



# リモート アクセス IPsec VPN

- [リモートアクセス IPsec VPN の概要 \(1 ページ\)](#)
- [Cisco Secure Client の AnyConnect VPN モジュールのライセンス要件 \(3 ページ\)](#)
- [リモートアクセス IPsec VPN の制限 \(3 ページ\)](#)
- [リモート アクセス IPsec VPN の設定 \(4 ページ\)](#)
- [ポスト量子事前共有キーを使用した VPN 認証 \(12 ページ\)](#)
- [ポータル アクセス ルールの設定 \(17 ページ\)](#)
- [地理位置情報に基づくリモートユーザーの VPN アクセスの設定 \(18 ページ\)](#)
- [リモート アクセス IPsec VPN の設定例 \(21 ページ\)](#)
- [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 \(22 ページ\)](#)
- [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 \(23 ページ\)](#)
- [リモート アクセス VPN の機能履歴 \(25 ページ\)](#)

## 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、接続は行われません。ただし、クライアントには通知されないため、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、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イネーブルにします。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（HMAC バリエーションとも呼ばれます）を指定します。

```
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有効期限まで存在する秒数) 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 integrity 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せんが、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時、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 44kkaol59636jnfxf
```

## 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リバース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IPsecVPN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)

- [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 \(7 ページ\)](#)
- [トンネル グループの定義 \(9 ページ\)](#)
- [ダイナミック クリプト マップの作成 \(10 ページ\)](#)
- [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 \(11 ページ\)](#)

## 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 資格情報マネージャー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 プロファイルの構成 \(15 ページ\)](#) 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 のクレデンシャル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

手順	操作	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 資格情報マネージャー (WCM) で PPK と PSK を構成します。	<a href="#">Windows 資格情報マネージャー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)</a>
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。	<a href="#">ポスト量子事前共有キー属性を使用した Secure Client の VPN プロファイルの構成 (15 ページ)</a>
4	ASA トンネルグループを構成します。	<a href="#">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)</a>
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。	-

手順	操作	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 資格情報マネージャー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 に別々の資格情報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)] > [資格情報マネージャー (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 進数文字列を指定します。
- 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 プロファイルの構成

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 の構成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> ASAy_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

## ポータル アクセス ルールの設定

HTTP ヘッダー内に存在するデータに基づいて、クライアントレス SSL VPN セッションを許可または拒否するグローバルなクライアントレス SSL VPN アクセスポリシーを構成できます。ASA は、このアクセスポリシーを、エンドポイントが認証する前に評価します。ASA は、アクセスポリシーに従ってクライアントレス SSL VPN セッションを拒否する場合、ただちにエンドポイントにエラーコードを返します。

#### 始める前に

ASA にログインし、グローバル構成モードを開始します。

#### 手順

---

**ステップ 1** 次のコマンドを使用して、クライアントレス SSL VPN 構成モードを開始します。

```
webvpn
```

**ステップ 2** 次のコマンドを使用し、HTTP ヘッダー内の HTTP ヘッダーコードまたは文字列に基づいて、クライアントレス SSL VPN セッションを許可または拒否します。

```
portal-access-rule priority {permit | deny [code code]} {any | user-agent match string}
```

表 2: `portal-access-rule` コマンドのキーワードと変数

パラメータ	説明
<code>priority</code>	ルールの優先順位を指定します。
<code>permit</code>	この設定に基づいて、クライアントレス SSL VPN 接続を許可します。
<code>deny</code>	この設定に基づいて、クライアントレス SSL VPN 接続を拒否します。
<code>code code</code>	HTTP メッセージコードを指定します。指定できる範囲は 200 ~ 599 です。
<code>user-agent match string</code>	要求元のユーザーエージェントのアプリケーション、オペレーティングシステム、ベンダー、またはバージョンを識別する文字列を指定します。

- 文字列を指定するには、文字列の先頭と末尾にワイルドカード (\*) を使用します。ワイルドカードを使用しないと、ルールがどの文字列とも一致しないか、予期したよりも大幅に少ない文字列としか一致しない場合があります。たとえば、`*Thunderbird*` と入力します。
- スペースを含む文字列を指定するには、文字列の先頭と末尾にワイルドカード (\*) を使用し、さらに先頭と末尾に引用符 (" ") を追加します。2 番目の例では、`my agent` が文字列です。

例 :

```
hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match *Thunderbird*
hostname(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match "my agent"
```

## 地理位置情報に基づくリモートユーザーの VPN アクセスの設定

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

地理位置情報ポリシーは、Web VPN ポータルにも適用できます。

## 手順

**ステップ 1** グローバル コンフィギュレーション モードでロケーションを定義するための地理位置情報オブジェクトグループを作成します。

```
object-group geolocation {object-group-name}
```

```
location {country-name}
```

例 :

```
hostname(config)# object-group geolocation South_Asia  
    location "Bangladesh"  
    location "Bhutan"  
    location "India"  
    location "Nepal"  
    location "Maldives"  
    location "Sri Lanka"
```

**ステップ 2** リモートクライアントに地理位置情報ベースのアクセス制御を許可するサービスアクセスポリシーを定義します。

```
service-access {permit|deny} [interface [interface-name] {geolocation object-group-name|any}
```

外部インターフェイスで南アジアからのリモートアクセス SSL ユーザーを許可するには、次のコマンドを実行します。

例 :

```
hostname(config)# service-access permit interface outside ra-ssl-client geolocation South_Asia
```

任意の場所からのすべてのリモートアクセスセッションを拒否するには、次のコマンドを実行します。

例 :

```
hostname(config)# service-access deny ra-ikev2 ra-ssl-client geolocation any
```

次のタスク

## 地理位置情報に基づくアクセス コントロール ポリシーのモニターおよびトラブルシュート

### サービスアクセスポリシーの確認

Cisco ASA デバイスの CLI から次のコマンドを実行します。

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

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

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

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

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

- **show geodb** : 地理位置情報テーブルの詳細を表示します。

**show geodb {ipv4|ipv6} [counters|context] [location country\_name|lookup ip\_address] [detail]**

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

```
firepower# show geodb ipv4
Geolocation Table - IPv4
Total number of mappings available: 532507
Last geolocation data read time: 17:02:13.000 IST Thu Jul 18 2024
Running geolocation update version: 2024-02-15-019
```

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

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

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

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

- **show geodb {ipv4|ipv6} lookup ip\_address** : 特定の IPv4 アドレスまたは IPv6 アドレスの地理位置情報を表示します。

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

### サービスアクセスポリシーのトラブルシューティング

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

## リモート アクセス 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_CRYPTOMAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
hostname/CTX2 (config) #crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTOMAP
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_CRYPTOMAP 65535 set ikev2
ipsec-proposal AES256 AES192 AES 3DES DES
hostname/CTX3 (config) #crypto map outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTOMAP
```

```
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)	<p>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。</p> <ul style="list-style-type: none"><li>• 3DES 暗号化</li><li>• DES 暗号化</li><li>• MD5 の整合性</li></ul> <p>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。</p>

## 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。