VPN の IP アドレス

- IP アドレス割り当てポリシーの設定 （1 ページ）
- ローカル IP アドレス プールの設定 （3 ページ）
- AAA アドレス指定の設定 （5 ページ）
- DHCP アドレス指定の設定 （6 ページ）

IP アドレス割り当てポリシーの設定

ASA 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できます。複数のアドレス割り当て方式を設定すると、ASA 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。

- aaa ユーザー単位で外部認証、認可、アカウンティング サーバー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ー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。この方法は IPv4 および IPv6 の割り当てポリシーに使用できます。
- dhcp DHCP サーバーから IP アドレスを取得します。DHCP を使用する場合は、DHCP サーバーを設定する必要があります。また、DHCP サーバーで使用可能な IP アドレスの範囲も定義する必要があります。この方法は IPv4 の割り当てポリシーに使用できます。
- **local** ：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もあります。この方法は IPv4 および IPv6 の割り当てポリシーに使用できます。
  - [Allow the reuse of an IP address so many minutes after it is released]：IP アドレスがアドレス プールに戻された後に、IP アドレスを再利用するまでの時間を指定します。遅延時間を設けることにより、IP アドレスがすぐに再割り当てされることによって発生する問題がファイアウォールで生じないようにできます。デフォルトでは、ASA は遅延時間を課しません。この設定要素は、IPv4 割り当てポリシーで使用できます。

次のいずれかの方式を使用して、IP アドレスをリモート アクセス クライアントに割り当てる方法を指定します。

IPv4 アドレス割り当ての設定

手順

ASA のアドレス割り当て方式を有効にして、IPv4 アドレスを VPN 接続に割り当てるときに使用します。IP アドレスを取得する使用可能な方式は、AAA サーバー、DHCP サーバー、またはローカル アドレス プールからの取得です。これらの方式はすべてデフォルトでイネーブルになっています。

vpn-addr-assign {**aaa** | **dhcp** | **local** [**reuse-delay** *minutes*]}

例：

たとえば、IP アドレスが解放された後に 0 ～ 480 分間の IP アドレスの再使用を設定できます。

```
hostname(config)#vpn-addr-assign aaa
hostname(config)#vpn-addr-assign local reuse-delay 180
```

この例では、コマンドの no 形式を使用してアドレス割り当て方式を無効にします。

```
hostname(config)# no vpn-addr-assign dhcp
```

IPv6 アドレス割り当ての設定

手順

ASA のアドレス割り当て方式を有効にして、IPv6 アドレスを VPN 接続に割り当てるときに使用します。IP アドレスを取得する使用可能な方式は、AAA サーバーまたはローカル アドレス プールからの取得です。これら両方の方式はデフォルトでイネーブルになっています。

ipv6-vpn-addr-assign {**aaa** | local}

例：

```
hostname(config)# ipv6-vpn-addr-assign aaa
```

この例では、コマンドの no 形式を使用してアドレス割り当て方式を無効にします。

```
hostname(config)# no ipv6-vpn-addr-assign local
```

アドレス割り当て方式の表示

手順

ASA で設定されているアドレス割り当て方式を表示するには、次のいずれかの方式を使用します。

- IPv4 アドレス割り当ての表示

  設定されているアドレス割り当て方式を表示します。設定されているアドレス方式は、aaa、dhcp、または local です。

```
show running-config all vpn-addr-assign
vpn-addr-assign aaa
vpn-addr-assign dhcp
vpn-addr-assign local
```

- IPv6 アドレス割り当ての表示

  設定されているアドレス割り当て方式を表示します。設定されているアドレス方式は、aaa または local となります。

```
show running-config all ipv6-vpn-addr-assign
ipv6-vpn-addr-assign aaa
ipv6-vpn-addr-assign local reuse-delay 0
```

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 IPv4 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。

VPN リモート アクセス トンネルに使用する IPv6 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 **ipv6 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。

ASA は、接続用の接続プロファイルまたはトンネル グループに基づいてアドレス プールを使用します。プールの指定順序は重要です。接続プロファイルまたはグループ ポリシーに複数のアドレス プールを設定すると、ASA は追加された順で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。

（注） アクティブなトンネルグループ内で現在使用されている（つまり、接続のためにエンドユーザーが利用できる）既存のアドレスプールを変更する場合は、変更ウィンドウで変更を行う必要があります。その際、次のことを確認してください。

- 接続されているユーザーはログオフされます。
- トンネルグループからアドレスプールが削除され、必要に応じて変更されます。
- 変更されたアドレスプールがトンネルグループに再び追加されます。

これ以外の方法でアドレスプールを変更すると、ASA の動作に不整合が生じる可能性があります。

ローカル IPv4 アドレス プールの設定

（注） CLI で、アクティブなトンネルグループ内で現在使用されている（つまり、接続のためにエンドユーザーが利用できる）既存のアドレスプールを変更する場合は、変更ウィンドウでこの変更を行うことを推奨します。接続されたユーザーをログオフし、アドレスプールをトンネルグループから削除し、必要に応じて変更してから、トンネルグループに再度追加する必要があります。これ以外の方法でアドレスプールを変更すると、ASA の動作に不整合が生じる可能性があります。

手順

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

例：

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

ステップ 2 アドレス プールを設定します。このコマンドは、プールの名前を指定し、IPv4 アドレスとサブネット マスクの範囲を指定します。

ip local pool*poolname first_address-last_address***mask***mask*

例：

この例では、*firstpool* という IP アドレス プールを設定します。開始アドレスは 10.20.30.40、終了アドレスは 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
```

この例では、**firstpool** という IP アドレス プールを削除します。

```
hostname(config)# no ip local pool firstpool
```

ローカル IPv6 アドレス プールの設定

手順

ステップ 1 アドレス割り当て方式として IP アドレス プールを設定します。**local** 引数を指定して ipv6-**vpn-addr-assign** コマンドを入力します。

例：

```
hostname(config)# ipv6-vpn-addr-assign local
```

ステップ 2 アドレスプールを設定します。このコマンドは、プールに名前を指定し、開始IPv6アドレス、ビット単位のプレフィックス長、および範囲内で使用するアドレスの数を特定します。

ipv6 local pool *pool_name starting_address prefix_length number_of_addresses*

例：

この例では、*ipv6pool* という IP アドレス プールを設定します。開始アドレスは 2001:DB8::1、プレフィックス長は 32 ビット、プールで使用するアドレス数は 100 です。

```
hostname(config)# ipv6 local pool ipv6pool 2001:DB8::1/32 100
```

この例では、*ipv6pool* という IP アドレス プールを削除します。

```
hostname(config)# no ipv6 local pool ipv6pool
```

AAA アドレス指定の設定

AAA サーバーを使用して 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 サーバーまたは AAA サーバー グループを設定する必要があります。コマンド リファレンスで **aaa-server protocol** コマンドを参照してください。

また、ユーザーはRADIUS認証用に設定された接続プロファイル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 サーバー 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)# 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。

手順

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 サーバー 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 サーバー 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)#
```

次のタスク

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、コマンド リファレンスを参照してください。

DHCP アドレス指定の設定

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 サーバー、およびその DHCP サーバーで使用可能な IP アドレスの範囲を設定する必要があります。その後、接続プロファイル単位で DHCP サーバーを定義します。また、オプションとして、該当の接続

プロファイルまたはユーザー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。

次の例では、firstgroup という名前の接続プロファイルに、172.33.44.19 の DHCP サーバーを定義しています。この例では、remotegroup というグループポリシーに対して、10.100.10.1 の 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 という接続プロファイル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 サーバーはアドレス 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。

始める前に

IPv4 アドレスを使用して、クライアント アドレスを割り当てる DHCP サーバーを識別できます。また、DHCP オプションはユーザーに転送されず、ユーザーはアドレス割り当てのみを受信します。

手順

ステップ 1 アドレス割り当て方式として IP アドレス プールを設定します。

vpn-addr-assign dhcp

ステップ 2 リモートアクセス接続プロファイルとして **firstgroup** という名前の接続プロファイルを設定します。

tunnel-group firstgroup type remote-access

ステップ 3 DHCP サーバーを設定できるように、接続プロファイルの一般属性コンフィギュレーション モードを開始します。

tunnel-group firstgroup general-attributes

ステップ 4 IPv4 アドレスで DHCP サーバーを定義し、トンネル グループ コンフィギュレーション モードを終了します。

dhcp-server *IPv4_address_of_DHCP_server*

IPv6 アドレスで DHCP サーバーを定義することはできません。接続プロファイルに複数の DHCP サーバー アドレスを指定できます。dhcp-server コマンドを入力します。このコマンドを使用すると、VPN クライアントの IP アドレスの取得を試みるときに、指定された DHCP サーバーに追加のオプションを送信するように ASA を設定できます。

例：

この例では、IP アドレス 172.33.44.19 の DHCP サーバーを設定しています。その後、トンネル グループ コンフィギュレーション モードを終了します。

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

ステップ 5 グループがまだ存在しない場合は、**remotegroup** という内部グループポリシーを作成します。

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

ステップ 6 （オプション）グループポリシー属性コンフィギュレーションモードを開始し、DHCP ネットワークスコープを定義します。

dhcp-network-scope *ip_address*

接続プロファイルのアドレスプールに DHCP サーバーを設定した場合、DHCP スコープはこのグループのプールに使用するサブネットを識別します。DHCP サーバーには、そのスコープによって識別される同じサブネット内のアドレスも設定されている必要があります。スコープを使用すると、この特定のグループに使用する DHCP サーバーで定義されているアドレスプールのサブセットを選択できます。

ネットワーク スコープを定義しない場合、DHCP サーバーはアドレス 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。

スコープを指定するには、目的のプールと同じサブネット上にあり、そのプール内にはないルーティング可能なアドレスを入力します。DHCP サーバーは、この IP アドレスが属するサブネットを判別し、そのプールからの IP アドレスを割り当てます。

ルーティングの目的で可能な場合は常に、インターフェイスの IP アドレスを使用することを推奨します。たとえば、プールが 10.100.10.2 ～ 10.100.10.254 で、インターフェイスアドレスが 10.100.10.1/24 の場合、DHCP スコープとして 10.100.10.1 を使用します。ネットワーク番号は使用しないでください。DHCP は IPv4 アドレス指定にのみ使用することができます。選択したアドレスがインターフェイスアドレスではない場合、スコープアドレスのスタティックルートを作成する必要があります。

例：

次の例では、remotegroup の属性コンフィギュレーション モードを開始し、DHCP スコープを 10.100.10.1 に設定します。

```
hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.100.10.1
```

例

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 remote-access
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 10.100.10.1
```

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。