CHAPTER 73

リモート アクセス IPsec VPN の設定

この章では、リモート アクセス IPsec VPN の設定方法について説明します。次の項目を取り上げます。

リモート アクセス IPsec VPN に関する情報

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。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。
- ASA が暗号キーを置き換える前に、この暗号キーを使用する最長時間の制限。

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アクセス リストのデータ 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、このマニュアルの第 77 章「LAN-to-LAN IPsec VPN の設定」の「IKEv1 トランスフォーム セットの作成」（P.77-5）を参照してください。

リモート アクセス IPsec VPN のライセンス要件

次の表に、この機能のライセンス要件を示します。

（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。

モデル	ライセンス要件[1]
ASA 5505	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンスと Security Plus ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10 または 25 セッション。* *共有ライセンスはサポートされていません。*[2] – AnyConnect Essentials ライセンス[3]：25 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：25 セッション。
ASA 5510	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンスと Security Plus ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* *オプションの共有ライセンス*[2]*：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：250 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： 基本ライセンスと Security Plus ライセンス：250 セッション。

モデル	ライセンス要件[1]
ASA 5520	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、または 750 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：750 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：750 セッション。
ASA 5540	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、または 2500 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：2500 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：2500 セッション。
ASA 5550	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：5000 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：5000 セッション。

モデル	ライセンス要件[1]
ASA 5580	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：10000 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：10000 セッション。
ASA 5512-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：250 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：250 セッション。
ASA 5515-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、または 250 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：250 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：250 セッション。

モデル	ライセンス要件[1]
ASA 5525-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、または 750 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：750 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：750 セッション。
ASA 5545-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、または 2500 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：2500 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：2500 セッション。
ASA 5555-X	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：5000 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：5000 セッション。

モデル	ライセンス要件[1]
ASA 5585-X（SSP-10）	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、または 5000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：5000 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：5000 セッション。
ASA 5585-X（SSP-20、-40、および -60）	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：10000 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：10000 セッション。
ASASM	• IKEv2 を使用した IPsec リモート アクセス VPN（次のいずれかを使用）： – AnyConnect Premium ライセンス： 基本ライセンス：2 セッション。 *オプションの永続または時間ベースのライセンス：10、25、50、100、250、500、750、1000、2500、5000、または 10000 セッション。* *オプションの共有ライセンス[2]：Participant または Server。Server ライセンスでは、500 ～ 50,000（500 単位で増加）および 50,000 ～ 545,000（1000 単位で増加）。* – AnyConnect Essentials ライセンス[3]：10000 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：10000 セッション。

1. 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。ASA 5505 では、組み合わせセッションの最大数は 10（基本ライセンスの場合）または 25（Security Plus ライセンスの場合）です。
2. 共有ライセンスによって、ASA は複数のクライアントの ASA の共有ライセンス サーバとして機能します。共有ライセンス プールは大規模ですが、個々の ASA によって使用されるセッションの最大数は、永続的なライセンスで指定される最大数を超えることはできません。

3. AnyConnect Essentials ライセンスにより、AnyConnect VPN クライアントは ASA へのアクセスが可能になります。このライセンスでは、ブラウザベースの SSL VPN アクセスまたは Cisco Secure Desktop はサポートされていません。これらの機能に対しては、AnyConnect Essentials ライセンスの代わりに AnyConnect Premium ライセンスがアクティブ化されます。

   （注）AnyConnect Essentials ライセンスの場合、VPN ユーザは、Web ブラウザを使用してログインし、AnyConnect クライアントのダウンロードと起動（WebLaunch）を実行できます。

   このライセンスと AnyConnect Premium SSL VPN ライセンスのいずれでイネーブル化されたかには関係なく、AnyConnect クライアント ソフトウェアには同じクライアント機能のセットが装備されています。

   特定の ASA では、AnyConnect Premium ライセンス（全タイプ）または Advanced Endpoint Assessment ライセンスを、AnyConnect Essentials ライセンスと同時にアクティブにすることはできません。ただし、同じネットワーク内の異なる ASA で、AnyConnect Essentials ライセンスと AnyConnect Premium ライセンスを実行することは可能です。

   デフォルトでは、ASA は AnyConnect Essentials ライセンスを使用しますが、このライセンスをディセーブルにして他のライセンスを使用するには **no anyconnect-essentials** コマンドを使用します。

   AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスでサポートされている機能の詳細なリストについては、『*AnyConnect Secure Mobility Client Features, Licenses, and OSs*』を参照してください。

   http://www.cisco.com/en/US/products/ps10884/products_feature_guides_list.html

注意事項と制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングルまたはマルチ コンテキスト モードでサポートされます。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードまたはトランスペアレント ファイアウォール モードではサポートされません。

フェールオーバーのガイドライン

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。

IPv6 のガイドライン

IPv6 はサポートされません。

リモート アクセス IPsec VPN の設定

この項では、リモート アクセス VPN を設定する方法について説明します。次の項目を取り上げます。

- 「インターフェイスの設定」（P.73-8）
- 「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」（P.73-9）
- 「アドレス プールの設定」（P.73-10）

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と内部と言います。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。

インターフェイスを設定するには、例に示すコマンド構文を使用して、次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**interface** {*interface*} **Example:** hostname(config)# interface ethernet0 hostname(config-if)#	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。
ステップ 2	**ip address** *ip_address* [*mask*] [**standby** *ip_address*] **Example:** hostname(config)# interface ethernet0 hostname(config-if)# hostname(config-if)# ip address 10.10.4.200 255.255.0.0	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。
ステップ 3	**nameif** *name* **Example:** hostname(config-if)# nameif outside hostname(config-if)#	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。
ステップ 4	**shutdown** **Example:** hostname(config-if)# no shutdown hostname(config-if)#	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ディセーブルです。

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

この項では、外部インターフェイスに ISAKMP ポリシーを設定する手順と、ポリシーをイネーブルにする方法について説明します。

手順の詳細

次のコマンドを実行します。

	コマンド	目的
ステップ 1	**crypto ikev1 policy** *priority* **authentication** {**crack** | **pre-share** | **rsa-sig**} **Example:** hostname(config)# crypto ikev1 policy 1 authentication pre-share hostname(config)#	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、Internet Key Exchange（IKE; インターネット キー交換）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。 この例および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	**crypto ikev1 policy** *priority* **encryption** {**aes** | **aes-192** | **aes-256** | **des** | **3des**} **Example:** hostname(config)# crypto ikev1 policy 1 encryption 3des hostname(config)#	IKE ポリシー内で使用する暗号化方式を指定します。
ステップ 3	**crypto ikev1 policy** *priority* **hash** {**md5** | **sha**} **Example:** hostname(config)# crypto ikev1 policy 1 hash sha hostname(config)#	IKE ポリシーのハッシュ アルゴリズム（HMAC バリアントとも呼ばれます）を指定します。
ステップ 4	**crypto ikev1 policy** *priority* **group** {**1** | **2** | **5**} **Example:** hostname(config)# crypto ikev1 policy 1 group 2 hostname(config)#	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。
ステップ 5	**crypto ikev1 policy** *priority* **lifetime** {*seconds*} **Example:** hostname(config)# crypto ikev1 policy 1 lifetime 43200 hostname(config)#	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。 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。

	コマンド	目的
ステップ 6	**crypto ikev1 enable** *interface-name* **Example:** hostname(config)# crypto ikev1 enable outside hostname(config)#	*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。
ステップ 7	**write memory** **Example:** hostname(config-if)# write memory Building configuration... Cryptochecksum: 0f80bf71 1623a231 63f27ccf 8700ca6d 11679 bytes copied in 3.390 secs (3893 bytes/sec) [OK] hostname(config-if)#	変更をコンフィギュレーションに保存します。

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。ガイドとして次の例で示すコマンド構文を使用します。

コマンド	目的
ip local pool *poolname first-address*—*last-address* [**mask** *mask*] **Example:** hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15 hostname(config)#	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。 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。

ユーザの追加

この項では、ユーザ名とパスワードを設定する方法について説明します。ガイドとして次の例で示すコマンド構文を使用します。

コマンド	目的
username *name* {**nopassword** | **password** *password* [**mschap** | **encrypted** | **nt-encrypted**]} [**privilege** *priv_level*] **Example:** hostname(config)# username testuser password 12345678 hostname(config)#	ユーザ、パスワード、および特権レベルを作成します。

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。

次の作業を実行します。

コマンド	目的
IKEv1 トランスフォーム セットの設定手順 **crypto ipsec ikev1 transform-set** *transform-set-name encryption-method* [*authentication*] **Example:** hostname(config)# **crypto ipsec transform set FirstSet esp-3des esp-md5-hmac** hostname(config)#	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。 *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**：トリプル 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。
IKEv2 プロポーザルの設定手順 **crypto ipsec ikev2 ipsec-proposal** *proposal_name* その後： **protocol** {**esp**} {**encryption** {**des** | **3des** | **aes** | **aes-192** | **aes-256** | **null**} | **integrity** {**md5** | **sha-1**} **Example:** hostname(config)# **crypto ipsec ikev2 ipsec-proposal secure_proposal** hostname(config-ipsec-proposal)# **protocol esp encryption des integrity md5**	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、Encapsulating Security Payload（ESP; カプセル化セキュリティ ペイロード）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）。 *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、米国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。ESP の整合性保護のための連邦情報処理標準（FIPS）。

トンネル グループの定義

この項では、トンネル グループを設定する方法について説明します。トンネル グループは、トンネル グループは、トンネル接続ポリシーを格納したレコードのセットです。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。これらは変更可能ですが、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。

次の作業を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**tunnel-group** *name* **type** *type* **Example:** hostname(config)# tunnel-group testgroup type ipsec-ra hostname(config)#	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。
ステップ 2	**tunnel-group** *name* **general-attributes** **Example:** hostname(config)# tunnel-group testgroup general-attributes hostname(config-tunnel-general)#	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。
ステップ 3	**address-pool** [(*interface name*)] **address_pool1** [...address_pool6] **Example:** hostname(config-general)# address-pool testpool	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。
ステップ 4	**tunnel-group** *name* **ipsec-attributes** **Example:** hostname(config)# tunnel-group testgroup ipsec-attributes hostname(config-tunnel-ipsec)#	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。
ステップ 5	**ikev1 pre-shared-key** *key* **Example:** hostname(config-tunnel-ipsec)# pre-shared-key 44kkaol59636jnfx	（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。 **（注）**　トンネル グループ webvpn 属性の証明書を使用して、IKEv2 の AAA 認証を設定します。

ダイナミック クリプト マップの作成

この項では、ダイナミック クリプト マップを設定する方法について説明します。ダイナミック クリプト マップは、すべてのパラメータを設定する必要のないポリシー テンプレートを定義します。このようなダイナミック クリプト マップにより、ASA は 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。リモート アクセス クライアントは、このカテゴリに入ります。

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します。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。

手順の詳細

	コマンド	目的
ステップ 1	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* **Example:** hostname(config)# crypto dynamic-map dyn1 1 set ikev1 transform-set FirstSet hostname(config)# 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* **Example:** hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal FirstSet hostname(config)#	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。
ステップ 2	**crypto dynamic-map** *dynamic-map-name dynamic-seq-num* **set reverse-route** **Example:** hostname(config)# crypto dynamic-map dyn1 1 set reverse route hostname(config)#	（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。

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

この項では、クリプト マップ エントリを作成する方法について説明します。クリプト マップを作成すると、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、前の項ダイナミック クリプト マップの作成で作成したものです。

次の作業を実行します。

手順の詳細

	コマンド	目的
ステップ 1	**crypto map** *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name* **Example:** hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1 hostname(config)#	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。
ステップ 2	**crypto map** *map-name* **interface** *interface-name* **Example:** hostname(config)# crypto map mymap interface outside hostname(config)#	クリプト マップを外部インターフェイスに適用します。

セキュリティ アプライアンスのコンフィギュレーションの保存

上記の設定タスクを実行したら、この例に示すようにコンフィギュレーションの変更を必ず保存します。

コマンド	目的
write memory **Example:** hostname(config-if)# write memory Building configuration... Cryptochecksum: 0f80bf71 1623a231 63f27ccf 8700ca6d 11679 bytes copied in 3.390 secs (3893 bytes/sec) [OK] hostname(config-if)#	変更をコンフィギュレーションに保存します。

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)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption 3des
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)# lifetime 43200
```

```
hostname(config)# crypto ikev1 outside
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev1 transform set FirstSet esp-3des esp-md5-hmac
hostname(config)# tunnel-group testgroup type remote-access
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-ipsec)# ikev1 pre-shared-key 44kkaol59636jnfx
hostname(config)# crypto dynamic-map dyn1 1 set ikev1 transform-set FirstSet
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
hostname(config)# crypto map mymap interface outside
hostname(config)# write memory
```

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)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# group 2
hostname(config-ikev2-policy)# integrity sha
hostname(config-ikev2-policy)# lifetime 43200
hostname(config-ikev2-policy)# prf sha
hostname(config)# crypto ikev2 outside
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec ikev2 ipsec-proposal FirstSet
hostname(config-ipsec-proposal)# protocol esp encryption 3des aes
hostname(config)# tunnel-group testgroup type remote-access
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
hostname(config)# tunnel-group testgroup webvpn-attributes
hostname(config-webvpn)# authentication aaa certificate
hostname(config)# crypto dynamic-map dyn1 1 set ikev2 ipsec-proposal FirstSet
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
hostname(config)# crypto map mymap interface outside
hostname(config)# write memory
```

リモート アクセス VPN の機能履歴

表 73-1 に、この機能のリリース履歴を示します。

表 73-1　機能 1 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。