CHAPTER 32

リモート アクセス IPSec VPN の設定

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、単一ユーザを中央サイトに接続することができます。

この章では、リモート アクセス 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」（P.32-1）
- 「インターフェイスの設定」（P.32-2）
- 「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.32-3）
- 「アドレス プールの設定」（P.32-4）
- 「ユーザの追加」（P.32-4）
- 「トランスフォーム セットの作成」（P.32-4）
- 「トンネル グループの定義」（P.32-5）
- 「ダイナミック クリプト マップの作成」（P.32-6）
- 「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」（P.32-7）

コンフィギュレーションのまとめ

この章では、次のコンフィギュレーションを使用して、リモート アクセス接続の設定方法について説明します。後の項で、手順の詳細を説明します。

```
hostname(config)# interface ethernet0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)# nameif outside
hostname(config)# 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)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec transform-set FirstSet esp-3des esp-md5-hmac
hostname(config)# tunnel-group testgroup type ipsec-ra
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-ipsec)# pre-shared-key 44kkaol59636jnfx
hostname(config)# crypto dynamic-map dyn1 1 set 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
```

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 10.10.4.200 255.255.0.0
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（ISAKMP）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。
- 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。
- 暗号キーのサイズを設定する Diffie-Hellman グループ。
- 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** コマンドを入力します。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　変更内容を保存するには、**write memory** コマンドを入力します。

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

アドレス プールの設定

セキュリティ アプライアンスでは、ユーザに IP アドレスを割り当てる方式が必要です。一般的な方式では、アドレス プールを使用します。また、DHCP サーバや AAA サーバでアドレスを割り当てる場合もあります。次の例では、アドレス プールを使用します。

ステップ 1　アドレス プールを設定するには、**ip local pool** コマンドを使用します。構文は次のとおりです。**ip local pool** *poolname first_address-last_address*. 次の例では、プール名は testpool です。

```
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)#
```

ステップ 2　変更を保存します。

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

ユーザの追加

に対するセキュリティ アプライアンスリモートアクセス ユーザを特定するには、ユーザ名とパスワードを設定します。

ステップ 1　ユーザを追加するには、**username** コマンドを入力します。構文は、**username** *username* **password** *password* です。次の例では、ユーザ名は testuser、パスワードは 12345678 です。

```
hostname(config)# username testuser password 12345678
hostname(config)#
```

ステップ 2　追加するユーザごとに、ステップ 1 を繰り返します。

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。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 36 章「LAN-to-LAN IPsec VPN の設定」のトランスフォーム セットの作成を参照してください。

ステップ 1　トランスフォーム セットを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec transform-set** コマンドを入力します。構文は次のとおりです。

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

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。

```
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)#
```

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。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。

基本的なリモート アクセス接続を確立するには、次のように 3 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 リモート アクセスに設定します。
- アドレス割り当て方式を設定します。次の例では、アドレス プールを使用します。
- 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 リモート アクセスに設定するには、**tunnel-group** コマンドを入力します。コマンド構文は、**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 タイプには、次のものがあります。

- 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 testgroup です。

```
hostname(config)# tunnel-group testgroup type ipsec-ra
hostname(config)#
```

ステップ 2　トンネル グループの認証方式を設定するには、一般属性モードに入り、**address-pool** コマンドを入力してアドレス プールを作成します。次の例では、グループの名前は testgroup で、アドレス プールの名前は testpool です。

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
```

ステップ 3　認証方式を設定するには、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。セキュリティ アプライアンスとクライアントの両方で同じ事前共有キーを使用する必要があります。

（注）　事前共有キーは VPN クライアントで使用されるキーの長さを超えることはできません。事前共有キーのサイズが異なる Cisco VPN Client がセキュリティ アプライアンスに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。

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 testgroup ipsec-attributes
hostname(config-ipsec)# pre-shared-key 44kkaol59636jnfx
```

ステップ 4　変更を保存します。

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

ダイナミック クリプト マップの作成

セキュリティ アプライアンスは、ダイナミック クリプト マップを使用してポリシー テンプレートを定義します。ポリシー テンプレートには、すべてのパラメータを設定する必要はありません。このようなダイナミック クリプト マップにより、セキュリティ アプライアンスは 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、セキュリティ アプライアンス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。

ステップ 1　ダイナミック 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 dynamic-map set transform-set** コマンドを入力します。

構文は、**crypto dynamic -map** *dynamic-map-name seq-num* **set transform-set** *transform-set-name* です。次の例では、ダイナミック マップの名前は dyn1、シーケンス番号は 1、トランスフォーム セット名は FirstSet です。

```
hostname(config)# crypto dynamic-map dyn1 1 set transform-set FirstSet
hostname(config)#
```

ステップ 2　このクリプト マップ エントリに基づく任意の接続で RRI をイネーブルにするには、**crypto dynamic-map set reverse route** コマンドを入力します。

```
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)#
```

ステップ 3　変更を保存します。

```
hostname(config)# write memory
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

次に、クリプト マップ エントリを作成します。これにより、セキュリティ アプライアンスは、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。これらのコマンドをグローバル 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　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 エントリを作成するには、**crypto map** コマンドを入力します。構文は、**crypto map** *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name* です。

```
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1

hostname(config)#
```

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 mymap interface outside
hostname(config)#
```