



Adresses IP pour les VPN

- [Configurer une politique d'attribution d'adresses IP, à la page 1](#)
- [Configurer les ensembles d'adresses IP locales, à la page 3](#)
- [Configurer l'adressage DHCP, à la page 5](#)
- [Attribuer des adresses IP aux utilisateurs locaux, à la page 7](#)

Configurer une politique d'attribution d'adresses IP.

L'ASA peut utiliser une ou plusieurs des méthodes suivantes pour affecter des adresses IP aux clients d'accès à distance. Si vous configurez plusieurs méthodes d'attribution d'adresse, l'ASA essaie chacune des options jusqu'à ce qu'il trouve une adresse IP. Par défaut, toutes les méthodes sont activées.

- **Use authentication server (Utiliser le serveur d'authentification)** : récupère les adresses à partir d'un serveur externe d'authentification, d'autorisation et de comptabilisation, sur une base par utilisateur. Si vous utilisez un serveur d'authentification sur lequel des adresses IP sont configurées, nous vous recommandons d'utiliser cette méthode. Vous pouvez configurer des serveurs AAA dans le volet Configuration > AAA Setup (Configuration AAA). Cette méthode est disponible pour les politiques d'attribution IPv4 et IPv6.
- **Use DHCP (Utiliser DHCP)** : obtient les adresses IP à partir d'un serveur DHCP. Si vous souhaitez utiliser DHCP, vous devez configurer un serveur DHCP. Vous devez également définir la plage d'adresses IP que le serveur DHCP peut utiliser. Si vous utilisez DHCP, configurez le serveur dans le volet Configuration > Remote Access VPN (VPN d'accès à distance) > DHCP Server (Serveur DHCP). Cette méthode est disponible pour les politiques d'attribution IPv4.
- **Use an internal address pool (Utiliser un ensemble d'adresses interne)** : les ensembles d'adresses configurés en interne constituent la méthode d'affectation la plus simple à configurer. Si vous utilisez cette méthode, configurez les ensembles d'adresses IP dans le volet Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools pane (Configuration > VPN d'accès à distance > Accès au réseau (client) > Affectation d'adresses > Ensembles d'adresses). Cette méthode est disponible pour les politiques d'attribution IPv4 et IPv6.
 - **Autoriser la réutilisation d'une adresse IP un certain nombre de minutes après sa libération** : Retarde la réutilisation d'une adresse IP après son retour dans l'ensemble d'adresses. L'ajout d'un délai permet d'éviter les problèmes que les pare-feu peuvent rencontrer lorsqu'une adresse IP est réaffectée rapidement. Par défaut, cette option n'est pas cochée, ce qui signifie que l'ASA n'applique pas de délai. Si vous souhaitez appliquer un délai, cochez la case correspondante et saisissez un nombre de minutes compris entre 1 et 480 pour retarder la réaffectation de l'adresse IP. Cet élément configurable est disponible pour les politiques d'attribution IPv4.

Utilisez l'une des méthodes suivantes pour préciser un moyen d'affecter les adresses IP aux clients d'accès à distance.

Configurer les options d'affectation d'adresses IP

Procédure

-
- Étape 1** Sélectionnez **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Address Assignment (Affectation d'adresses) > Assignment Policy (Politique d'affectation)**.
- Étape 2** Dans la zone IPv4 Policy (politique IPv4), cochez la méthode d'affectation d'adresse pour l'activer ou décochez-la pour la désactiver. Ces méthodes sont activées par défaut :
- Utiliser le serveur d'authentification. Active l'utilisation d'un serveur d'authentification, d'autorisation et de comptabilité (AAA) que vous avez configuré pour fournir les adresses IP.
 - Utiliser DHCP. Active l'utilisation d'un serveur DHCP (Dynamic Host Configuration Protocol) que vous avez configuré pour fournir des adresses IP.
 - Use internal address pools (Utiliser des ensembles d'adresses internes) : active l'utilisation d'un ensemble d'adresses locales configuré sur l'ASA.
- Si vous activez **Use internal address pools** (Utiliser des ensembles d'adresses internes), vous pouvez également activer la réutilisation d'une adresse IPv4 après sa libération. Vous pouvez spécifier une plage de minutes de 0 à 480 après laquelle l'adresse IPv4 peut être réutilisée.
- Étape 3** Dans la zone IPv6 Policy (politique IPv6), cochez la méthode d'affectation d'adresse pour l'activer ou décochez-la pour la désactiver. Ces méthodes sont activées par défaut :
- Utiliser le serveur d'authentification. Active l'utilisation d'un serveur d'authentification, d'autorisation et de comptabilité (AAA) que vous avez configuré pour fournir les adresses IP.
 - Utiliser des ensembles d'adresses internes : active l'utilisation d'un ensemble d'adresses locales configuré sur l'ASA.
- Étape 4** Cliquez sur **Apply** (Appliquer).
- Étape 5** Cliquez sur **OK**.
-

Afficher les méthodes d'attribution d'adresses

Procédure

Sélectionnez **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau [client]) > Address Assignment (Affectation d'adresses) > Assignment Policy (Stratégie d'affectation)**.

Configurer les ensembles d'adresses IP locales

Pour configurer des ensembles d'adresses IPv4 ou IPv6 pour les tunnels VPN d'accès à distance, ouvrez ASDM et choisissez **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Address Management (Gestion des adresses) > Address Pools (Ensembles d'adresses) > Add/Edit IP Pool (Ajouter/Modifier un ensemble d'adresses IP)**. Pour supprimer un ensemble d'adresses, ouvrez ASDM et choisissez **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Address Management (Gestion des adresses) > Address Pools (Ensembles d'adresses)**. Sélectionnez l'ensemble d'adresses que vous souhaitez supprimer, et cliquez sur **Delete** (Supprimer).

L'ASA utilise les ensembles d'adresses en fonction du profil de connexion ou de la stratégie de groupe associés à la connexion. L'ordre dans lequel vous spécifiez les ensembles est important. Si vous configurez plusieurs ensembles d'adresses pour un profil de connexion ou une politique de groupe, l'ASA les utilise dans l'ordre dans lequel vous les avez ajoutées à l'ASA.

Si vous affectez des adresses à partir d'un sous-réseau non local, nous vous suggérons d'ajouter des pools qui se situent dans les limites de sous-réseau pour faciliter l'ajout de routes pour ces réseaux.

Configurer les ensembles d'adresses IPv4 locales

La zone IP Pool (Ensemble d'adresses IP) affiche les ensembles d'adresses configurés par nom avec leur plage d'adresses IP, par exemple : de 10.10.147.100 à 10.10.147.177. S'il n'existe aucun ensemble, la zone est vide. L'ASA utilise ces ensembles dans l'ordre indiqué : si toutes les adresses du premier ensemble ont été affectées, elle utilise l'ensemble suivant, et ainsi de suite.

Si vous affectez des adresses à partir d'un sous-réseau non local, nous vous suggérons d'ajouter des pools qui se situent dans les limites de sous-réseau pour faciliter l'ajout de routes pour ces réseaux.

Procédure

- | | |
|----------------|--|
| Étape 1 | Sélectionnez Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Address Assignment (Attribution d'adresses) > Address Pools (Ensembles d'adresses) . |
| Étape 2 | Pour ajouter une adresse IPv4, cliquez sur Add (Ajouter) > IPv4 Address Pool (Ensemble d'adresses IPv4) . Pour modifier un ensemble d'adresses existant, choisissez l'ensemble d'adresses dans la table d'ensemble d'adresses et cliquez sur Edit (Modifier). |
| Étape 3 | Dans la boîte de dialogue Add/Edit IP Pool (Ajouter/Modifier un ensemble d'adresses IP), saisissez les renseignements suivants : <ul style="list-style-type: none">• Nom : saisissez le nom de l'ensemble d'adresses IP. Il peut comporter jusqu'à 64 caractères• Adresse de départ : saisissez la première adresse IP disponible dans chaque ensemble configuré. Utilisez la notation décimale à points, par exemple : 10.10.147.100.• Adresse de fin : saisissez la dernière adresse IP disponible dans chaque ensemble configuré. Notation décimale à points de l'utilisateur, par exemple : 10.10.147.177.• Masque de sous-réseau : identifie le sous-réseau sur lequel cet ensemble d'adresses IP se trouve. |

Étape 4 Cliquez sur **Apply** (Appliquer).

Étape 5 Cliquez sur **OK**.

Configurer les ensembles d'adresses IPv6 locales

La zone IP Pool (Ensemble IP) affiche les ensembles d'adresses configurées par nom avec une plage d'adresses IP de départ, le préfixe d'adresse et le nombre d'adresses configurables dans l'ensemble. S'il n'y a aucun ensemble, la zone est vide. L'ASA utilise ces ensembles dans l'ordre indiqué : si toutes les adresses du premier ensemble ont été affectées, elle utilise l'ensemble suivant, et ainsi de suite.

Si vous affectez des adresses à partir d'un sous-réseau non local, nous vous suggérons d'ajouter des pools qui se situent dans les limites de sous-réseau pour faciliter l'ajout de routes pour ces réseaux.

Procédure

Étape 1 Sélectionnez **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Address Assignment (Affectation d'adresses) > Address Pools (Ensembles d'adresses)**.

Étape 2 Pour ajouter une adresse IPv6, cliquez sur **Add > (Ajouter) > IPv6 Address Pool (Ensemble d'adresses IPv6)**. Pour modifier une ensemble d'adresses existant, choisissez l'ensemble d'adresses dans le tableau des ensembles d'adresses et cliquez sur **Edit** (Modifier).

Étape 3 Dans la boîte de dialogue Add/Edit IP Pool (Ajouter/Modifier un ensemble d'adresses IP), saisissez les informations suivantes :

- **Nom** : affiche le nom de chaque ensemble d'adresses configurée.

Adresse IP de départ : saisissez la première adresse IP disponible dans l'ensemble d'adresses configuré.
Par exemple : 2001:DB8::1.

- **Longueur du préfixe** : saisissez la longueur du préfixe d'adresse IP en bits. Par exemple, 32 représente /32 en notation CIDR. La longueur du préfixe définit le sous-réseau sur lequel réside l'ensemble d'adresses IP.

- **Number of Addresses(nombre d'adresses)** : Détermine le nombre d'adresses IPv6, en commençant par l'adresse IP de départ, qui se trouvent dans l'ensemble.

Étape 4 Cliquez sur **Apply** (Appliquer).

Étape 5 Cliquez sur **OK**.

Affecter des ensembles d'adresses internes aux stratégies de groupe

La boîte de dialogue Add or Edit Group Policy (Ajouter ou modifier une stratégie de groupe) vous permet de préciser les ensembles d'adresses, les protocoles de tunnellation, les filtres, les paramètres de connexion et les serveurs pour la stratégie de groupe interne Network (Client) Access (Accès réseau [client]) en cours d'ajout ou de modification. Pour chacun des champs de cette boîte de dialogue, le fait de cocher la case Inherit

(Hériter) permet au paramètre correspondant de prendre sa valeur à partir de la stratégie de groupe par défaut. Inherit (Hériter) est la valeur par défaut de tous les attributs de cette boîte de dialogue.

Remarque : vous pouvez configurer des ensembles d'adresses IPv4 et IPv6 pour la même stratégie de groupe. Si les deux versions des adresses IP sont configurées dans la même politique de groupe, les clients configurés pour IPv4 obtiendront une adresse IPv4, les clients configurés pour IPv6 obtiendront une adresse IPv6 et les clients configurés pour à la fois les adresses IPv4 et IPv6 obtiendront à la fois une adresse IPv4 et une adresse IPv6.

Procédure

-
- | | |
|----------------|--|
| Étape 1 | Connectez-vous à l'ASA à l'aide d'ASDM et sélectionnez Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Group Policies (Stratégies de groupe) . |
| Étape 2 | Créez une nouvelle stratégie de groupe ou sélectionnez la stratégie de groupe que vous souhaitez configurer avec un ensemble d'adresses internes, puis cliquez sur Edit (Modifier).

Le volet General attributes (Attributs généraux) est sélectionné par défaut dans la boîte de dialogue de stratégie de groupe. |
| Étape 3 | Utilisez le champ Address Pools (Ensembles d'adresses) pour préciser un ensemble d'adresses IPv4 pour cette stratégie de groupe. Cliquez sur Select (Sélectionner) pour ajouter ou modifier un ensemble d'adresses IPv4. |
| Étape 4 | Utilisez le champ IPv6 Address Pools (Ensembles d'adresses IPv6) pour préciser un ensemble d'adresses IPv6 à utiliser pour cette stratégie de groupe. Cliquez sur Select (Sélectionner) pour ajouter ou modifier un ensemble d'adresses IPv6. |
| Étape 5 | Cliquez sur OK . |
| Étape 6 | Cliquez sur Apply (Appliquer). |
-

Configurer l'adressage DHCP

Pour utiliser DHCP afin d'attribuer des adresses aux clients VPN, vous devez d'abord configurer un serveur DHCP et la plage d'adresses IP que le serveur DHCP peut utiliser. Vous définissez ensuite le serveur DHCP par profil de connexion. Vous pouvez également définir une portée de réseau DHCP dans la stratégie de groupe associée à un profil de connexion ou un nom d'utilisateur.

L'exemple suivant définit le serveur DHCP à l'adresse 172.33.44.19 pour le profil de connexion nommé **FirstGroup**. L'exemple définit également une portée de réseau DHCP de 10.100.10.1 pour la stratégie de groupe appelée **remotegroup**. (La stratégie de groupe appelée remotegroup est associée au profil de connexion appelé firstgroup). Si vous ne définissez pas de portée réseau, le serveur DHCP attribue les adresses IP dans l'ordre des ensembles d'adresses configurés. Il parcourt les ensembles jusqu'à ce qu'il identifie une adresse non attribuée.

Avant de commencer

Vous ne pouvez utiliser une adresse IPv4 que pour identifier un serveur DHCP afin d'attribuer des adresses client. De plus, les options DHCP ne sont pas transférées aux utilisateurs ; ils reçoivent uniquement une attribution d'adresse.

Procédure

Étape 1

Configurez vos serveurs DHCP.

Vous ne pouvez pas attribuer d'adresses IPv6 à Secure Client à l'aide d'un serveur DHCP.

- a) Vérifiez que DHCP est activé dans **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Address Assignment (Attribution d'adresses) > Assignment Policy (Politique d'attribution)**.
- b) Configurez vos serveurs DHCP en sélectionnant **Configuration > Remote Access VPN (VPN d'accès à distance) > DHCP Server (Serveur DHCP)**.

Étape 2

Définissez le serveur DHCP dans le profil de connexion.

- a) Sélectionnez **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Secure ClientConnection Profiles (Profils de connexion Secure Client/AnyConnect)**.
- b) Dans la zone Connection Profiles (Profils de connexion), cliquez sur **Add (Ajouter)** ou **Edit (Modifier)**.
- c) Cliquez sur **Basic** (De base) dans l'arborescence de configuration du profil de connexion.
- d) Dans la zone Client Address Assignment (affectation d'adresses client), saisissez l'adresse IPv4 du serveur DHCP que vous souhaitez utiliser pour attribuer les adresses IP aux clients. Par exemple, **172.33.44.19**.

Étape 3

Modifiez la stratégie de groupe associée au profil de connexion pour définir la portée de DHCP.

- a) Sélectionnez **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Group Policies (Stratégies de groupe)**.
- b) Cliquez deux fois sur la stratégie de groupe que vous souhaitez modifier.
- c) Cliquez sur **Server (Serveur)** dans l'arborescence de configuration.
- d) Développez la zone **More Options** (Plus d'options) en cliquant sur la flèche vers le bas.
- e) Décochez **DHCP Scope Inherit** (Hériter de la portée DHCP) et définissez la portée DHCP.

Si vous configurez des serveurs DHCP pour l'ensemble d'adresses dans le profil de connexion, la portée de DHCP identifie les sous-réseaux à utiliser pour le regroupement pour ce groupe. Le serveur DHCP doit également avoir des adresses dans le même sous-réseau identifié par la portée. La portée vous permet de sélectionner un sous-ensemble des ensembles d'adresses définis dans le serveur DHCP à utiliser pour ce groupe précis.

Si vous ne définissez pas de portée réseau, le serveur DHCP attribue les adresses IP dans l'ordre des ensembles d'adresses configurés. Il parcourt les ensembles jusqu'à ce qu'il identifie une adresse non attribuée.

Pour spécifier une portée, saisissez une adresse routable sur le même sous-réseau que l'ensemble souhaité, mais en dehors de cet ensemble. Le serveur DHCP détermine à quel sous-réseau cette adresse IP appartient et attribue une adresse IP de cet ensemble d'adresses.

Nous vous recommandons d'utiliser l'adresse IP d'une interface chaque fois que cela est possible à des fins de routage. Par exemple, si l'ensemble d'adresses est 10.100.10.2-10.100.10.254 et que l'adresse d'interface est 10.100.10.1/24, utilisez 10.100.10.1 comme portée DHCP. N'utilisez pas le numéro de

réseau. Vous ne pouvez utiliser DHCP que pour l'adressage IPv4. Si l'adresse que vous choisissez n'est pas une adresse d'interface, vous devrez peut-être créer une voie de routage statique pour l'adresse de portée.

- f) Cliquez sur **OK**.
- g) Cliquez sur **Apply** (Appliquer).

Attribuer des adresses IP aux utilisateurs locaux

Les comptes d'utilisateurs locaux peuvent être configurés pour utiliser une stratégie de groupe, et certains attributs Secure Client peuvent également être configurés. Ces comptes d'utilisateurs fournissent un repli si les autres sources d'adresses IP échouent, de sorte que les administrateurs auront toujours un accès.

Avant de commencer

Pour ajouter ou modifier un utilisateur, choisissez **Configuration > Remote Access VPN (VPN d'accès à distance) > AAA/Local Users (AAA/Utilisateurs locaux) > Local Users (Utilisateurs locaux)**, puis cliquez sur **Add (Ajouter)** ou **Edit (Modifier)**.

Par défaut, la case **Inherit** (Hériter) est cochée pour chaque paramètre sur l'écran Edit User Account (Modifier le compte d'utilisateur), ce qui signifie que le compte d'utilisateur hérite de la valeur de ce paramètre de la stratégie de groupe par défaut, DfltGrpPolicy.

Pour remplacer chaque paramètre, décochez la case **Inherit** (Hériter) et saisissez une nouvelle valeur. Les étapes détaillées qui suivent décrivent les paramètres d'adresse IP. Consultez [Configurer les attributs de politique VPN pour un utilisateur local](#) pour les détails complets de configuration.

Procédure

- | | |
|----------------|--|
| Étape 1 | Démarrez ASDM et choisissez Configuration > Remote Access VPN (VPN d'accès à distance) > AAA/Local Users (AAA/Utilisateurs locaux) > Local Users > (Utilisateurs locaux) . |
| Étape 2 | Sélectionnez l'utilisateur que vous souhaitez configurer et cliquez sur Edit (Modifier). |
| Étape 3 | Dans le volet de gauche, cliquez sur VPN Policy (Politique VPN). |
| Étape 4 | Pour définir une adresse IPv4 dédiée à cet utilisateur, saisissez une adresse IPv4 et un masque de sous-réseau dans la zone Adresse IPv4 dédiée (facultatif) . |
| Étape 5 | Pour définir une adresse IPv6 dédiée à cet utilisateur, saisissez une adresse IPv6 avec un préfixe IPv6 dans la zone Adresse IPv6 dédiée (facultatif) . Le préfixe IPv6 indique le sous-réseau sur lequel se trouve l'adresse IPv6. |
| Étape 6 | Cliquez sur Apply (Appliquer) pour enregistrer les modifications apportées à la configuration en cours d'exécution. |

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.