CHAPTER 31

VPN の IP アドレスの設定

この章では、IP アドレスの割り当て方式について説明します。

インターネットワーク接続は、IP アドレスによって可能になります。IP アドレスは、送信者と受信者の両方に接続用の番号が割り当てられている必要があるという点で、電話番号に似ています。ただし、VPN では、実際には 2 セットのアドレスが存在します。最初のセットは、パブリック ネットワーク上でクライアントとサーバを接続します。この接続が確立されると、2 番目のセットが VPN トンネル経由でクライアントとサーバを接続します。

セキュリティ アプライアンスのアドレス管理では、この IP アドレスの 2 番目のセットを扱います。これらのプライベート IP アドレスは、クライアントをトンネル経由でプライベート ネットワーク上のリソースに接続し、プライベート ネットワークに直接接続されているかのようなクライアント機能を提供します。また、ここでは、クライアントに割り当てられたプライベート IP アドレスのみを扱います。プライベート ネットワーク上のその他のリソースに割り当てられた IP アドレスは、VPN 管理ではなく、ネットワーク管理業務の一部に位置づけられます。したがって、ここで IP アドレスに言及する場合は、クライアントをトンネルのエンドポイントとして機能させる、プライベート ネットワークのアドレッシング方式で取得される IP アドレスを意味します。

この章は、次の項で構成されています。

IP アドレスの割り当て方式の設定

セキュリティ アプライアンスでは、リモート アクセス クライアントに IP アドレスを割り当てる際に、次の 1 つ以上の方式を使用することができます。複数のアドレス割り当て方式を設定すると、セキュリティ アプライアンスは IP アドレスが見つかるまで各オプションを検索します。デフォルトでは、すべての方式がイネーブルになっています。現在のコンフィギュレーションを表示するには、**show running-config all vpn-addr-assign** コマンドを入力します。

- **aaa**：ユーザ単位で外部認証サーバからアドレスを取得します。IP アドレスが設定された認証サーバを使用している場合は、この方式を使用することをお勧めします。
- **dhcp**：DHCP サーバから IP アドレスを取得します。DHCP を使用する場合は、DHCP サーバを設定する必要があります。また、DHCP サーバで使用可能な IP アドレスの範囲も定義する必要があります。

- **local**：**内部アドレス プールを使用します。**内部的に設定されたアドレス プールは、最も設定が簡単なアドレス プール割り当て方式です。ローカルを選択する場合は、**ip-local-pool** コマンドを使用して、使用する IP アドレスの範囲を定義する必要があります。

リモート アクセス クライアントへの IP アドレス割り当て方式を指定するには、グローバル コンフィギュレーション モードで **vpn-addr-assign** コマンドを入力します。構文は、**vpn-addr-assign {aaa | dhcp | local}** です。

ローカル IP アドレス プールの設定

VPN リモート アクセス トンネルに使用する IP アドレス プールを設定するには、グローバル コンフィギュレーション モードで **ip local pool** コマンドを入力します。アドレス プールを削除するには、このコマンドの **no** 形式を入力します。

セキュリティ アプライアンスは、該当の接続用のトンネル グループに基づいたアドレス プールを使用します。1 つのトンネル グループに複数のアドレス プールを設定する場合、セキュリティ アプライアンスは設定された順にそれらのプールを使用します。

ローカルでないサブネットのアドレスを割り当てる場合は、そのようなネットワーク用のルートの追加が容易になるように、サブネットの境界を担当するプールを追加することをお勧めします。

ローカル アドレス プールのコンフィギュレーションの概要は、次のようになります。

```
hostname(config)# vpn-addr-assign local
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
hostname(config)
```

ステップ 1　アドレス割り当て方式として IP アドレス プールを設定するには、**local** 引数を指定して **vpn-addr-assign** コマンドを入力します。

```
hostname(config)# vpn-addr-assign local
hostname(config)#
```

ステップ 2　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、ip local pool** *poolname first-address—last-address* **mask** *mask* です。

次に、firstpool という名前で IP アドレス プールを設定する例を示します。開始アドレスは 10.20.30.40 で、最終アドレスは 10.20.30.50 です。ネットワーク マスクは 255.255.255.0 です。

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
hostname(config)
```

AAA アドレッシングの設定

AAA サーバを使用して VPN リモート アクセス クライアントにアドレスを割り当てるには、まず AAA サーバまたは AAA サーバ グループを設定する必要があります。『*Cisco Security Appliance Command Reference*』の **aaa-server protocol** コマンドと、このマニュアルの第 13 章「AAA サーバとローカル データベースの設定」の AAA サーバ グループおよびサーバの識別を参照してください。

また、ユーザは RADIUS 認証用に設定されたトンネル グループと一致している必要があります。

次の例は、firstgroup という名前のトンネル グループに、RAD2 という AAA サーバ グループを定義する方法を示しています。例の中に 1 つ余分な手順が入っていますが、これは以前にそのトンネル グループに名前を付け、トンネル グループ タイプを定義していた場合のためです。この手順が次の例に記載されているのは、これらの値を設定しない限り、後続の tunnel-group コマンドにアクセスできないので、注意を促すためです。

この例で作成されるコンフィギュレーションの概要は、次のとおりです。

```
hostname(config)# vpn-addr-assign aaa
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)# authentication-server-group RAD2
```

IP アドレッシング用に AAA を設定するには、次の手順を実行します。

ステップ 1　アドレス割り当て方式として AAA を設定するには、**aaa** 引数を指定して **vpn-addr-assign** コマンドを入力します。

```
hostname(config)# vpn-addr-assign aaa
hostname(config)#
```

ステップ 2　firstgroup というトンネル グループをリモート アクセスまたは LAN-to-LAN トンネル グループとして確立するには、**type** キーワードを指定して **tunnel-group** コマンドを入力します。次の例では、リモート アクセス トンネル グループを設定しています。

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

ステップ 3　一般属性コンフィギュレーション モードに入り、firstgroup というトンネル グループの AAA サーバ グループを定義するには、**general-attributes** 引数を指定して **tunnel-group** コマンドを入力します。

```
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)#
```

ステップ 4　認証に使用する AAA サーバ グループを指定するには、**authentication-server-group** コマンドを入力します。

```
hostname(config-general)# authentication-server-group RAD2
hostname(config-general)#
```

このコマンドには、この例で示すより多くの引数があります。詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。

DHCP アドレッシングの設定

DHCP を使用して VPN クライアントのアドレスを割り当てるには、まず DHCP サーバ、およびその DHCP サーバで使用可能な IP アドレスの範囲を設定する必要があります。その後、トンネル グループ単位で DHCP サーバを定義します。また、オプションとして、該当のトンネル グループまたはユーザ名に関連付けられたグループ ポリシー内に、DHCP ネットワーク スコープも定義できます。このスコープは、使用する IP アドレス プールを DHCP サーバに指定するための、IP ネットワーク番号または IP アドレスです。

次の例では、firstgroup という名前のトンネル グループに、IP アドレス 172.33.44.19 の DHCP サーバを定義しています。また、この例では、remotegroup というグループ ポリシーに対して、192.86.0.0 という DHCP ネットワーク スコープも定義しています （remotegroup というグループ ポリシーは、

firstgroup というトンネル グループに関連付けられています)。ネットワーク スコープを定義しない場合、DHCP サーバはアドレス プールの設定順にプール内を探して IP アドレスを割り当てます。未割り当てのアドレスが見つかるまで、プールが順に検索されます。

次のコンフィギュレーションには、本来不要な手順が含まれています。これらは、以前にそのトンネル グループに名前を付け、トンネル グループ タイプをリモート アクセスとして定義していたり、グループ ポリシーに名前を付け、内部または外部として指定していた場合のためです。これらの手順が次の例に記載されているのは、これらの値を設定しない限り、後続の tunnel-group コマンドおよび group-policy コマンドにアクセスできないので、注意を促すためです。

この例で作成されるコンフィギュレーションの概要は、次のとおりです。

```
hostname(config)# vpn-addr-assign dhcp
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)# exit
hostname(config)# group-policy remotegroup internal
hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)# dhcp-network-scope 192.86.0.0
```

IP アドレッシング用に DHCP サーバを設定するには、次の手順を実行します。

ステップ 1　アドレス割り当て方式として DHCP を設定するには、**dhcp** 引数を指定して **vpn-addr-assign** コマンドを入力します。

```
hostname(config)# vpn-addr-assign dhcp
hostname(config)#
```

ステップ 2　firstgroup というトンネル グループをリモート アクセスまたは LAN-to-LAN トンネル グループとして確立するには、**type** キーワードを指定して **tunnel-group** コマンドを入力します。次の例では、リモート アクセス トンネル グループを設定しています。

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

ステップ 3　一般属性コンフィギュレーション モードに入って DHCP サーバを定義するには、**general-attributes** 引数を指定して **tunnel-grou**p コマンドを入力します。

```
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config)#
```

ステップ 4　DHCP サーバを定義するには、**dhcp-server** コマンドを入力します。次の例では、IP アドレス 172.33.44.19 の DHCP サーバを設定しています。

```
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)#
```

ステップ 5　トンネル グループ モードを終了します。

```
hostname(config-general)# exit
hostname(config)#
```

ステップ 6　remotegroup というグループ ポリシーを、内部的または外部的に設定されたグループとして定義するには、**internal** 引数または **external** 引数を指定して **group-policy** コマンドを入力します。次の例では、内部グループを設定しています。

```
hostname(config)# group-policy remotegroup internal
hostname(config)#
```

ステップ 7　（任意）グループ ポリシー属性コンフィギュレーション モードに入り、DHCP サーバで使用する IP アドレスのサブネットワークを設定するには、**attributes** キーワードを指定して **group-policy** コマンドを入力します。

```
hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)#
```

ステップ 8　（任意）remotegroup というグループ ポリシーのユーザにアドレスを割り当てるために DHCP サーバで使用する IP アドレスの範囲を指定するには、dhcp-network-scope コマンドを入力します。次の例では、192.86.0.0 というネットワーク スコープを設定しています。

```
hostname(config-group-policy)# dhcp-network-scope 192.86.0.0
hostname(config-group-policy)#
```