LAN-to-LAN IPsec VPN

LAN-to-LAN VPN は、地理的に異なる場所にあるネットワークを接続します。

シスコのピアや、関連するすべての標準に準拠したサードパーティのピアとの LAN-to-LAN IPsec 接続を作成できます。これらのピアは、IPv4 と IPv6 のアドレッシングを使用して、内部アドレスと外部アドレスの任意の組み合わせを持つことができます。

ASA では、ping 以外のローカル発信トラフィックは VPN トンネルを通過できません。

この章では、LAN-to-LAN VPN 接続の構築方法について説明します。

コンフィギュレーションのまとめ

ここでは、この章で説明するサンプルの LAN-to-LAN コンフィギュレーションの概要を説明します。後の項で、手順の詳細を説明します。

```
hostname(config)# interface ethernet0/0
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
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 aes
hostname(config-ikev1-policy)# hash sha
```

```
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)# lifetime 43200
hostname(config)# crypto ikev1 enable outside
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# # encryption aes
hostname(config-ikev2-policy)# group 2
hostname(config-ikev12-policy)# prf sha
hostname(config-ikev2-policy)# lifetime 43200
hostname(config)# crypto ikev2 enable outside
hostname(config)#  crypto ipsec ikev1 transform-set FirstSet esp-aes esp-sha-hmac
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)# protocol esp encryption aes
hostname(config-ipsec-proposal)# protocol esp integrity sha-1
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0
150.150.0.0 255.255.0.0
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key 44kkaol59636jnfx
hostname(config)# crypto map abcmap 1 match address l2l_list
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)# crypto map abcmap 1 set ikev1 transform-set FirstSet
hostname(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
hostname(config)# crypto map abcmap interface outside
hostname(config)# write memory
```

マルチコンテキストモードでのサイトツーサイトVPNの設定

マルチモードでサイトツーサイト VPN をサポートするには、次の手順を実行します。これらの手順を実行して、リソース割り当てがどのように分解されるのかを確認できます。

手順

ステップ 1 マルチモードの VPN を設定し、リソース クラスを設定し、許可されたリソースの一部として VPN ライセンスを選択します。「Configuring a Class for Resource Management」で、これらの設定手順を説明します。次に設定例を示します。

```
class ctx1
 limit-resource VPN Burst Other 100
 limit-resource VPN Other 1000
```

ステップ 2 コンテキストを設定し、VPNライセンスを許可する設定したクラスのメンバーにします。次に設定例を示します。

```
context context1
 member ctx1
 allocate-interface GigabitEthernet3/0.2
 allocate-interface GigabitEthernet3/1.2
 allocate-interface Management0/0
 config-url disk0:/sm_s2s_ik1_ip4_no_webvpn.txt
 join-failover-group 1
```

ステップ 3 接続プロファイル、ポリシー、クリプトマップなどを、サイトツーサイト VPN のシングル コンテキストの VPN 設定と同様に設定します。

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。

（注） ASA の外部インターフェイス アドレス（IPv4 と IPv6 の両方）は、プライベート側のアドレス空間と重複していてはなりません。

手順

ステップ 1 インターフェイス コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで、設定するインターフェイスのデフォルト名を指定して **interface** コマンドを入力します。次の例で、インターフェイスは ethernet0 です。

```
hostname(config)# interface ethernet0/0
hostname(config-if)#
```

ステップ 2 インターフェイスの IP アドレスとサブネット マスクを設定するには、**ip address** コマンドを入力します。次の例で、IP アドレスは 10.10.4.100、サブネット マスクは 255.255.0.0 です。

```
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)#
```

ステップ 3 インターフェイスに名前を付けるには、**nameif** コマンドを入力します。最大 48 文字です。この名前は、設定した後での変更はできません。次の例で、ethernet0 インターフェイスの名前は outside です。

```
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するには、**shutdown** コマンドの **no** バージョンを入力します。デフォルトでは、インターフェイスはディセーブルです。

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

ステップ 5 変更を保存するには、**write memory** コマンドを入力します。

```
hostname(config-if)# write memory
hostname(config-if)#
```

ステップ 6 同じ手順で、2 番目のインターフェイスを設定します。

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

ISAKMP は、2 台のホストで IPsec Security Association（SA; 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。これは、SA 属性のフォーマットに合意するための共通のフレームワークを提供します。これには、SA に関するピアとのネゴシエーション、および SA の変更または削除が含まれます。ISAKMP のネゴシエーションは 2 つのフェーズ（フェーズ 1 とフェーズ 2）に分かれています。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 では、データを保護するトンネルが作成されます。

IKE は、IPsec を使用するための SA の設定に ISAKMP を使用します。IKE は、ピアの認証に使用される暗号キーを作成します。

ASA は、レガシー Cisco VPN Client から接続するための IKEv1、および AnyConnect VPN クライアントの IKEv2 をサポートしています。

ISAKMP ネゴシエーションの条件を設定するには、IKE ポリシーを作成します。このポリシーには、次のものが含まれます。

- IKEv1 ピアに要求する認証タイプ。証明書を使用する RSA 署名または事前共有キー（PSK）です。
- 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。
- 暗号キー決定アルゴリズムの強度を決定するデフィーヘルマン グループ。ASA はこのアルゴリズムを使用して、暗号キーとハッシュ キーを導出します。
- IKEv2 では、別個の Pseudo-Random Function（PRF; 疑似乱数関数）をアルゴリズムとして使用して、IKEv2 トンネルの暗号化に必要なキー関連情報とハッシュ操作を取得していました。
- ASA が暗号キーを使用する時間の制限。この時間が経過すると暗号キーを置き換えます。

IKEv1 ポリシーを使用して、パラメータごとに 1 つの値を設定します。IKEv2 では、単一のポリシーに対して、複数の暗号化タイプと認証タイプ、および複数の整合性アルゴリズムを設定できます。ASA は、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを送信することなく、許可されるすべてのトランスフォームを伝送するために単一のプロポーザルを送信できます。

ここでは、IKEv1 および IKEv2 ポリシーを作成して、インターフェイスでイネーブルにする手順について説明します。

• IKEv1 接続の ISAKMP ポリシーの設定 （5 ページ）
• IKEv2 接続の ISAKMP ポリシーの設定 （6 ページ）

IKEv1 接続の ISAKMP ポリシーの設定

IKEv1 接続の ISAKMP ポリシーを設定するには、**crypto ikev1 policy** priority コマンドを使用して IKEv1 ポリシー コンフィギュレーション モードを開始します。ここでは IKEv1 のパラメータを設定できます。

手順

ステップ 1 IPSec IKEv1 ポリシー コンフィギュレーション モードを開始します。次に例を示します。

```
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)#
```

ステップ 2 認証方式を設定します。次の例では、事前共有キーを設定します。

```
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)#
```

ステップ 3 暗号方式を設定します。次に、 を設定する例を示します。

```
hostname(config-ikev1-policy)# encryption aes
hostname(config-ikev1-policy)#
```

ステップ 4 HMAC 方式を設定します。次の例では、SHA-1 に設定します。

```
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)#
```

ステップ 5 Diffie-Hellman グループを設定します。次に、グループ 14 を設定する例を示します。

```
hostname(config-ikev1-policy)# group 14
```

```
hostname(config-ikev1-policy)#
```

ステップ 6 暗号キーのライフタイムを設定します。次の例では、43,200 秒（12 時間）に設定します。

```
hostname(config-ikev1-policy)# lifetime 43200
hostname(config-ikev1-policy)#
```

ステップ 7 シングル コンテキスト モードまたはマルチ コンテキスト モードで、outside というインターフェイス上の IKEv1 をイネーブルにします。

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

ステップ 8 変更を保存するには、**write memory** コマンドを入力します。

```
hostname(config)# write memory
hostname(config)#
```

IKEv2 接続の ISAKMP ポリシーの設定

IKEv2 接続の ISAKMP ポリシーを設定するには、**crypto ikev2 policy** priority コマンドを使用して IKEv2 ポリシー コンフィギュレーション モードを開始します。ここでは IKEv2 のパラメータを設定できます。

手順

ステップ 1 IPsec IKEv2 ポリシー コンフィギュレーション モードを開始します。次に例を示します。

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)#
```

ステップ 2 暗号方式を設定します。次に、AES を設定する例を示します。

```
hostname(config-ikev2-policy)# encryption aes
hostname(config-ikev2-policy)#
```

ステップ 3 Diffie-Hellman グループを設定します。次に、グループ 15 を設定する例を示します。

```
hostname(config-ikev2-policy)# group 15
hostname(config-ikev2-policy)#
```

ステップ 4 アルゴリズムとして使用する疑似乱数関数（PRF）を設定し、IKEv2 トンネルの暗号化に必要なキー関連情報とハッシュ操作を取得します。次の例では、SHA-1（HMACバリアント）を設定します。

```
hostname(config-ikev12-policy)# prf sha
hostname(config-ikev2-policy)#
```

ステップ 5 暗号キーのライフタイムを設定します。次の例では、43,200 秒（12 時間）に設定します。

```
hostname(config-ikev2-policy)# lifetime seconds 43200
hostname(config-ikev2-policy)#
```

ステップ 6 outside というインターフェイス上の IKEv2 をイネーブルにします。

```
hostname(config)# crypto ikev2 enable outside
hostname(config)#
```

ステップ 7 変更を保存するには、**write memory** コマンドを入力します。

```
hostname(config)# write memory
hostname(config)#
```

IKEv2 の複数キー交換

IKEv2 は、Diffie-Hellman（DH）グループを使用して、イニシエータとレスポンダの間で共有秘密を確立します。IKEv2 は、量子コンピュータ攻撃から IPsec 通信を保護するための追加のキー交換をサポートしています。各交換には異なる DH グループを使用します。SA セットアップ用に計算される共有秘密は、各交換から取得するすべてのキーの組み合わせです。IKE SA は、IKE ピア間での複数のキー交換後に確立されます。

ASA は、複数キー交換に 7 つの新しいトランスフォームタイプを使用します。

- 追加のキー交換 1（IANA 値 6）
- 追加のキー交換 2（IANA 値 7）
- 追加のキー交換 3（IANA 値 8）
- 追加のキー交換 4（IANA 値 9）
- 追加のキー交換 5（IANA 値 10）
- 追加のキー交換 6（IANA 値 11）
- 追加のキー交換 7（IANA 値 12）

最大 7 つの複数キー交換を設定できます。設定する追加のキー交換ごとに DH グループを指定する必要があります。ASA は、以前の交換で得たキーを使用して中間キー交換を暗号化します。イニシエータピアとレスポンダピアが DH グループについて合意しない場合、ネゴシエーションは失敗し、**NO_PROPOSAL_CHOSEN** エラー通知がイニシエータに送信されます。トランスフォームを [なし（none）] に設定することもできます。[なし（none）] を選択すると、キー交換は行われません。

イニシエータについて、キー交換方式が追加のキー交換 *n* に対して **[なし（none）]** に設定されている場合：

- レスポンダは、追加のキー交換 *n* のキー交換方式として **[なし（None）]** を選択できます。
- 追加のキー交換はオプションです。

プロポーザルのネゴシエーションを成功させるには、イニシエータのプロポーザルのすべてのトランスフォームがレスポンダのトランスフォームと一致する必要があります。

次に、イニシエータの例を示します。

```
crypto ikev2 policy 1
encryption aes
integrity sha256
group 14
prf sha256
lifetime seconds 120
additional-key-exchange 5
key-exchange-method none
```

レスポンダには、プロポーザルを一致させるために追加のキー交換 5 が必要です。

ピアが追加のキー交換をサポートしていない場合は、次のいずれかが発生します。

- イニシエータにレスポンダのプロポーザルと一致する別の IKEv2 プロポーザルがある場合、IKEv2 SA が確立されます。
- ピアは IKE_SA_INIT 交換メッセージ内の追加のキー交換のトランスフォームタイプを不明なトランスフォームタイプとして扱い、プロポーザルをスキップします。ネゴシエーションは失敗し、**NO_PROPOSAL_CHOSEN** エラー通知がイニシエータに送信されます。

この機能の詳細については、RFC 9242 を参照してください。

IKEv2 複数キー交換の注意事項と制限事項

- 最大 7 つの複数キー交換を持つことができます。
- 後続のキー交換で同じ DH グループを使用することはできません。

この機能について、ASA は次をサポートしません。

- IKEv1
- 従来のキー交換とポスト量子アルゴリズムベースのキー交換の組み合わせ。
- リモート アクセス VPN サイト間 VPN のみが IKEv2 複数キー交換をサポートします。
- クラスタ

IKEv2 の複数キー交換の設定

この設定はオプションです。量子コンピュータ攻撃から IPsec 通信を保護したい場合は、設定を実行できます。

始める前に

- 注意事項と制限事項を確認します。詳細については、IKEv2 複数キー交換の注意事項と制限事項 （8 ページ）を参照してください。
- IKEv2 ポリシーの暗号化アルゴリズム、ハッシュアルゴリズム、認証方式、および SA ライフタイムを設定します。詳細については、IKEv1 ポリシーと IKEv2 ポリシーの設定を参照してください。

手順

ステップ 1 IKEv2 ポリシーを作成します。

crypto ikev2 policy *policy_index*

プロンプトには、IKEv2 ポリシー設定モードが表示されます。

例：

```
hostname(config)# crypto ikev2 policy 1
```

ステップ 2 IKEv2 ポリシーの追加のキー交換トランスフォームを設定します。

additional-key-exchange *<1-7>*

プロンプトには、IKEv2 ポリシーの追加のキー交換設定モードが表示されます。1 つのポリシーに最大 7 つのキー交換トランスフォームを設定できます。

例：

```
hostname(config-ikev2-policy)# additional-key-exchange 1
```

ステップ 3 追加のキー交換トランスフォームに 1 つ以上の DH グループを定義して、キー交換方式を設定します。

key-exchange-method *<DH_group>*

DH グループを 14、15、16、19、20、21、または 31 と指定します。トランスフォームを [なし（none）] に設定することもできます。[なし（none）] を選択すると、キー交換は行われません。

例：

```
hostname(config-ikev2-policy-ake)# key-exchange-method 21 31
```

ステップ 4 IKEv2 ポリシーに複数のキー交換を設定するには、手順 2 と 3 を繰り返します。

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# additional-key-exchange 1
hostname(config-ikev2-policy-ake)# key-exchange-method 21 31
hostname(config-ikev2-policy)# additional-key-exchange 2
```

```
hostname(config-ikev2-policy-ake)# key-exchange-method 20 21
hostname(config-ikev2-policy)# additional-key-exchange 3
hostname(config-ikev2-policy-ake)# key-exchange-method 19 20 none
...
```

次のタスク

設定を確認します。詳細については、IKEv2 複数キー交換設定の確認 （10 ページ）を参照してください。

IKEv2 複数キー交換設定の確認

IKEv2 複数キー交換の設定を表示または確認するには、次の show コマンドを使用します。

- **show running-config crypto ikev2**

```
crypto ikev2 policy 1
encryption aes
integrity sha256
group 14
prf sha256
lifetime seconds 120
additional-key-exchange 1
key-exchange-method 21 31
additional-key-exchange 2
key-exchange-method 20 21
...
```

- **show crypto ikev2 sa detail**

```
IKEv2 SAs:
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local Remote fvrf/ivrf Status Role
41567725 192.168.15.1/500 192.168.15.2/500 READY INITIATOR
Encr: AES-CBC, keysize: 128, Hash: SHA96, DH Grp:14, Auth sign: PSK, Auth verify:
PSK
Additional Key Exchange Group: AKE1: 31 AKE2: 21 AKE3: 20 AKE4: 19 AKE5: 16 AKE6:
15 AKE7: 14
Life/Active Time: 120/5 sec
Session-id: 4
Status Description: Negotiation done
Local spi: 6BB6B7BFA0BAADF4 Remote spi: 7030C7xxx xxxxxxE9DBDE77EB
Local id: 192.168.15.1
Remote id: 192.168.15.2
Local req mess id: 9 Remote req mess id: 0
Local next mess id: 9 Remote next mess id: 0
Local req queued: 9 Remote req queued: 0
Local window: 1 Remote window: 1
DPD configured for 10 seconds, retry 2
NAT-T is not detected
IKEv2 Fragmentation Configured MTU: 576 bytes, Overhead: 28 bytes, Effective MTU:
548 bytes
Parent SA Extended Status:
Delete in progress: FALSE
Marked for delete: FALSE
Child sa: local selector 20.0.0.0/0 - 20.0.0.255/65535
remote selector 30.0.0.0/0 - 30.0.0.255/65535
ESP spi in/out: 0x4a7d5da2/0x56a28fa8
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

IKEv1 トランスフォーム セットの作成

IKEv1 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。

次の表に、有効な暗号化方式と認証方式を示します。

表 *1*：有効な暗号化方式と認証方式

有効な暗号化方式	有効な認証方式
	esp-sha-hmac（デフォルト）
esp-aes（128 ビット暗号化）（デフォルト）	
esp-aes-192	
esp-aes-256	
esp-null	

パブリック インターネットなどの非信頼ネットワークを介して接続された 2 つの ASA 間で IPsec を実装する通常の方法は、トンネル モードです。トンネル モードはデフォルトであり、設定は必要ありません。

トランスフォーム セットを設定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで次のサイト間タスクを実行します。

手順

ステップ 1 グローバル コンフィギュレーション モードで、**crypto ipsec ikev1 transform-set** コマンドを入力します。次の例では、名前が FirstSet で、暗号化と認証に esp-aes と esp-sha-hmac を使用するトランスフォームセットを設定しています。構文は次のようになります。

esp-sha-hmac（デフォルト）

crypto ipsec ikev1 transform-set *transform-set-nameencryption-method authentication-method*

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

```
hostname(config)#
```

ステップ 2 変更を保存します。

```
hostname(config)# write memory
hostname(config)#
```

IKEv2 プロポーザルの作成

IKEv2 では、単一のポリシーに対して、複数の暗号化タイプと認証タイプ、および複数の整合性アルゴリズムを設定できます。ASA は、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを送信することなく、許可されるすべてのトランスフォームを伝送するために単一のプロポーザルを送信できます。

次の表に、有効な IKEv2 暗号化方式と認証方式を示します。

表 *2:* 有効な *IKEv2* 暗号化方式と整合性方式

有効な暗号化方式	有効な整合性方式
	sha（デフォルト）
aes （デフォルト）：128 ビット キーを使用した AES。	
aes-192	
aes-256	

IKEv2 プロポーザルを設定するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで次のタスクを実行します。

手順

ステップ 1 グローバル コンフィギュレーション モードで **crypto ipsec ikev2 ipsec-proposal** コマンドを使用して、プロポーザルの複数の暗号化および整合性タイプを指定できる IPSec プロポーザル コンフィギュレーション モードを開始します。この例では、secure がプロポーザルの名前です。

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

ステップ 2 次に、プロトコルおよび暗号化タイプを入力します。サポートされている唯一のプロトコルは ESP です。次に例を示します。

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

hostname(config-ipsec-proposal)#
```

ステップ 3 整合性タイプを入力します。次に例を示します。

```
hostname(config-ipsec-proposal)# protocol esp integrity sha-1
hostname(config-ipsec-proposal)#
```

ステップ 4 変更を保存します。

ACL の設定

ASA は、アクセス コントロール リストを使用してネットワーク アクセスをコントロールします。デフォルトでは、適応型セキュリティ アプライアンスはすべてのトラフィックを拒否します。トラフィックを許可する ACL を設定する必要があります。詳細については、一般的操作用コンフィギュレーション ガイドの「Information About Access Control Lists」を参照してください。

この LAN-to-LAN VPN 制御接続で設定する ACL は、送信元 IP アドレスと変換された宛先 IP アドレス、および任意指定のポートに基づいています。接続の両側に、互いにミラーリングする ACL を設定します。

VPN トラフィック用の ACL は、変換アドレスを使用します。

（注） VPN フィルタを使用した ACL の設定方法の詳細については、リモート アクセスの VLAN の指定またはグループ ポリシーへの統合アクセス コントロール ルールの適用を参照してください。

手順

ステップ 1 **access-list extended** コマンドを入力します。

access-list *listname* **extended permit ip** *source-ipaddress source-netmask destination-ipaddress destination-netmask*

次の例では、192.168.0.0 のネットワーク内にある IP アドレスから 150.150.0.0 のネットワークにトラフィックを送信する、l2l_list という名前の ACL を設定します。

```
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0
150.150.0.0 255.255.0.0
hostname(config)#
```

ステップ 2 ACL をミラーリングする接続のもう一方の側の ASA に、ACL を設定します。

1つのクリプトマップのACLで定義されたサブネット、または同じクリプトマップに接続された2つの異なる暗号ACLで定義されたサブネットは重複できません。

次の例では、該当ピアのプロンプトはhostname2です。

```
hostname2(config)# access-list l2l_list extended permit ip 150.150.0.0 255.255.0.0
192.168.0.0 255.255.0.0
hostname(config)#
```

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を格納したレコードのセットです。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IPsec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IPsec 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。

IKEバージョン1および2の主な相違点は、使用できる認証方式にあります。IKEv1では、両方のVPNエンドで1つのタイプの認証のみが許可されます（つまり、事前共有キーまたは証明書）。しかし、IKEv2では、別のローカルおよびリモート認証CLIを使用して非対称認証方式を設定できます（つまり、送信元に対しては事前共有キー認証を設定し、応答側に対しては証明書認証を設定できます）。したがって、IKEv2を使用すると、両方の側がそれぞれ異なるクレデンシャルで認証する非対称認証を使用できます（事前共有キーまたは証明書）。

また、環境に合った新しいトンネル グループを1つ以上作成することもできます。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。

基本的なLAN-to-LAN接続を確立するには、次のように2つの属性をトンネル グループに設定する必要があります。

- 接続タイプをIPsec LAN-to-LANに設定します。
- IPアドレスの認証方式（つまり、IKEv1とIKEv2用の事前共有キー）を設定します。

手順

ステップ1 接続タイプをIPsec LAN-to-LANに設定するには、**tunnel-group**コマンドを入力します。

構文は、**tunnel-group** *name***type** *type*です。ここで、nameはトンネル グループに割り当てる名前であり、typeはトンネルのタイプです。CLIで入力するトンネル タイプは次のとおりです。

- **remote-access** （IPsec、SSL、およびクライアントレス SSL リモート アクセス）
- **ipsec-l2l** （IPsec LAN-to-LAN）

次の例では、トンネル グループの名前は、LAN-to-LAN ピアの IP アドレスである 10.10.4.108 です。

```
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)#
```

（注）
IP アドレス以外の名前が付いている LAN-to-LAN トンネル グループは、トンネル認証方式がデジタル証明書である、またはピアが Aggressive モードを使用するように設定されている（あるいはその両方の）場合に限り使用できます。

ステップ 2 事前共有キーを使用するように認証方式を設定するには、ipsec 属性モードに入り、**ikev1pre-shared-key** コマンドを入力して事前共有キーを作成します。この LAN-to-LAN 接続の両方の ASA で、同じ事前共有キーを使用する必要があります。

キーは、1 ～ 128 文字の英数字文字列です。

次の例で、IKEv1 事前共有キーは 44kkaol59636jnfx です。

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1-pre-shared-key 44kkaol59636jnfx
```

ステップ 3 変更を保存します。

```
hostname(config)# write memory
hostname(config)#
```

トンネルが稼働中であることを確認するには、**show vpn-sessiondb summary**、**show vpn-sessiondb detail l2l**、または **show crypto ipsec sa** コマンドを使用します。

クリプト マップの作成とインターフェイスへの適用

クリプトマップエントリは、IPsec セキュリティ アソシエーションの次のような各種要素をまとめたものです。

- IPsec で保護する必要のあるトラフィック（ACL で定義）
- IPsec で保護されたトラフィックの送信先（ピアで指定）
- トラフィックに適用される IPsec セキュリティ（トランスフォーム セットで指定）
- IPsec トラフィックのローカル アドレス（インターフェイスにクリプト マップを適用して指定）

IPsec が成功するためには、両方のピアに互換性のあるコンフィギュレーションを持つクリプト マップ エントリが存在する必要があります。2 つのクリプト マップ エントリが互換性を持つためには、両者が少なくとも次の基準を満たす必要があります。

- クリプトマップエントリに、互換性を持つ暗号ACL（たとえば、ミラーイメージACL）が含まれている。応答するピアがダイナミック クリプト マップを使用している場合は、ASA の暗号 ACL のエントリがピアの暗号 ACL によって「許可」されている必要があります。
- 各クリプト マップ エントリが他のピアを識別する（応答するピアがダイナミック クリプト マップを使用していない場合）。
- クリプトマップエントリに、共通のトランスフォームセットが少なくとも1つ存在する。

所定のインターフェイスに対して複数のクリプト マップ エントリを作成する場合は、各エントリのシーケンス番号（seq-num）を使用して、エントリにランクを付けます。seq-num が小さいほど、プライオリティが高くなります。クリプト マップ セットを持つインターフェイスでは、ASA はまずトラフィックをプライオリティの高いマップエントリと照合して評価します。

リバースルートインジェクション（RRI）がクリプトマップに適用されている場合、そのマップはASA上のインターフェイスごとに一意である必要があります。つまり、同じクリプトマップは複数のインターフェイスに適用できないということです。複数のクリプトマップを複数のインターフェイスに適用すると、ルートが正しくクリーンアップされないことがあります。複数のインターフェイスに 1 つのクリプト マップが必要な場合は、一意に定義したマップを各ルートで使用する必要があります。

次の条件のいずれかに当てはまる場合は、所定のインターフェイスに対して複数のクリプト マップ エントリを作成します。

- 複数のピアで異なるデータ フローを処理する場合。
- 異なるタイプのトラフィック（同一または個別のピアへの）に異なる IPsec セキュリティを適用する場合。たとえば、あるサブネットセット間のトラフィックは認証し、別のサブネットセット間のトラフィックは認証および暗号化するような場合です。この場合は、異なるタイプのトラフィックを 2 つの個別の ACL で定義し、各 暗号 ACL に対して個別にクリプト マップ エントリを作成します。

複数のインターフェイスへの暗号マップの適用

デュアル ISP の場合、ASA の外部インターフェイスとバックアップ インターフェイスに暗号マップを適用できます。この設定を使用する場合、origin-only オプションは使用できません。この冗長性が必要な場合は、仮想トンネルインターフェイス（VTI）を使用する必要があります。

複数のインターフェイスで暗号マップを使用する場合：

- ルーティングプロトコルまたはルートトラッキングが必要です。
- リモート側もルーティングプロトコルを使用していることを確認してください。

- ASAは優先度の低いルートを持つインターフェイスでリモートサイトからの接続を許可するため、同じ暗号マップに対して複数のインターフェイスを慎重に選択する必要があります。

クリプト マップを作成してグローバル コンフィギュレーション モードで外部インターフェイスに適用するには、シングル コンテキスト モードまたはマルチ コンテキスト モードで次の手順を実行します。

手順

ステップ 1 ACL をクリプト マップ エントリに割り当てるには、**crypto map match address** コマンドを入力します。

構文は、**crypto map** map-name seq-num **match address** aclname です。次の例では、マップ名は abcmap、シーケンス番号は 1、ACL 名は **l2l_list** です。

```
hostname(config)# crypto map abcmap 1 match address l2l_list
hostname(config)#
```

ステップ 2 IPsec 接続用のピアを指定するには、**crypto map set peer** コマンドを入力します。

構文は、**crypto map** map-name seq-num **set peer** {ip_address1 | hostname1}[... ip_address10 | hostname10] です。次の例では、ピア名は 10.10.4.108 です。

```
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)#
```

ステップ 3 クリプトマップ エントリに IKEv1 トランスフォーム セットを指定するには、**crypto map ikev1 set transform-set** コマンドを入力します。

構文は、**crypto map** map-name seq-num **ikev1 set transform-set** transform-set-name です。 次の例では、トランスフォームセット名は FirstSet です。

```
hostname(config)# crypto map abcmap 1 set transform-set FirstSet
hostname(config)#
```

ステップ 4 クリプト マップ エントリに IKEv2 プロポーザルを指定するには、crypto map ikev2 set ipsec-proposal コマンドを入力します。

構文は、**crypto map** map-name seq-num set **ikev2 ipsec-proposal proposal-name** です。 次の例では、プロポーザル名は secure です。

crypto map コマンドでは、1 つのマップ インデックスに複数の IPsec プロポーザルを指定できます。この場合、複数のプロポーザルがネゴシエーションの一部として IKEv2 ピアに送信され、プロポーザルの順序はクリプト マップ エントリの順序付け時に管理者が決定します。

（注）
連結モード（AES-GCM/GMAC）および通常モード（その他すべて）のアルゴリズムが IPsec プロポーザルにある場合、ピアに単一のプロポーザルを送信できません。この場合、2 つのプ

ロポーザルが必要となります（連結モードのアルゴリズムに1つ、通常モードのアルゴリズムに 1 つ）。

```
hostname(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
hostname(config)#
```

クリプト マップのインターフェイスへの適用

クリプト マップ セットは、IPsec トラフィックが通過する各インターフェイスに適用する必要があります。ASA は、すべてのインターフェイスで IPsec をサポートします。クリプトマップセットをインターフェイスに適用すると、ASA はすべてのインターフェイス トラフィックをクリプト マップ セットと照合して評価し、接続時やセキュリティ アソシエーションのネゴシエート時に、指定されたポリシーを使用します。

また、クリプト マップをインターフェイスにバインドすると、セキュリティ アソシエーション データベースやセキュリティ ポリシー データベースなどのランタイム データ構造も初期化されます。クリプトマップを後から変更すると、ASA は自動的にその変更を実行コンフィギュレーションに適用します。既存の接続はすべてドロップされ、新しいクリプトマップの適用後に再確立されます。

設定済みのクリプトマップを外部インターフェイスに適用するには、次の手順を実行します。

手順

ステップ 1 **crypto map interface** コマンドを入力します。構文は、**crypto map** map-name **interface** interface-name です。

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

ステップ 2 変更を保存します。

```
hostname(config)# write memory
hostname(config)#
```

ダイナミックサイト間 VPN の概要

ダイナミックサイト間 VPN では、ループバック インターフェイスは VPN トンネルの送信元と接続先として使用されます。これらのインターフェイスを使用すると、ピアを更新せずにセキュリティゲートウェイ間でサイト間ピアを移動できます。ループバックアドレスがルーティングプロトコル経由で伝達されると、ASA は、ピアの構成を変更することなく、リモートピア

から新しいセキュリティ ゲートウェイ クラスターにトラフィックをシームレスにリダイレクトします。

（注） この機能は、評価ライセンスでは機能しません。

ダイナミックサイト間 VPN でループバック インターフェイスを使用するメリット

- 冗長性：VPN 接続は、物理リンクまたはインターフェイスの障害が発生しても持続します。これは、ループバック インターフェイスが複数の物理インターフェイスを介して到達可能なままであるためです。クラスターでは、ループバック インターフェイスを備えたノードに障害が発生すると、インターフェイスとセッションは代替ノードに移行します。
- ダイナミック ループバック アドレスの再割り当て：VPN 接続は、ループバックアドレスを別のセキュリティ ゲートウェイ クラスターに再割り当てしている間、リモートピアへの変更を必要とせずに維持されます。
- ダイナミックパスの選択：VPN接続は、ルーティングプロトコルがサイト間のベストパスを動的に選択するときに最適化され、パフォーマンスと信頼性の両方が向上します。

ループバック インターフェイスでダイナミック VPN を使用するための前提条件

一般的な前提条件

この機能は、次に対してのみサポートされています。

- Cisco Secure Firewall 4200 シリーズ バージョン 9.24.1
- レイヤ 2 クラスタリング
- ダイナミック暗号マップに紐づけられたスタティック暗号マップ。

ライセンスの前提条件

この機能には、次のライセンスが必要です。

- 強力な暗号化を備えた基本ライセンス。
- 分散モード VPN 向けキャリアライセンス。

ループバックインターフェイスを使用したダイナミックサイト間VPNの設定

始める前に

必ずループバック インターフェイスでダイナミック VPN を使用するための前提条件（19 ページ） を確認してください。

手順

ステップ 1 **interface** コマンドを使用して、外部インターフェイスを設定します。

a) **nameif** コマンドを使用して、ループバック インターフェイスの名前を設定します。
b) **security-level** コマンドを使用して、セキュリティレベルを設定します。
c) **ip address** コマンドを使用して、インターフェイスの IP アドレスを設定します。

例：

```
hostname(config)# interface ethernet0/0
hostname(config-if)#nameif outside
hostname(config-if)#security-level 0
hostname(config-if)#ip address 192.0.2.17 255.255.255.0
```

ステップ 2 **interface** コマンドを使用して、レイヤ 2 ループバック インターフェイスを設定します。

a) **description** コマンドを使用して、説明を設定します。
b) **nameif** コマンドを使用して、ループバック インターフェイスの名前を設定します。
c) **ip address** コマンドを使用して、ループバック インターフェイスの IP アドレスを設定します。

例：

```
hostname(config)# interface Loopback2
hostname(config-if)#description Loopback to terminate Group 2
hostname(config-if)#nameif LB2
hostname(config-if)#ip address 209.165.201.1 255.255.255.252
```

ステップ 3 **crypto ipsec ikev2 ipsec-proposal** *proposal tag* コマンドを使用して、IKEv2 IPsec プロポーザルを設定します。

a) **description** コマンドを使用して、説明を設定します。
b) **protocol esp encryption** コマンドを使用して、暗号化プロトコルを設定します。
c) **protocol esp integrity** コマンドを使用して、暗号化と完全性プロトコルを設定します。

例：

```
hostname(config)#crypto ipsec ikev2 ipsec-proposal ESP-AES-SHA
hostname(config-ipsec-proposal)#protocol esp encryption aes
hostname(config-ipsec-proposal)#protocol esp integrity sha-256
```

ステップ 4 **crypto ikev2 policy** *policy_index* コマンドを使用して、IKEv2 ポリシーを設定します。

a) **protocol esp encryption** コマンドを使用して、暗号化プロトコルを設定します。

b) **protocol esp integrity** コマンドを使用して、暗号化と完全性プロトコルを設定します。
c) **group** コマンドを使用して、Diffie-Hellman グループを設定します。
d) アルゴリズムとして使用する疑似乱数関数（PRF）を設定し、**prf** コマンドを使用して、IKEv2 トンネル暗号化に必要なキー関連情報とハッシュ操作を取得します。
e) **lifetime** コマンドを使用して、暗号化キーのライフタイムを設定します。

例：

```
hostname(config)#crypto ikev2 policy 1
hostname(config-ikev2-policy)#protocol esp encryption aes-256
hostname(config-ikev2-policy)#protocol esp integrity sha
hostname(config-ikev2-policy)#group 5
hostname(config-ikev2-policy)#prf sha
hostname(config-ikev2-policy)#lifetime seconds 86400
```

ステップ 5 ダイナミック暗号マップの設定：

a) **crypto dynamic-map** *dynamic-map-name dynamic-sequence-num* **set ikev2 ipsec-proposal** *transform-set-name1* コマンドを使用して、ダイナミック暗号マップを設定し、そのマップに対して IKEv2 トランスフォームセットを指定します。
b) **crypto dynamic-map** *dynamic-map-name dynamic-sequence-num* **set reverse-route** コマンドを使用して、この暗号マップエントリに基づいて任意の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。

例：

```
hostname(config)#crypto dynamic-map dmap 1 set ikev2 ipsec-proposal ESP-AES-SHA
hostname(config)#crypto dynamic-map dmap 1 set reverse-route
```

ステップ 6 スタティック暗号マップの設定：

a) **crypto map** *map-name sequence-num* **ipsec-isakmp dynamic** *dynamic-map-name* コマンドを使用して、スタティック暗号マップセットにダイナミック暗号マップセットを追加します。
b) **crypto map** *map-name* **interface** *loopback_interface* コマンドを使用して、ループバック インターフェイスにスタティック暗号マップを適用します。

例：

```
hostname(config)#crypto map vpn 1 ipsec-isakmp dynamic dmap
hostname(config)#crypto map vpn interface LB2
```

ステップ 7 デフォルトの LAN 間トンネルグループの設定：

a) **tunnel-group DefaultL2LGroup ipsec-attributes** コマンドを使用して、デフォルトの LAN 間トンネルグループの IPsec IKEv2 属性を設定します。
b) **ikev2 remote-authentication pre-shared-key** *key* コマンドを使用して、リモートピアを認証するための事前共有キー（PSK）を設定します。
c) **ikev2 local-authentication pre-shared-key** *key* コマンドを使用して、ローカルデバイスを認証するための事前共有キー（PSK）を設定します。

例：

```
hostname(config)#tunnel-group DefaultL2LGroup ipsec-attributes
hostname(config-tunnel-ipsec)#ikev2 remote-authentication pre-shared-key ****
hostname(config-tunnel-ipsec)#ikev2 local-authentication pre-shared-key ****
```

ステップ 8 **crypto ikev2 enable** *loopback_interface* コマンドを使用して、ループバック インターフェイスで IKEv2 を有効にします。

例：

```
hostname(config)#crypto ikev2 enable LB2
```

ステップ 9 ループバック インターフェイスをアドバタイズするようにルーティングプロトコルを設定します。

例：

OSPF の設定例：

```
hostname(config)#router ospf 1
hostname(config-router)#network 203.0.113.0 255.255.255.0 area 0
hostname(config-router)#network 209.165.201.1 255.255.255.252 area 0
hostname(config-router)#log-adj-changes
hostname(config-router)#redistribute connected

hostname(config)#interface outside
hostname(config-interface)#ospf cost 1
hostname(config-interface)#ospf message-digest-key 1 md5 *****
hostname(config-interface)#ospf authentication message-digest
```

ダイナミックサイト間 VPN 設定の検証

次の show コマンドを使用して、ダイナミックサイト間 VPN （ループバック インターフェイスを使用）の設定を検証します：

show vpn-sessiondb det l2l

```
asa-node2/data-node# show vpn-sessiondb det l2l

Session Type: LAN-to-LAN Detailed

Connection   : DefaultL2LGroup
Index        : 399                    IP Addr      : <Peer-IP>
Protocol     : IKEv2 IPsec
Encryption   : IKEv2: (1)AES128  IPsec: (1)AES128
Hashing      : IKEv2: (1)SHA256  IPsec: (1)SHA256
Bytes Tx     : 58680                  Bytes Rx     : 86152
Login Time   : 09:59:41 EDT Tue Apr 8 2025
Duration     : 0h:01m:21s
Session State: Cluster Owner (backup is asa-node1)

IKEv2 Tunnels: 1
IPsec Tunnels: 1

IKEv2:
  Tunnel ID    : 399.1
  UDP Src Port : 500                    UDP Dst Port : 500
  Rem Auth Mode: preSharedKeys
  Loc Auth Mode: preSharedKeys
  Encryption   : AES128                 Hashing      : SHA256
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86319 Seconds
  PRF          : SHA256                 D/H Group    : 14
  Filter Name  : trace
```

```
IPsec:
  Tunnel ID    : 399.2
  Local Addr   : 209.165.201.1 255.255.255.0/0/0
  Remote Addr  : 192.0.2.20 255.255.255.0/0/0
  Encryption   : AES128                Hashing      : SHA256
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 28715 Seconds
  Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
  Bytes Tx     : 58680                 Bytes Rx     : 86152
  Pkts Tx      : 978
```

show crypto ikev2 sa

```
asa-node2/data-node# show crypto ikev2 sa
IKEv2 SAs:
Session-id:399, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local                        Remote
fvrf/ivrf     Status         Role
   724781 209.165.201.1/500           192.0.2.20/500
Global/Global      READY    RESPONDER

   ...
```

show crypto ipsec sa

```
asa-node2/data-node# show crypto ipsec sa

interface: LB2
    Crypto map tag: dyn-loop1, seq num: 65535, local addr: 209.165.201.1

   ...
```

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。