VPN の IP アドレス

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、アカウンティング（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、アカウンティング（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。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。

注意事項と制約事項

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。

DHCP を使用した IP アドレスの割り当て

DHCP サーバを設定してから、DHCP サーバを使用するグループ ポリシーを作成します。そのグループ ポリシーを選択すると、DHCP サーバが VPN 接続のアドレスを割り当てます。

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。
    1. ASDM を使用して ASA に接続します。
    2. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Assignment Policy] で DHCP がイネーブルになっていることを確認します。
    3. [Configuration] > [Remote Access VPN] > [DHCP Server] を選択して、DHCP サーバを設定します。
2. グループ ポリシーに DHCP IP アドレス指定を割り当てます。
    1. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] を選択します。

2. [Connection Profiles] エリアで [Add] または [Edit] をクリックします。
3. 接続プロファイルの設定ツリーで、[Basic] をクリックします。
4. [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。
5. 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。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。
6. 編集するグループ ポリシーをダブルクリックします。
7. 設定ツリーで、[Server] をクリックします。
8. 下矢印をクリックして、[More Options] エリアを拡大表示します。
9. DHCP スコープの [Inherit] のチェックを外します。
10. 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 アドレスを入力します。たとえば、**192.86.0.0** と指定します。
11. [OK] をクリックします。
12. [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。