



リモート アクセス IPsec VPN

- [リモート アクセス IPsec VPN について \(1 ページ\)](#)
- [Cisco Secure Client の AnyConnect VPN モジュールのライセンス要件 \(3 ページ\)](#)
- [IPsec VPN の制約事項 \(3 ページ\)](#)
- [リモート アクセス IPsec VPN の設定 \(3 ページ\)](#)
- [リモート アクセス IPsec VPN の設定例 \(11 ページ\)](#)
- [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 \(12 ページ\)](#)
- [マルチコンテキストモードでの AnyConnect クライアント IPsec IKEv2 リモートアクセス VPN の設定例 \(13 ページ\)](#)
- [リモート アクセス VPN の機能履歴 \(15 ページ\)](#)

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。

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。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。

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。

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-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** (任意) 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-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、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 \(6 ページ\)](#)
- [ユーザーの追加 \(6 ページ\)](#)
- [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 \(8 ページ\)](#)
- [ダイナミッククリプトマップの作成 \(9 ページ\)](#)
- [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 \(10 ページ\)](#)

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 AnyConnect クライアント 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 クライアントリモートアクセス 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 AnyConnect 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
```

```
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、 などの TCP/IP ネットワーク上のセキュアな接続を実現し、ユーザーを中央サイトに接続することを実現します。 |
| IPsec IKEv2 のリモート アクセス VPN | 8.4(1) | AnyConnect クライアントの IPsec IKEv2 がサポートされました。 |
| 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 IKEv2 RA サポートが追加されました。Mobike は常に有効です。 IKEv2 RA VPN 接続のための mobike 通信ルータビリティ チェックを有効にできる <code>mobike-rrc</code> 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 クライアント やサードパーティの 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 アクセスセッションを確立できるように ASA を設定する必要があります。 認証ペイロードに署名する <code>ikev2 rsa-signature</code> 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 クライアントを使用して、ASA へのリモート アクセスセッションを確立する際の、SHA-1 ハッシュによる認証ペイロードの署名をサポート。 |
| 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、リリース 9.14(1) で削除されます。 <ul style="list-style-type: none"> • 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) が廃止されました。グループ 2 およびグループ 1 は廃止され、以降のリリースでサポートされます。 |

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。