CHAPTER 36

LAN-to-LAN IPsec VPN の設定

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。

（注） ASA は、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 接続をサポートしています。

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。内容は次のとおりです。

コンフィギュレーションのまとめ

ここでは、この章で作成するサンプルの 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
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)# no shutdown
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)# isakmp policy 1 hash sha
hostname(config)# isakmp policy 1 group 2
hostname(config)# isakmp policy 1 lifetime 43200
hostname(config)# isakmp enable outside
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
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-ipsec)# 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 transform-set FirstSet
hostname(config)# crypto map abcmap interface outside
```

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

インターフェイスの設定

セキュリティ アプライアンスには、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、セキュリティ アプライアンスの 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。

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
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** 形式を入力します。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

Internet Security Association and Key Management Protocol は IKE とも呼ばれ、2 台のホストで 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 つの部分に分割されます。

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、次を含む ISAKMP ポリシーを作成します。

- 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。
- Hashed Message Authentication Code 方式。送信者の身元を保証し、搬送中にメッセージが変更されていないことを保証します。
- 暗号キー判別アルゴリズムを強化する Diffie-Hellman グループ。このアルゴリズムを使用して、セキュリティ アプライアンスは暗号キーとハッシュ キーを導出します。
- セキュリティ アプライアンス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。

IKE ポリシーのキーワードとその値の詳細については、このマニュアルの「IPsec と ISAKMP の設定」の章の 表 27-1（P.27-3）を参照してください。

ISAKMP ポリシーを設定するには、グローバル コンフィギュレーション モードで、各種の引数を指定して **isakmp policy** コマンドを使用します。ISAKMP ポリシー コマンドの構文は次のとおりです。

isakmp policy *priority* **attribute_name** [**attribute_value** | *integer*]

次の手順を実行し、ガイドとして次の例で示すコマンド構文を使用します。

ステップ 1　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。このステップおよび後続のすべてのステップで、プライオリティは 1 です。

```
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)#
```

ステップ 2　暗号方式を設定します。次の例では、3DES に設定します。

```
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)#
```

ステップ 3　HMAC 方式を設定します。次の例では、SHA-1 に設定します。

```
hostname(config)# isakmp policy 1 hash sha
hostname(config)#
```

ステップ 4　Diffie-Hellman グループを設定します。次の例では、グループ 2 に設定します。

```
hostname(config)# isakmp policy 1 group 2
hostname(config)#
```

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)# isakmp 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。

```
hostname(config)# isakmp 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)#
```

トランスフォーム セットの作成

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。セキュリティ アプライアンス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。

表 36-1 に、有効な暗号化方式と認証方式を示します。

表 36-1　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-des	esp-md5-hmac
esp-3des（デフォルト）	esp-sha-hmac（デフォルト）
esp-aes（128 ビット暗号化）	
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 つのセキュリティ アプライアンス間で 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、次の手順を実行します。

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 transform-set** コマンドを入力します。次の例では、名前が FirstSet で、暗号化と認証にそれぞれ esp-3des と esp-md5-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。

crypto ipsec transform-set *transform-set-name* ***encryption-method authentication-method***

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

ステップ 2　変更を保存します。

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

ACL の設定

セキュリティ アプライアンスは、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、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。ACL の詳細については、第 16 章「アクセス リストでのトラフィックの識別」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。

（注）　VPN トラフィック用の ACL は、変換アドレスを使用します。詳細については、「NAT 使用時にアクセス リストで使用する IP アドレス」（P.16-3）を参照してください。

ACL を設定するには、次の手順を実行します。

ステップ 1　**access-list extended** コマンドを入力します。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。構文は、**access-list** *listname* **extended permit ip** *source-ipaddress source-netmask destination-ipaddress destination-netmask* です。

```
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　接続のもう一方の側のセキュリティ アプライアンスに、上記の ACL をミラーリングする ACL を設定します。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。セキュリティ アプライアンスは、トンネル グループを内部的に保存します。

セキュリティ アプライアンス 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 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。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、セキュリティ アプライアンスは、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。
- 認証方式を設定します。次の例では、事前共有キーを使用します。

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。

- **ipsec-ra**（IPsec 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)#
```

ステップ 2　認証方式を事前共有キーに設定するには、ipsec 属性モードに入り、**pre-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 接続の両方のセキュリティ アプライアンスで、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、事前共有キーは 44kkaol59636jnfx です。

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

ステップ 3　変更を保存します。

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

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（アクセス リストで定義）
- 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、互換性を持つ暗号アクセス リスト（たとえば、ミラー イメージ アクセス リスト）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、セキュリティ アプライアンスのクリプト アクセス リストのエントリがピアのクリプト アクセス リストによって「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、セキュリティ アプライアンス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。

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 つの個別のアクセス リストで定義し、各暗号アクセス リストに対して個別にクリプト マップ エントリを作成します。

クリプト マップを作成して外部インターフェイスに割り当てるには、グローバル コンフィギュレーション モードで **crypto map** コマンドをいくつか入力します。これらのコマンドではさまざまな引数を使用しますが、構文はすべて **crypto map** *map-name-seq-num* で始まります。次の例では、マップ名は abcmap で、シーケンス番号は 1 です。

これらのコマンドは、グローバル コンフィギュレーション モードで入力します。

ステップ 1　アクセス リストをクリプト 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、アクセス リスト名は **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 エントリにトランスフォーム セットを指定するには、**crypto map set transform-set** コマンドを入力します。

構文は、**crypto map** *map-name seq-num* **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)#
```

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。セキュリティ アプライアンスは、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、セキュリティ アプライアンス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、セキュリティ アプライアンス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。

ステップ 1　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、**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)#
```