



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 \(3 ページ\)](#)
- [DHCP アドレス指定の設定 \(6 ページ\)](#)
- [ローカル ユーザへの IP アドレスの割り当て \(7 ページ\)](#)

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。

- **[Use authentication server]** : ユーザ単位で外部認証、認可、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。AAA サーバは、**[Configuration] > [AAA Setup]** ペインで設定できます。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。
- **[Use 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。DHCP を使用する場合は、**[Configuration] > [Remote Access VPN] > [DHCP Server]** ペインでサーバを設定します。この方法は IPv4 の割り当てポリシーに使用できます。
- **[Use an internal address pool]** : 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。この方法を使用する場合は、**[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools]** ペインで IP アドレスプールを設定します。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。
- **[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、これはチェック

クされません。つまり、ASAは遅延時間を課しません。遅延時間を設定する場合は、チェックボックスをオンにし、IPアドレスを再割り当てするまでの時間を1～480の範囲で指定します。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。

IPアドレス割り当てオプションの設定

手順

ステップ1 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Assignment Policy] を選択します。

ステップ2 [IPv4 Policy] エリアで、アドレス割り当て方式をオンにして有効にするか、オフにして無効にします。次の方法は、デフォルトで有効になっています。

- [Use Authentication server]: IPアドレスを提供するために設定した認証、許可、アカウントिंग (AAA) サーバを使用できるようにします。
- [Use DHCP]: IPアドレスを提供するために設定したダイナミックホストコンフィギュレーションプロトコル (DHCP) サーバを使用できるようにします。
- [Use internal address pools] : ASA で設定されたローカルアドレスプール設定を使用できるようにします。

[Use internal address pools] を有効にする場合、IPv4アドレスが解放された後、そのアドレスの再利用を有効にできます。You can specify a range of minutes from 0-480 after which the IP v4 address can be reused.

ステップ3 [IPv6 Policy] エリアで、アドレス割り当て方式をオンにして有効にするか、オフにして無効にします。次の方法は、デフォルトで有効になっています。

- [Use Authentication server]: IPアドレスを提供するために設定した認証、許可、アカウントिंग (AAA) サーバを使用できるようにします。
- [Use internal address pools] : ASA で設定されたローカルアドレスプール設定を使用できるようにします。

ステップ4 [Apply] をクリックします。

ステップ5 [OK] をクリックします。

アドレス割り当て方式の表示

手順

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Assignment Policy] の順に選択します。

ローカル IP アドレス プールの設定

VPN リモート アクセス トンネルに対して IPv4 または IPv6 アドレス プールを設定するには、ASDM を開き、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Management] > [Address Pools] > [Add/Edit IP Pool] を選択します。アドレス プールを削除するには、ASDM を開き、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Management] > [Address Pools] を選択します。削除するアドレス プールを選択し、[Delete] をクリックします。

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。

ローカル IPv4 アドレス プールの設定

[IP Pool] エリアには、設定されたアドレス プールが、名前ごとに、それぞれの IP アドレス範囲（たとえば、10.10.147.100～10.10.147.177）とともに表示されます。プールが存在しない場合、エリアは空です。ASA は、リストに表示される順番でこれらのプールを使用します。最初のプール内のアドレスがすべて割り当てられると、次のプールのアドレスが使用され、以下同様に処理されます。

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。

手順

ステップ 1 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools] を選択します。

ステップ 2 IPv4 アドレスを追加するには、**[Add] > [IPv4 Address pool]** をクリックします。既存のアドレス プールを編集するには、アドレス プール テーブルで、**[Edit]** をクリックします。

ステップ 3 **[Add/Edit IP Pool]** ダイアログボックスで、次の情報を入力します。

- **[Pool Name]** : アドレス プールの名前を入力します。最大 64 文字を指定できます。
- **[Starting Address]** : 設定されたそれぞれのプールで使用可能な最初の IP アドレスを示します。たとえば 10.10.147.100 のように、ドット付き 10 進数表記を使用します。
- **[Ending Address]** : 設定されたそれぞれのプールで使用可能な最後の IP アドレスを示します。たとえば 10.10.147.177 のように、ドット付き 10 進数表記を使用します。
- **[Subnet Mask]** : この IP アドレスが常駐するサブネットを指定します。

ステップ 4 **[Apply]** をクリックします。

ステップ 5 **[OK]** をクリックします。

ローカル IPv6 アドレス プールの設定

[IP Pool] エリアには、設定されたアドレス プールが、名前ごとに、開始 IP アドレス範囲、アドレスプレフィックス、プールに設定できるアドレス数とともに表示されます。プールが存在しない場合、エリアは空です。ASA は、リストに表示される順番でこれらのプールを使用します。最初のプール内のアドレスがすべて割り当てられると、次のプールのアドレスが使用され、以下同様に処理されます。

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。

手順

ステップ 1 **[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools]** を選択します。

ステップ 2 IPv6 アドレスを追加するには、**[Add] > [IPv6 Address pool]** をクリックします。既存のアドレス プールを編集するには、アドレス プール テーブルで、**[Edit]** をクリックします。

ステップ 3 **[Add/Edit IP Pool]** ダイアログボックスで、次の情報を入力します。

- **[Name]** : 設定された各アドレス プールの名前を表示します。
[Starting IP Address] : 設定されたプールで使用可能な最初の IP アドレスを入力します。たとえば、2001:DB8::1 となります。
- **[Prefix Length]** : IP アドレスプレフィックス長をビット単位で入力します。たとえば、32 は CIDR 表記で /32 を表します。プレフィックス長は、IP アドレスが常駐するプールのサブネットを定義します。

- [Number of Addresses] : 開始 IP アドレスから始まる、プールにある IPv6 アドレスの数を指定します。

ステップ 4 [Apply] をクリックします。

ステップ 5 [OK] をクリックします。

グループポリシーへの内部アドレス プールの割り当て

[Add or Edit Group Policy] ダイアログボックスでは、追加または編集している内部ネットワーク（クライアント）アクセスグループポリシーのアドレスプール、トンネリングプロトコル、フィルタ、接続設定、およびサーバを指定できます。このダイアログボックスの各フィールドで、[Inherit] チェックボックスを選択すると、対応する設定の値をデフォルトグループポリシーから取得できます。[Inherit] は、このダイアログボックスの属性すべてのデフォルト値です。

同じグループポリシーで IPv4 と IPv6 両方のアドレスポリシーを設定できます。同じグループポリシーに両方のバージョンの IP アドレスが設定されている場合、IPv4 に設定されたクライアントは IPv4 アドレス、IPv6 に設定されたクライアントは IPv6 アドレスを取得し、IPv4 アドレスと IPv6 アドレス両方に設定されたクライアントは IPv4 アドレスと IPv6 アドレス両方を取得します。

手順

-
- ステップ 1 ASDM を使用して ASA に接続し、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。
 - ステップ 2 新しいグループポリシーを作成するか、内部アドレスプールを設定するグループポリシーを作成し、[Edit] をクリックします。
[General attributes] ペインは [group policy] ダイアログで、デフォルトで選択されています。
 - ステップ 3 [Address Pools] フィールドを使用して、このグループポリシーの IPv4 アドレスプールを指定します。[Select] をクリックし、IPv4 アドレスプールを追加または編集します。
 - ステップ 4 [IPv6 Address Pools] フィールドを使用して、このグループポリシーに使用する IPv6 アドレスプールを指定します。[Select] をクリックし、IPv6 アドレスプールを追加または編集します。
 - ステップ 5 [OK] をクリックします。
 - ステップ 6 [Apply] をクリックします。
-

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、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。

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 サーバを識別できます。また、DHCP オプションはユーザに転送されず、ユーザはアドレス割り当てのみを受信します。

手順

ステップ 1 DHCP サーバを設定します。

DHCP サーバを使用して IPv6 アドレスを AnyConnect クライアントに割り当てることはできません。

- a) [設定 (Configuration)] > [リモートアクセス VPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [アドレス割り当て (Address Assignment)] > [割り当てポリシー (Assignment Policy)] で DHCP が有効になっていることを確認します。
- b) [設定 (Configuration)] > [リモートアクセス VPN (Remote Access VPN)] > [DHCP サーバ (DHCP Server)] を選択して、DHCP サーバを設定します。

ステップ 2 接続プロファイルで DHCP サーバを定義します。

- a) [設定 (Configuration)] > [リモートアクセス VPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [AnyConnect 接続プロファイル (AnyConnect Connection Profiles)] を選択します。
- b) [Connection Profiles] エリアで [Add] または [Edit] をクリックします。
- c) 接続プロファイルの設定ツリーで、[Basic] をクリックします。
- d) [Client Address Assignment] エリアで、クライアントに IP アドレスを割り当てるために使用する DHCP サーバの IPv4 アドレスを入力します。たとえば、**172.33.44.19** と指定します。

ステップ 3 DHCP スコープを定義するために、接続プロファイルに関連付けられたグループポリシーを編集します。

- a) [設定 (Configuration)] > [リモートアクセスVPN (Remote Access VPN)] > [ネットワーク (クライアント) アクセス (Network (Client) Access)] > [グループポリシー (Group Policies)] を選択します。
- b) 編集するグループ ポリシーをダブルクリックします。
- c) 設定ツリーで、[Server] をクリックします。
- d) 下矢印をクリックして、[More Options] エリアを拡大表示します。
- e) [DHCPスコープの継承 (DHCP Scope Inherit)] をオフにして、DHCP スコープを定義します。

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。

- f) [OK] をクリックします。
- g) [適用 (Apply)] をクリックします。

ローカル ユーザへの IP アドレスの割り当て

グループ ポリシーを使用するようにローカル ユーザ アカウントを設定し、また AnyConnect 属性を設定することもできます。IP アドレスの他のソースに障害が発生した場合に、これらのユーザ アカウントがフォールバックを提供するので、管理者は引き続きアクセスできます。

始める前に

ユーザを追加または編集するには、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] の順に選択し、[Add] または [Edit] をクリックします。

デフォルトでは、[Edit User Account] 画面の設定ごとに [Inherit] チェックボックスがオンになっています。つまり、ユーザアカウントは、デフォルトグループポリシー DfltGrpPolicy のその設定の値を継承するということです。

各設定内容をオーバーライドする場合は、[Inherit] チェックボックスをオフにし、新しい値を入力します。次の詳細な手順では IP アドレスの設定について説明します。設定の完全な詳細については [ローカル ユーザの VPN ポリシー属性の設定](#) を参照してください。

手順

-
- ステップ 1 ASDM を開始し、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] の順に選択します。
 - ステップ 2 設定するユーザを選択し、[Edit] をクリックします。
 - ステップ 3 左側のペインで、[VPN Policy] をクリックします。
 - ステップ 4 このユーザに対して専用の IPv4 アドレスを設定する場合は、[Dedicated IPv4 Address (Optional)] 領域で、IPv4 アドレスとサブネットマスクを入力します。
 - ステップ 5 このユーザに専用の IPv6 アドレスを設定するには、[Dedicated IPv6 Address (Optional)] 領域に IPv6 プレフィックスを含む IPv6 アドレスを入力します。IPv6 プレフィックスは、IPv6 アドレスが常駐するサブネットを示します。
 - ステップ 6 [Apply] をクリックして変更内容を実行コンフィギュレーションに保存します。
-