の暗号化/整合性/PRF 暗号は廃止され、以降のリリース 9.14(1) で削除されます。 • 3DES 暗号化 • DES 暗号化 • MD5 の整合性 IKEv1 での DH グループ 14（デフォルト）サポートが追加されました。グループ 2 およびグループ 5 コマンドオプションは廃止され、以降のリリース 9.14(1) で削除されます。

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