Adresses IP pour les VPN

Configurer une politique d'attribution d'adresses IP

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

- aaa (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. Cette méthode est disponible pour les politiques d'attribution IPv4 et IPv6.
- 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. Cette méthode est disponible pour les politiques d'attribution IPv4.
- **local** les ensembles d'adresses configurés en interne constituent la méthode d'affectation la plus simple à configurer. Si vous choisissez local, vous devez également utiliser la **ip-local-pool** commande pour définir la plage d'adresses IP à utiliser. Cette méthode est disponible pour les politiques d'attribution IPv4 et IPv6.
  - Allow the reuse of an IP address so many minutes after it is released (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 l'ASA n'applique pas de délai. 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 adresses IPv4

Procédure

Activez une méthode d'affectation d'adresse que l'ASA utilise lors de l'affectation d'une adresse IPv4 aux connexions VPN. Les méthodes disponibles pour obtenir une adresse IP sont celles d'un serveur AAA, d'un serveur DHCP ou d'un ensemble d'adresses locales. Ceux-ci sont activés par défaut.

vpn-addr-assign {**aaa** | **dhcp** | **local** [**reuse-delay** *minutes*]}

Exemple :

Par exemple, vous pouvez configurer la réutilisation d'une adresse IP entre 0 et 480 minutes après la libération de l'adresse IP.

```
hostname(config)#vpn-addr-assign aaa
hostname(config)#vpn-addr-assign local reuse-delay 180
```

Cet exemple utilise la forme no de la commande pour désactiver une méthode d'affectation d'adresse.

```
hostname(config)# no vpn-addr-assign dhcp
```

Configurer l'attribution des adresses IPv6

Procédure

Activez une méthode d'attribution d'adresse que l'ASA utilise lors de l'affectation d'une adresse IPv6 aux connexions VPN. Les méthodes disponibles pour obtenir une adresse IP proviennent d'un serveur AAA ou d'un ensemble d'adresses locales. Ces deux méthodes sont activées par défaut.

ipv6-vpn-addr-assign {**aaa** | local}

Exemple :

```
hostname(config)# ipv6-vpn-addr-assign aaa
```

Cet exemple utilise la forme no de la commande pour désactiver une méthode d'affectation d'adresse.

```
hostname(config)# no ipv6-vpn-addr-assign local
```

Afficher les méthodes d'attribution d'adresses

Procédure

Utilisez l'une de ces méthodes pour afficher la méthode d'affectation d'adresse configurée sur l'ASA :

- Afficher les affectations d'adresses IPv4

  Afficher la méthode d'affectation d'adresse configurée. La méthode d'adresse configurée peut être AAA, DHCP ou locale.

  ```
  show running-config all vpn-addr-assign
  vpn-addr-assign aaa
  vpn-addr-assign dhcp
  vpn-addr-assign local
  ```

- Afficher les affectations d'adresses IPv6

  Afficher la méthode d'affectation d'adresse configurée. Les méthodes d'adresse configurées peuvent être AAA ou locales.

  ```
  show running-config all ipv6-vpn-addr-assign
  ipv6-vpn-addr-assign aaa
  ipv6-vpn-addr-assign local reuse-delay 0
  ```

Configurer les ensembles d'adresses IP locales

Pour configurer les ensembles d'adresses IPv4 à utiliser pour les tunnels VPN d'accès à distance, saisissez la commande **ip local pool** en mode de configuration globale. Pour supprimer des ensembles d'adresses, saisissez la forme **no** de cette commande.

Pour configurer les ensembles d'adresses IPv6 à utiliser pour les tunnels VPN d'accès à distance, saisissez la commande **ipv6 local pool** en mode de configuration globale. Pour supprimer des ensembles d'adresses, saisissez la forme **no** de cette commande.

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.

Remarque Lorsque vous modifiez des ensembles d'adresses existants actuellement utilisés dans un groupe de tunnels actif (c'est-à-dire ouvert aux utilisateurs finaux pour les connexions), vous devez effectuer la modification dans une fenêtre de maintenance et vous assurer de ce qui suit :

- Les utilisateurs connectés sont déconnectés.
- Les ensembles d'adresses sont supprimés du groupe de tunnels et modifiés au besoin.
- Les ensembles d'adresses modifiés sont ensuite rajoutés dans le groupe de tunnels.

Si un ensemble d'adresses n'est pas modifié de cette manière, il peut entraîner des incohérences dans le comportement de l'ASA.

Configurer les ensembles d'adresses IPv4 locales

Remarque Lorsque vous souhaitez modifier dans l'interface de ligne de commande un ensemble d'adresses existant actuellement utilisé dans un groupe de tunnels actif (c'est-à-dire ouvert aux utilisateurs finaux pour les connexions), il est recommandé d'effectuer cette modification pendant une fenêtre de changement. Les utilisateurs connectés doivent être déconnectés, l'ensemble d'adresses doit être supprimé du groupe de tunnels, modifié au besoin, puis ajouté de nouveau au groupe de tunnels. Si cela n'est pas fait de cette manière, des incohérences peuvent se produire dans le comportement de l'ASA.

Procédure

Étape 1 Configurez les ensembles d'adresses IP comme méthode d'attribution d'adresses. Saisissez la commande **vpn-addr-assign** avec l'argument **local**.

Exemple :

```
hostname(config)# vpn-addr-assign local
```

Étape 2 Configurez un ensemble d'adresses. La commande nomme l'ensemble, précise une plage d'adresses IPv4 et le masque de sous-réseau.

ip local pool*poolname first_address-last_address***mask***mask*

Exemple :

Cet exemple configure un ensemble d'adresses IP nommé *firstpool*. L'adresse de début est 10.20.30.40 et l'adresse de fin est 10.20.30.50. Le masque de sous-réseau est 255.255.255.0.

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

Cet exemple supprime l'ensemble d'adresses IP nommé **firstpool**.

```
hostname(config)# no ip local pool firstpool
```

Configurer les ensembles d'adresses IPv6 locaux

Procédure

Étape 1 Pour configurer les ensembles d'adresses IP comme méthode d'affectation, saisissez la commande ipv6-**vpn-addr-assign** avec l'argument **local**.

Exemple :

```
hostname(config)# ipv6-vpn-addr-assign local
```

Étape 2 Configurez l'ensemble d'adresses. La commande nomme l'ensemble, identifie l'adresse IPv6 de départ, la longueur du préfixe en bits et le nombre d'adresses à utiliser dans la plage.

ipv6 local pool *pool_name starting_address prefix_length number_of_addresses*

Exemple :

Cet exemple configure un ensemble d'adresses IP nommé *ipv6pool*. L'adresse de départ est 2001:DB8::1, la longueur du préfixe est de 32 bits et le nombre d'adresses à utiliser dans l'ensemble est de 100.

```
hostname(config)# ipv6 local pool ipv6pool 2001:DB8::1/32 100
```

Cet exemple supprime l'ensemble d'adresses IP nommé *ipv6ensemble*.

```
hostname(config)# no ipv6 local pool ipv6pool
```

Configurer l'adressage AAA

Pour utiliser un serveur AAA afin d'attribuer des adresses aux clients d'accès à distance VPN, vous devez d'abord configurer un serveur ou un groupe de serveurs AAA. Consultez la commande **aaa-server protocol** dans la référence de commande.

En outre, l'utilisateur doit correspondre à un profil de connexion configuré pour l'authentification RADIUS.

Les exemples suivants illustrent comment définir un groupe de serveurs AAA appelé RAD2 pour le groupe de tunnels nommé FirstGroup. Il comprend une étape de plus que nécessaire, en ce que vous avez peut-être nommé le groupe de tunnels et défini le type de groupe de tunnels. Cette étape s'affiche dans l'exemple suivant pour vous rappeler que vous n'avez pas accès aux commandes de groupe de tunnels suivantes tant que vous n'avez pas défini ces valeurs.

Voici un aperçu de la configuration créée par ces exemples :

```
hostname(config)# vpn-addr-assign aaa
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config)# authentication-server-group RAD2
```

Pour configurer AAA pour l'adressage IP, procédez comme suit :

Procédure

Étape 1 Pour configurer AAA comme méthode d'affectation d'adresses, entrez la commande **vpn-addr-assign** avec l'argument **aaa** :

```
hostname(config)# vpn-addr-assign aaa
hostname(config)#
```

Étape 2 Pour établir le groupe de tunnels appelé FirstGroup en tant que groupe de tunnels d'accès à distance ou LAN à LAN, saisissez la commande **tunnel-group** avec le mot-clé **type**. L'exemple suivant configure un groupe de tunnels d'accès à distance.

```
hostname(config)# tunnel-group firstgroup type ipsec-ra
hostname(config)#
```

Étape 3 Pour passer en mode de configuration d'attributs généraux, qui vous permet de définir un groupe de serveurs AAA pour le groupe de tunnels appelé FirstGroup, saisissez la commande **tunnel-group** avec l'argument **general-attributes**.

```
hostname(config)# tunnel-group firstgroup general-attributes
hostname(config-general)#
```

Étape 4 Pour préciser le groupe de serveurs AAA à utiliser pour l'authentification, saisissez la commande **authentication-server-group**.

```
hostname(config-general)# authentication-server-group RAD2
hostname(config-general)#
```

Prochaine étape

Cette commande comporte plus d'arguments que cet exemple inclut. Consultez la référence de commande pour en savoir plus.

Configurer l'adressage DHCP

Pour utiliser le 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 réseau DHCP dans la stratégie de groupe associée à un profil de connexion ou à 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 réseau DHCP de 10.100.10.1 pour la stratégie de groupe nommée **remotegroup**. (La stratégie de groupe nommée remotegroup est associée au profil de connexion nommé 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 les ensembles d'adresses IP comme méthode d'attribution d'adresses.

vpn-addr-assign dhcp

Étape 2 Définissez le profil de connexion appelé **firstgroup** comme profil de connexion d'accès à distance.

tunnel-group firstgroup type remote-access

Étape 3 Entrez en mode de configuration general-attributes pour le profil de connexion afin de pouvoir configurer un serveur DHCP.

tunnel-group firstgroup general-attributes

Étape 4 Définissez le serveur DHCP au moyen de son adresse IPv4, puis quittez le mode de configuration tunnel-group.

dhcp-server *IPv4_address_of_DHCP_server*

Vous ne pouvez pas définir un serveur DHCP au moyen d'une adresse IPv6. Vous pouvez préciser plusieurs adresses de serveur DHCP pour un profil de connexion. Entrez la commande dhcp-server. Cette commande vous permet de configurer l'ASA pour envoyer des options supplémentaires aux serveurs DHCP précisés lorsqu'il tente d'obtenir des adresses IP pour les clients VPN.

Exemple :

L'exemple configure un serveur DHCP à l'adresse IP 172.33.44.19. Ensuite, quittez le mode de configuration tunnel-group.

```
hostname(config-general)# dhcp-server 172.33.44.19
hostname(config-general)# exit
hostname(config)#
```

Étape 5 Si le groupe n'existe pas déjà, créez une stratégie de groupe interne appelée **remotegroup**.

```
hostname(config)# group-policy remotegroup internal
```

Étape 6 (Facultatif) Entrez en mode de configuration des attributs group-policy et définissez la portée réseau DHCP.

dhcp-network-scope *ip_address*

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.

Remarque

Pour préciser une portée, entrez une adresse routable sur le même sous-réseau que l'ensemble d'adresses souhaité, mais à l'extérieur 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.

Exemple :

L'exemple suivant passe en mode de configuration des attributs pour remotegroup et définit la portée DHCP à 10.100.10.1.

```
hostname(config)# group-policy remotegroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.100.10.1
```

Exemple

Voici un résumé de la configuration créée par ces exemples :

```
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 10.100.10.1
```

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.

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.

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.