CHAPTER 72

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。

ASA 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。

この章の内容は、次のとおりです。

- 「IP アドレスの割り当てポリシーの設定」（P.72-1）
- 「ローカル IP アドレス プールの設定」（P.72-3）
- 「AAA アドレッシングの設定」（P.72-5）
- 「DHCP アドレッシングの設定」（P.72-6）

IP アドレスの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、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**：ユーザ単位で外部認証、許可、アカウンティング 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。この方式は、IPv4 および IPv6 割り当てポリシーで使用できます。
- **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。この方式は、IPv4 割り当てポリシーで使用できます。
- **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があります。この方式は、IPv4 および IPv6 割り当てポリシーで使用できます。

– [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。

次の方法のいずれかを使用して、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。

- コマンドラインでの IPv4 アドレス割り当ての設定
- コマンドラインでの IPv6 アドレス割り当ての設定

コマンドラインでの IPv4 アドレス割り当ての設定

コマンド	目的
vpn-addr-assign {aaa | dhcp | local [reuse-delay *minutes*]}	ASA のアドレス割り当て方式をイネーブルにして、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、DHCP サーバ、またはローカル アドレス プールからの取得です。これらの方式すべてはデフォルトでイネーブルになっています。
例： hostname(config)# **vpn-addr-assign aaa**	
例： hostname(config)# **vpn-addr-assign local reuse-delay 180**	ローカル IP アドレス プールの場合、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。
例： hostname(config)# **no vpn-addr-assign dhcp**	アドレス割り当て方式をディセーブルにするには、コマンドの no 形式を使用します。

コマンドラインでの IPv6 アドレス割り当ての設定

コマンド	目的
ipv6-vpn-addr-assign {aaa | local}	ASA のアドレス割り当て方式をイネーブルにして、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。
例： hostname(config)# **ipv6-vpn-addr-assign aaa**	
例： hostname(config)# **no ipv6-vpn-addr-assign local**	アドレス割り当て方式をディセーブルにするには、コマンドの no 形式を使用します。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

アドレス割り当て方式の表示

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。

コマンドラインからの IPv4 アドレス割り当ての表示

コマンド	目的

show running-config all vpn-addr-assign
 	
例：
`hostname(config)# show running-config all vpn-addr-assign`
	設定されているアドレス割り当て方式を示します。設定されているアドレス方式は、aaa、dhcp、または local となります。
	`vpn-addr-assign aaa`
	`vpn-addr-assign dhcp`
	`vpn-addr-assign local`

コマンドラインからの IPv6 アドレス割り当ての表示

コマンド	目的

show running-config all ipv6-vpn-addr-assign
 	
例：
`hostname(config)# show running-config all ipv6-vpn-addr-assign`
	設定されているアドレス割り当て方式を示します。設定されているアドレス方式は、aaa または local となります。
	
	`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 グループに基づいたアドレス 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 ASA に追加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 IP アドレス プールを設定するには、次のいずれかの方法を使用します。

- 「CLI を使用したローカル IPv4 アドレス プールの設定」（P.72-4）
- 「CLI を使用したローカル IPv6 アドレス プールの設定」（P.72-4）

CLI を使用したローカル IPv4 アドレス プールの設定

	コマンド	目的
ステップ 1	**vpn-addr-assign local** **例：** hostname(config)# **vpn-addr-assign local**	**local** 引数を指定して **vpn-addr-assign** コマンドを入力し、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。「「コマンドラインでの IPv4 アドレス割り当ての設定」（P.72-2）」も参照してください。
ステップ 2	**ip local pool** *poolname first_address–last_address* **mask** *mask* **例：** hostname(config)# ip local pool **firstpool** **10.20.30.40-10.20.30.50** mask **255.255.255.0** **例：** hostname(config)# no ip local pool **firstpool**	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。 最初の例では、**firstpool** という名前で IP アドレス プールを設定しています。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。 2 番目の例では、**firstpool** という名前の IP アドレス プールを削除しています。

CLI を使用したローカル IPv6 アドレス プールの設定

	コマンド	目的
ステップ 1	**ipv6-vpn-addr-assign local** **例：** hostname(config)# **ipv6-vpn-addr-assign local**	**local** 引数を指定して **ipv6-vpn-addr-assign** コマンドを入力し、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。「「コマンドラインでの IPv6 アドレス割り当ての設定」（P.72-2）」も参照してください。
ステップ 2	**ipv6 local pool** *pool_name starting_address prefix_length number_of_addresses* **例：** hostname(config)# **ipv6 local pool** *ipv6pool 2001:DB8::1/32 100* **例：** hostname(config)# **no ipv6 local pool** *ipv6pool*	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。 最初の例では、**ipv6pool** という名前で IP アドレス プールを設定しています。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。 2 番目の例では、**ipv6pool** という名前の IP アドレス プールを削除しています。

モード

次の表は、この機能を使用できるモードを示したものです。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

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。コマンド リファレンスの **aaa-server protocol** コマンドの項、および「AAA サーバ グループの設定」（P.38-11）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 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、コマンド リファレンス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、接続プロファイル単位で DHCP サーバを定義します。また、オプションとして、該当の接続プロファイル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** という名前の接続プロファイルに、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、以前にその接続プロファイルに名前を付け、接続プロファイル 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。

注意事項と制限事項

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 サーバを識別できます。

CLI を使用した DHCP アドレッシングの設定

	コマンド	目的
ステップ 1	`vpn-addr-assign dhcp`	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。**dhcp** 引数を指定して **vpn-addr-assign** コマンドを入力します。「コマンドラインでの IPv4 アドレス割り当ての設定」(P.72-2)」も参照してください。
ステップ 2	`tunnel-group firstgroup type remote-access`	リモート アクセス接続プロファイルとして firstgroup という接続プロファイルを確立します。 **type** キーワードおよび **remote-access** 引数を指定して **tunnel-group** コマンドを入力します。

	コマンド	目的
ステップ 3	`tunnel-group firstgroup` **`general-attributes`**	DHCP サーバ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。 **general-attributes** 引数を指定して **tunnel-group** コマンドを入力します。
ステップ 4	`dhcp-server` *`IPv4_address_of_DHCP_server`* **例：** `hostname(config-general)# dhcp-server` **`172.33.44.19`** `hostname(config-general)#`	IPv4 アドレスで DHCP サーバを定義します。IPv6 アドレスで DHCP サーバ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 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 アドレスを取得しようとしているときに指定した DHCP サーバ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。詳細については、『*Cisco Security Appliance Command Reference*』の **dhcp-server** コマンドを参照してください。 この例では、IP アドレス 172.33.44.19 の DHCP サーバを設定しています。
ステップ 5	`hostname(config-general)#` **`exit`** `hostname(config)#`	トンネル グループ モードを終了します。
ステップ 6	`hostname(config)# group-policy remotegroup` **`internal`**	**remotegroup** という内部グループ ポリシーを作成します。 内部グループ ポリシーを作成するには、**internal** 引数を指定して **group-policy** コマンドを入力します。 この例では、内部グループを設定しています。

	コマンド	目的
ステップ 7	hostname(config)# group-policy remotegroup **attributes** **例：** hostname(config)# group-policy remotegroup **attributes** hostname(config-group-policy)#	（任意）グループ ポリシー属性コンフィギュレーション モードを開始し、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します。 **attributes** キーワードを指定して **group-policy** コマンドを入力します。 この例では、**remotegroup** グループ ポリシーのグループ ポリシー属性コンフィギュレーション モードを開始しています。
ステップ 8	hostname(config-group-policy)# **dhcp-network-scope 192.86.0.0** hostname(config-group-policy)#	（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。 この例では、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。 **（注）** dhcp-network-scope は、DHCP プールのサブセットではなく、ルーティング可能な IP アドレスである必要があります。DHCP サーバは、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。ルーティングの理由により、ASA のインターフェイスを dhcp-network-scope として使用することをお勧めします。任意の IP アドレスを dhcp-network-scope として使用できますが、ネットワークにスタティック ルートを追加する必要がある場合があります。

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 192.86.0.0
```