



リモート アクセス IPsec VPN

- [リモート アクセス IPsec VPN について \(1 ページ\)](#)
- [リモート アクセス IPsec VPN for 3.1 のライセンス要件 \(3 ページ\)](#)
- [IPsec VPN の制約事項 \(4 ページ\)](#)
- [リモート アクセス IPsec VPN の設定 \(4 ページ\)](#)
- [リモート アクセス IPsec VPN の設定例 \(12 ページ\)](#)
- [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 \(13 ページ\)](#)
- [マルチコンテキスト モードでの AnyConnect IPsec IKEv2 リモート アクセス VPN の設定例 \(14 ページ\)](#)
- [リモート アクセス VPN の機能履歴 \(16 ページ\)](#)

リモート アクセス IPsec VPN について

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ション中に、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。

AnyConnect 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。このようにするには、ASA 上で内部的なアドレス プールを作成するか、ASA 上のローカル ユーザ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。この機能は、IKEv2/IPsec プロトコルに対してはサポートされません。

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。

リモート アクセス IPsec VPN for 3.1 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。

IKEv2 を使用した IPsec リモート アクセス VPN には、別途購入可能な AnyConnect Plus または Apex ライセンスが必要です。AnyConnect ライセンスを購入する場合は、次の最大値を参照してください。IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイト間 VPN では、基本ライセンスに付属の Other VPN ライセンスが使用されます。すべてのタイプの組み合わせ VPN セッションの最大数は、この表に示す最大セッション数を越えることはできません。

モデル	ライセンス要件
ASA 5506-X、5506H-X、5506W-X	• IKEv2 を使用した IPsec リモート アクセス VPN : 50 セッション。 • IKEv1 を使用した IPsec リモート アクセス VPN および IKEv1 または IKEv2 を使用した IPsec サイトツーサイト VPN : • 基本ライセンス : 10 セッション。 • Security Plus ライセンス : 50 セッション。
ASA 5508-X	100 セッションです。
ASA 5512-X	250 セッションです。
ASA 5515-X	250 セッションです。
ASA 5516-X	300 セッションです。

モデル	ライセンス要件
ASA 5525-X	750 セッションです。
ASA 5545-X	2500 セッションです。
ASA 5555-X	5000 セッションです。
ASA 5585-X (SSP-10)	5000 セッションです。
ASA 5585-X (SSP-20、-40、および -60)	10,000 セッションです。
ASASM	10,000 セッションです。
ASAv5	250 セッションです。
ASAv10	250 セッションです。
ASAv30	750 セッションです。

IPsec VPN の制約事項

- 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。

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 コンフィギュレーション モードからインターフェイス コンフィギュレーション 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、インターフェイスはディセーブルです。shutdown

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 | aes-192 | aes-256 | des | 3des}

例 :

```
hostname(config)# crypto ikev1 policy 1 encryption 3des
hostname(config)#
```

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 {md5 | 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 {1 | 2 | 5}

例 :

```
hostname(config)# crypto ikev1 policy 1 group 2
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 をイネーブルにします。

crypto ikev1 enable *interface-name*

例 :

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

ステップ 7 変更をコンフィギュレーションに保存します。

write memory

アドレス プールの設定

ASA では、ユーザに 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)#
```

ユーザの追加

手順

ユーザ、パスワード、および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-des : 56 ビットの DES-CBC を使用する場合。
- esp-3des : Triple DES アルゴリズムを使用する場合。
- 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 :

IKEv1 トランスフォーム セットの設定手順

```
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)#
```

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** {des | 3des | aes | aes-192 | aes-256 | null} | **integrity** {md5 | sha-1}}

encryption には、次のいずれかの値を指定します。

- des : ESP に 56 ビットの DES-CBC 暗号化を使用する場合。
- 3des : (デフォルト) ESP にトリプル DES 暗号化アルゴリズムを使用する場合。
- aes : ESP に 128 ビット キー暗号化で AES 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。
- **null** : ESP に暗号化を使用しない場合。

integrity には、次のいずれかの値を指定します。

- **md5** : ESP の整合性保護のための md5 アルゴリズムを指定。
- **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 des integrity md5
```

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 *nametype 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 *namegeneral-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 nameipsec-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、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 キー

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。

次の作業を実行します。

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-numset* **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-numset* 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 FirstSet
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注入をイネーブルにします。

crypto dynamic-map *dynamic-map-name* *dynamic-seq-numset* 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、前の項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** 変更をコンフィギュレーションに保存します。

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 \(7 ページ\)](#)
- [ユーザの追加 \(7 ページ\)](#)
- [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 \(11 ページ\)](#)

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 を設定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 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 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) #

hostname/CTX2 (config) #crypto ikev2 enable outside client-services port 443
hostname/CTX2 (config) #crypto ikev2 remote-access trustpoint ASDM_TrustPoint0

```

マルチコンテキストモードでの AnyConnect 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 AnyConnect リモート アクセス IPsec/IKEv2 VPN 用の ASA を設定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 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 Cisco Anyconnect ファイルを使用できます。

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

ユーザ 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
```

```
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)	AnyConnect Secure Mobility Client に対する 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)	AnyConnect 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 を構成することをサポートします。