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

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。

- [Use authentication server] *：*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。[Configuration] > [AAA Setup] ペインで AAA サーバを設定できます。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。この方式は、IPv4 割り当てポリシーで使用できます。

- [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、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 の割り当てポリシーに使用できます。

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。

- ASDM を使用した IP アドレス割り当ての設定

ASDM を使用した IP アドレス割り当ての設定

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。

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。

ASDM を使用した IPv4 および IPv6 のアドレス割り当ての表示

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

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。

- 「ASDM を使用したローカル IPv4 アドレス プールの設定」（P.4-3）
- 「ASDM を使用したローカル IPv6 アドレス プールの設定」（P.4-4）

ASDM を使用したローカル IPv4 アドレス プールの設定

[IP Pool] エリアには、設定された各アドレス 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。最初のプールのすべてのアドレスが割り当てられると、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。

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。

ASDM を使用したローカル IPv6 アドレス プールの設定

[IP Pool] エリアには、設定された各アドレス 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。最初のプールのすべてのアドレスが割り当てられると、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。

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。

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
•	—	•	—	—

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。

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。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。

DHCP サーバの設定

以下の指示に従って DHCP を使用するよう IP アドレス割り当てポリシーを設定します。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。

ステップ 1　ASDM を使用して ASA に接続します。

ステップ 2　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Assignment Policy] で DHCP がイネーブルにされていることを確認します。

ステップ 3　[Configuration] > [Remote Access VPN] > [DHCP Server] を選択して、DHCP サーバを設定します。

グループ ポリシーへの DHCP IP アドレスの割り当て

ステップ 1　[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [AnyConnect Connection Profiles] を選択します。

ステップ 2　[Connection Profiles] エリアで [Add] または [Edit] をクリックします。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 6　編集するグループ ポリシーをダブルクリックします。

ステップ 7　設定ツリーで、[Servers] をクリックします。

ステップ 8　下矢印をクリックして、[More Options] エリアを拡大表示します。

ステップ 9　DHCP スコープの [Inherit] のチェックを外します。

ステップ 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** と入力します。

ステップ 11　[OK] をクリックします。

ステップ 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。

ここでは、ローカル ユーザのすべての属性を設定する方法について説明します。

前提条件

この手順では、既存のユーザを編集する方法について説明します。ユーザを追加するには、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] を選択し、[Add] をクリックします。詳細については、『*Cisco ASA 5500 Configuration Guide Using ASDM*』の第 42 章「Configuring AAA Servers and the Local Database」の「Adding a User Account to the Local Database」を参照してください。

ユーザの編集

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。

各設定内容を上書きする場合は、[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「手順の詳細」で、[Edit User Account] 画面の各設定について説明しています。

手順の詳細

ステップ 1　ASDM を開始し、[Configuration] > [Remote Access VPN] > [AAA/Local Users] > [Local Users] を選択します。

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。

[Edit User Account] 画面が開きます。

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　ユーザのグループ ポリシーを指定します。ユーザ ポリシーは、このグループ ポリシーの属性を継承します。この画面にデフォルト グループ ポリシーの設定を**継承するよう**設定されている他のフィールドがある場合、このグループ ポリシーで指定された属性がデフォルト グループ ポリシーの属性より優先されます。

ステップ 5　ユーザが使用できるトンネリング プロトコルを指定するか、グループ ポリシーから値を継承するかどうかを指定します。目的の [Tunneling Protocols] チェックボックスをオンにし、使用できる VPN トンネリング プロトコルを選択します。選択されたプロトコルのみが使用可能になります。次の選択肢があります。

- （SSL/TLS を利用する VPN）クライアントレス SSL VPN では、Web ブラウザを使用して VPN コンセントレータへのセキュアなリモート アクセス トンネルを確立し、ソフトウェア クライアントもハードウェア クライアントも必要としません。クライアントレス SSL VPN を使用すると、HTTPS インターネット サイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有（Web 対応）、電子メール、およびその他の TCP ベース アプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。
- SSL VPN クライアントは、Cisco AnyConnect Client アプリケーションのダウンロード後にユーザが接続できるようにします。ユーザは、最初にクライアントレス SSL VPN 接続を使用してこのアプリケーションをダウンロードします。ユーザが接続するたびに、必要に応じてクライアント アップデートが自動的に行われます。
- [IPsec IKEv1] : IP セキュリティ プロトコル。IPsec は最もセキュアなプロトコルとされており、VPN トンネルのほぼ完全なアーキテクチャを提供します。Site-to-Site（ピアツーピア）接続、および Cisco VPN クライアントと LAN 間の接続の両方で IPsec IKEv1 を使用できます。
- [IPsec IKEv2] : AnyConnect Secure Mobility Client 対応の IPsec IKEv2。IKEv2 を使用した IPsec による AnyConnect 接続では、SSL VPN 接続が使用できる同じ機能セットを利用できます。
- L2TP over IPSec では、複数の PC やモバイル PC に採用されている一般的なオペレーティング システムに付属の VPN クライアントを使用するリモート ユーザが、パブリック IP ネットワークを介して ASA およびプライベート企業ネットワークへのセキュアな接続を確立できるようにします。

（注）　プロトコルを選択しなかった場合は、エラー メッセージが表示されます。

ステップ 6　使用するフィルタ（IPv4 または IPv6）を指定するか、またはグループ ポリシーの値を継承するかどうかを指定します。フィルタは、ASA を経由して着信したトンネリングされたデータ パケットを、送信元アドレス、宛先アドレス、プロトコルなどの基準によって、許可するか拒否するかを決定するルールで構成されます。フィルタおよびルールを設定するには、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] > [Add/Edit] > [General] > [More Options] > [Filter] を選択します。

[Manage] をクリックして、ACL と ACE を追加、編集、および削除できる [ACL Manager] ペインを表示します。

ステップ 7　接続プロファイル（トンネル グループ ロック）がある場合、それを継承するかどうか、または選択したトンネル グループ ロックを使用するかどうかを指定します。特定のロックを選択すると、ユーザのリモート アクセスはこのグループだけに制限されます。[Tunnel Group Lock] では、VPN クライアントで設定されたグループと、そのユーザが割り当てられているグループが同じかどうかをチェックすることによって、ユーザが制限されます。同一ではなかった場合、ASA はユーザによる接続を禁止します。[Inherit] チェックボックスがオフの場合、デフォルト値は [None] です。

ステップ 8　[Store Password on Client System] 設定をグループから継承するかどうかを指定します。[Inherit] チェックボックスをオフにすると、[Yes] および [No] のオプション ボタンが有効になります。[Yes] をクリックすると、ログオン パスワードがクライアント システムに保存されます（セキュリティが低下するおそれのあるオプションです）。接続ごとにユーザにパスワードの入力を求めるようにするには、[No] をクリックします（デフォルト）。セキュリティを最大限に確保するためにも、パスワードの保存は*許可しない*ことを推奨します。

ステップ 9　このユーザに適用するアクセス時間ポリシーを指定する、そのユーザの新しいアクセス時間ポリシーを作成する、または [Inherit] チェックボックスをオンのままにします。デフォルトは [Inherit] です。また、[Inherit] チェックボックスがオフの場合のデフォルトは [Unrestricted] です。

[Manage] をクリックして、[Add Time Range] ダイアログボックスを開きます。このダイアログボックスでアクセス時間の新規セットを指定できます。

ステップ 10　ユーザによる同時ログオン数を指定します。Simultaneous Logons パラメータは、このユーザに指定できる最大同時ログオン数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログオンが無効になり、ユーザ アクセスを禁止します。

（注）　最大値を設定して制限しておかない同時に多数の接続が許可されるため、セキュリティとパフォーマンスの低下を招くおそれがあります。

ステップ 11　ユーザ接続時間の**最大接続時間**を分で指定します。ここで指定した時間が経過すると、システムは接続を終了します。最短時間は 1 分、最長時間は 2147483647 分（4000 年超）です。接続時間を無制限にするには、[Unlimited] チェックボックスをオンにします（デフォルト）。

ステップ 12　ユーザのアイドル タイムアウトを分で指定します。この期間、このユーザの接続に通信アクティビティがなかった場合、システムは接続を終了します。最短時間は 1 分で、最長時間は 10080 分です。この値は、クライアントレス SSL VPN 接続のユーザには適用されません。

ステップ 13　セッション アラート間隔を設定します。[Inherit] チェックボックスをオフにすると、自動的に [Default] チェックボックスがオンになります。これにより、セッション アラート間隔が 30 分に設定されます。新しい値を指定する場合は、[Default] チェックボックスをオフにして、セッション アラート間隔（1 ～ 30 分）を分数ボックスで指定します。

ステップ 14　アイドル アラート間隔を設定します。[Inherit] チェックボックスをオフにすると、自動的に [Default] チェックボックスがオンになります。これにより、アイドル アラート間隔が 30 分に設定されます。新しい値を指定する場合は、[Default] チェックボックスをオフにして、セッション アラート間隔（1 ～ 30 分）を分数ボックスで指定します。

ステップ 15　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] 領域（任意）で、IPv4 アドレスおよびサブネット マスクを入力します。

ステップ 16　このユーザに対して専用の IPv6 アドレスを設定する場合は、[Dedicated IPv6 Address] フィールド（任意）で、IPv6 アドレスを IPv6 プレフィックスとともに入力します。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 17　クライアントレス SSL の設定を行う場合は、左側のペインで、[Clientless SSL VPN] をクリックします。各設定内容を上書きする場合は、[Inherit] チェックボックスをオフにし、新しい値を入力します。

ステップ 18　[Apply] をクリックします。

変更内容が実行コンフィギュレーションに保存されます。