Déploiements avancés du VPN AnyConnect pour Firepower Threat Defense avec FMC

Dernière modification : 2025-05-28

Déploiements avancés du VPN AnyConnect pour Firepower Threat Defense avec FMC

Ce document explique comment déployer le VPN AnyConnect avancé pour Cisco FTD sur Cisco FMC à l'aide de FlexConfig, y compris la tunnellisation fractionnée dynamique et les cartes d'attributs LDAP.

Tunnellisation fractionnée dynamique

Les rubriques suivantes expliquent la tunnellisation fractionnée dynamique pour Cisco Firepower Threat Defense (FTD) et comment la configurer à l'aide de FlexConfig dans Cisco Firepower Management Center (FMC) 6.4. Cette configuration peut s'appliquer aux versions ultérieures qui ne prennent pas directement en charge la tunnellisation fractionnée dynamique.

À propos de la tunnellisation fractionnée dynamique

La tunnellisation fractionnée statique implique de définir les adresses IP des hôtes et des réseaux qui doivent être inclus ou exclus du tunnel VPN d'accès à distance. Vous pouvez améliorer la tunnellisation fractionnée en définissant la tunnellisation fractionnée dynamique.

La tunnellisation fractionnée dynamique vous permet d'affiner le tunnellisation fractionnée en fonction des noms de domaine DNS. Étant donné que les adresses IP associées aux noms de domaine complets (FQDN) peuvent changer ou simplement différer selon la région, la définition de tunnellisation fractionnée en fonction des noms DNS offre une définition plus dynamique de quel trafic doit être inclus ou ne doit pas être inclus dans le tunnel de VPN d'accès à distance. Si des adresses renvoyées en raison de noms de domaine exclus se trouvent dans l'ensemble d'adresses inclus dans le VPN, elles seront exclues.

Les domaines exclus ne sont pas bloqués. Au lieu de cela, le trafic vers ces domaines est conservé en dehors du tunnel VPN. Par exemple, vous pourriez envoyer du trafic à Cisco Webex sur l'Internet public, libérant ainsi de la bande passante de votre tunnel VPN pour le trafic ciblant les serveurs de votre réseau protégé.

Vous pouvez configurer cette fonctionnalité en utilisant l'IU de FMC à partir des versions 7.0 ou ultérieures. Pour plus d'informations sur la configuration de cette fonctionnalité, consultez Configurer la tunnellisation fractionnée dynamique AnyConnect sur FTD géré par FMC. Pour les anciennes versions de FMC, vous devez le configurer à l'aide de FlexConfig, comme indiqué dans Configurer la tunnellisation fractionnée dynamique en utilisant FlexConfig, à la page 1.

Configurer la tunnellisation fractionnée dynamique en utilisant FlexConfig

La configuration du tunnel fractionné dynamique est basée sur la création d'un attribut AnyConnect personnalisé du type **dynamique-split-exclude-domains**, puis sur l'ajout de cet attribut aux politiques de groupe utilisées dans vos profils de connexion VPN d'accès à distance.

Notez que vous pouvez également créer un attribut personnalisé **dynamic-split-include-domains** pour définir les domaines à inclure dans le tunnel qui seraient autrement exclus en fonction de l'adresse IP. Cependant, cet exemple envisage d'exclure les domaines.

Avant de commencer

Cette configuration requiert au moins AnyConnect 4.5.

Cet exemple suppose que vous ayez déjà configuré le VPN d'accès à distance et qu'il fonctionne correctement. Cela inclut la création des politiques de groupe auxquelles vous ajoutez l'attribut de tunnellisation fractionnée dynamique. N'utilisez pas FlexConfig pour créer la politique de groupe, utilisez-le pour modifier une politique de groupe existante uniquement.

Vous n'avez pas besoin d'avoir configuré la tunnellisation fractionnée basée sur l'adresse IP statique lorsque vous définissez une liste d'exclusion dynamique. Cependant, si vous décidez de créer une liste d'inclusion dynamique, vous devez avoir activé la tunnellisation fractionnée et exclu certaines adresses IP. La tunnellisation fractionnée dynamique pour inclure des domaines n'a de sens que si vous incluez du trafic qui serait autrement exclu dans une situation de tunnellisation fractionnée basée sur l'adresse IP.

Procédure

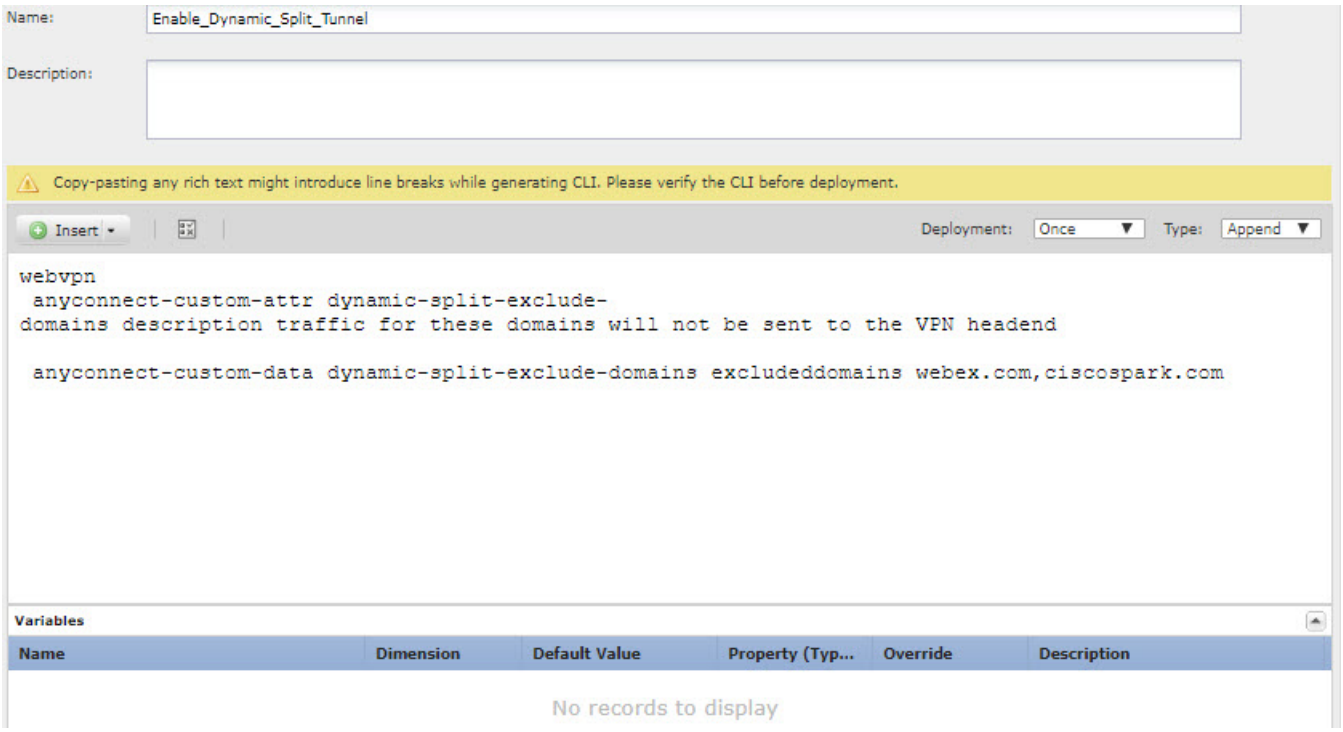
Étape 1 Créez l'objet FlexConfig deploy-once/append qui crée l'attribut personnalisé de tunnellisation fractionnée dynamique et affecte à l'attribut les noms de domaine qui doivent être exclus du tunnel VPN et être plutôt envoyés sur l'Internet public.

a) Choisissez **Objects** > **Object Management** (Objets, Gestion des objets).
b) Choisissez **FlexConfig** > **FlexConfig Object** (FlexConfig, Objets FlexConfig) dans la table des matières.
c) Cliquez sur **Add FlexConfig Object** (Ajouter un objet FlexConfig), configurez les propriétés suivantes, puis cliquez sur **Save** (Enregistrer).

- **Name** : nom de l'objet. Par exemple, Enable_Dynamic_Split_Tunnel.
- **Deployment** (Déploiement) : sélectionnez **Once** (une fois). Ces commandes doivent être configurées une seule fois.
- **Type** : conservez la valeur par défaut, **Append** (Ajouter). Les commandes sont envoyées à l'appareil après les commandes des fonctionnalités directement prises en charge.
- **Object body** (Corps de l'objet) : dans le corps de l'objet, saisissez les commandes requises pour créer un attribut du type **dynamique-split-exclude-domains**, puis ajoutez les données, qui sont un nom d'attribut et une liste des noms de domaine à exclure. Par exemple, pour créer un attribut nommé excludeddomains (domaines exclus) et pour exclure les domaines webex.com et ciscospark.com, les commandes seraient les suivantes. Notez que la description est facultative, mais si elle est incluse, il ne s'agit pas d'une commande distincte, mais fait partie de la commande **anyconnect-custom-attr**. Pour les noms de domaine, séparez-les par une virgule, mais n'incluez pas d'espaces.

```
webvpn
 anyconnect-custom-attr dynamic-split-exclude-domains description traffic for these
 domains will not be sent to the VPN headend
 anyconnect-custom-data dynamic-split-exclude-domains excludeddomains
webex.com,ciscospark.com
```

Le corps de l'objet doit ressembler à ce qui suit :



Étape 2 (Recommandé.) Si vous utilisez des politiques de groupe personnalisées, créez un objet FlexConfig deploy-once/append pour configurer l'attribut personnalisé de tunnellisation fractionnée dynamique dans les politiques de groupe.

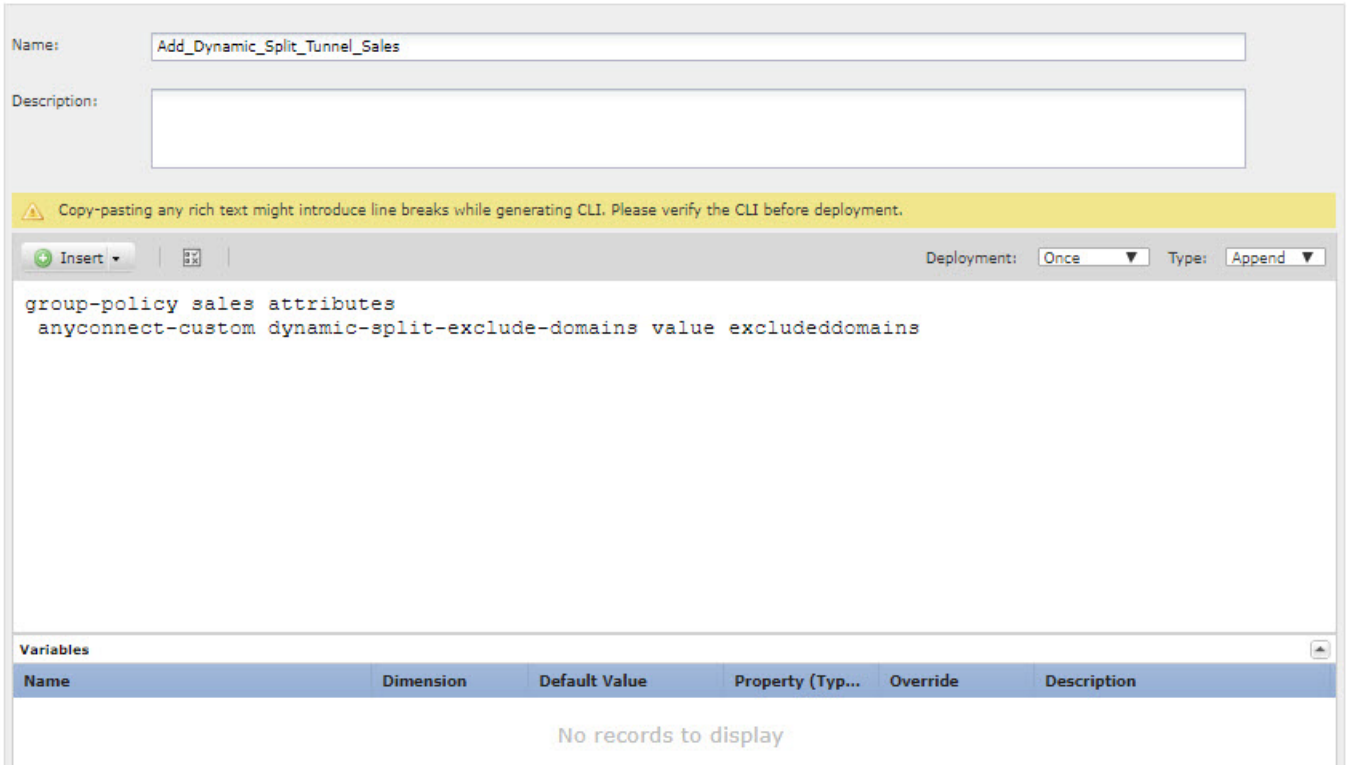
Le système n'annulera pas les modifications que vous apportez aux politiques de groupe personnalisées. Vous devez donc déployer les modifications une fois. Si vous utilisez plusieurs politiques de groupe, vous pouvez utiliser un seul objet FlexConfig pour ajouter l'attribut personnalisé à chaque politique à tour de rôle. Vous pouvez également créer un objet FlexConfig par politique de groupe. Le résultat sera le même, le choix dépendra donc de vos propres exigences pour la modularisation de votre politique FlexConfig.

Sur la page des objets FlexConfig, Cliquez sur **Add FlexConfig Object** (Ajouter un objet FlexConfig), configurez les propriétés suivantes, puis cliquez sur **Save** (Enregistrer).

- **Name** : nom de l'objet. Par exemple, Add_Dynamic_Split_Tunnel_Sales.
- **Deployment** (Déploiement) : sélectionnez **Once** (une fois).
- **Type** : conservez la valeur par défaut, **Append** (Ajouter).
- **Object body** (Corps de l'objet) : dans le corps de l'objet, tapez les commandes requises pour ajouter l'attribut personnalisé à la politique de groupe. Par exemple, si l'attribut que vous avez créé s'intitulecludeddomains (domaines exclus) et que la politique de groupe s'intitule « sales » (ventes), les commandes sont les suivantes :

```
group-policy sales attributes
 anyconnect-custom dynamic-split-exclude-domains value excludeddomains
```

Le corps de l'objet doit ressembler à ce qui suit :



Étape 3 (Non recommandé). Si vous utilisez la politique de groupe par défaut, nommée DfltGrpPolicy, créez un objet FlexConfig deploy-everytime/append pour configurer l'attribut personnalisé de tunnellisation fractionnée dynamique dans la politique de groupe.

Vous devez déployer cet objet à chaque fois, car lors de chaque déploiement, le système annulera toute modification personnalisée de la politique par défaut.

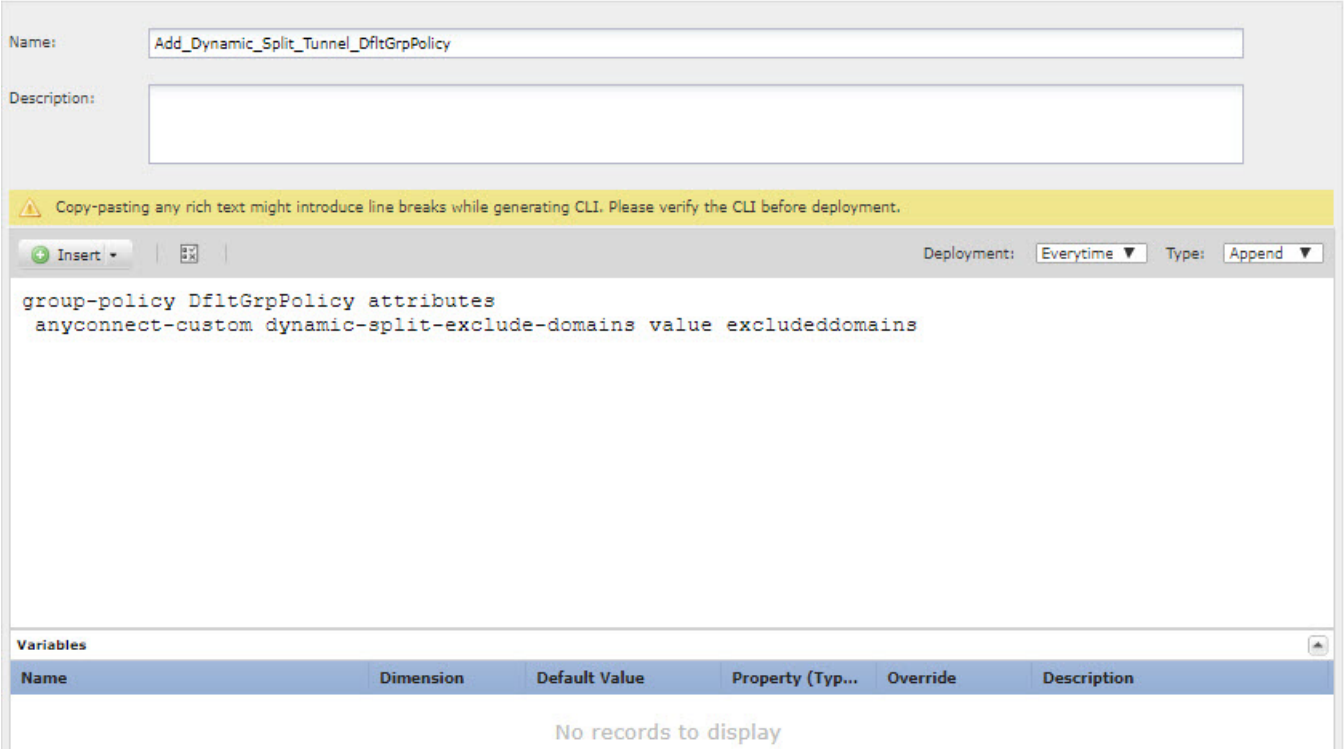
Nous vous recommandons de créer des politiques de groupe personnalisées plutôt que d'utiliser DfltGroupPolicy.

Sur la page des objets FlexConfig, Cliquez sur **Add FlexConfig Object** (Ajouter un objet FlexConfig), configurez les propriétés suivantes, puis cliquez sur **Save** (Enregistrer).

- **Name** : nom de l'objet. Par exemple, Add_Dynamic_Split_Tunnel_DfltGrpPolicy.
- **Deployment** (déploiement) : sélectionnez **Anytime** (À tout moment). Ces commandes doivent être configurées une seule fois.
- **Type** : conservez la valeur par défaut, **Append** (Ajouter). La commande doit être envoyée après que le système a annulé les attributs personnalisés dans la politique de groupe par défaut.
- **Object body** (Corps de l'objet) : dans le corps de l'objet, tapez les commandes requises pour ajouter l'attribut personnalisé à la politique de groupe. Par exemple, si l'attribut que vous avez créé s'int), les commandes sont les suivantes :

```
group-policy DfltGrpPolicy attributes
 anyconnect-custom dynamic-split-exclude-domains value excludeddomains
```

Le corps de l'objet doit ressembler à ce qui suit :



Étape 4 Créez la politique FlexConfig qui déploie ces objets.

a) Sélectionnez **Devices** > **FlexConfig** (Appareils, FlexConfig).

b) Cliquez sur **New Policy** (Nouvelle politique) ou si une politique FlexConfig existante doit être affectée (ou est déjà affectée) aux appareils cibles, modifiez simplement cette dernière.

Lors de la création d'une nouvelle politique, affectez les appareils cibles à la politique dans la boîte de dialogue où vous nommez la politique.

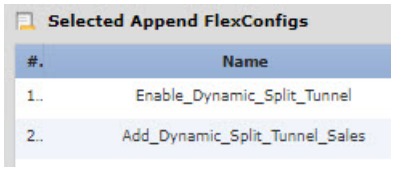
c) Utilisez Ctrl+clic pour sélectionner l'objet FlexConfig dans le dossier **User Defined** (Défini par l'utilisateur) dans la table des matières, puis cliquez sur > pour l'ajouter à la politique.

Les objets doivent être ajoutés à la liste **Selected Appended FlexConfigs** (FlexConfigs sélectionnées et ajoutées).

d) Utilisez le glisser-déposer pour vous assurer que les objets sont dans le bon ordre.

L'objet qui crée l'objet d'attribut personnalisé doit venir avant les objets qui attribuent cet attribut aux politiques de groupe. Sinon, si vous essayez d'ajouter un attribut personnalisé qui n'existe pas encore, vous obtiendrez une erreur.

La liste devrait ressembler à ce qui suit si vous avez un seul objet qui configure vos politiques de groupe personnalisées :



e) Cliquez sur **Save** (Enregistrer).

f) Si vous n'avez pas encore affecté tous les périphériques ciblés à la politique, cliquez sur le lien **Policy Affectations** (Affectations de politiques) ci-dessous Save and make the assignments now (Enregistrer et effectuer les affectations maintenant).

g) Cliquez sur **Preview Config** (Aperçu de la configuration et dans la boîte de dialogue d'aperçu, sélectionnez l'un des périphériques attribués.

Le système génère un aperçu de l'interface de ligne de commande de configuration qui sera envoyée au périphérique. Vérifiez que les commandes générées à partir de l'objet semblent correctes. Celles-ci seront affichées à la fin de l'aperçu. Notez que vous verrez également les commandes générées à partir d'autres modifications que vous avez apportées aux fonctionnalités gérées. Pour les commandes de tunnellisation fractionnée dynamique, vous devriez voir quelque chose de similaire à ce qui suit :

```
###Flex-config Appended CLI ###
webvpn
 anyconnect-custom-attr dynamic-split-exclude-domains description traffic for these
domains will not be sent to the VPN headend
 anyconnect-custom-data dynamic-split-exclude-domains excludeddomains
webex.com,ciscospark.com
group-policy sales attributes
 anyconnect-custom dynamic-split-exclude-domains value excludeddomains
```

Étape 5 Déployez vos modifications.

Étape 6 Vérifiez la configuration.

- Vous pouvez vérifier que les commandes ont été configurées sur chaque appareil FTD. Utilisez une session SSH avec l'appareil ou avec l'outil CLI dans FMC (**System** > **Health** > **Monitor** [Système, Intégrité, Vérifier], cliquez sur l'appareil, puis sur **Advanced Troubleshooting** [Dépannage avancé], puis sélectionnez l'onglet **Threat Defense CLI**). Voici les commandes qui afficheront la configuration.
  - **show running-config webvpn**
  - **show running-config anyconnect-custom-data**
  - **show running-config group-policy** *name*, (nom), où vous remplacez *name* par un nom de politique de groupe tel que sales (ventes).
- Vous pouvez vérifier que le système se comporte correctement à partir d'un client AnyConnect. Ouvrez les statistiques du client. Le champ **Dynamic Tunnel Exclusions** (Exclusions de tunnel dynamique) devrait afficher la liste des noms de domaine que vous excluez.

Retirer la tunnellisation fractionnée dynamique en utilisant FlexConfig

Si vous ne souhaitez plus utiliser la tunnellisation fractionnée, vous devez créer un objet FlexConfig pour retirer la configuration des appareils sur lesquels vous avez déployé la fonctionnalité. Le simple retrait des objets FlexConfig de la politique FlexConfig n'est pas suffisant.

Procédure

Étape 1 Créez l'objet FlexConfig deploy-once/append qui supprime l'attribut personnalisé de chaque politique de groupe qui l'utilise, puis supprime l'attribut.

Vous devez d'abord supprimer l'attribut des politiques personnalisées avant de le supprimer. Si vous essayez de supprimer un attribut en cours d'utilisation, le système vous en empêchera et vous verrez une erreur de déploiement. Vous devez donc insérer les commandes dans le bon ordre pour que cet objet fonctionne correctement.

a) Choisissez **Objects** > **Object Management** (Objets, Gestion des objets).
b) Choisissez **FlexConfig** > **FlexConfig Object** (FlexConfig, Objets FlexConfig) dans la table des matières.
c) Cliquez sur **Add FlexConfig Object** (Ajouter un objet FlexConfig), configurez les propriétés suivantes, puis cliquez sur **Save** (Enregistrer).

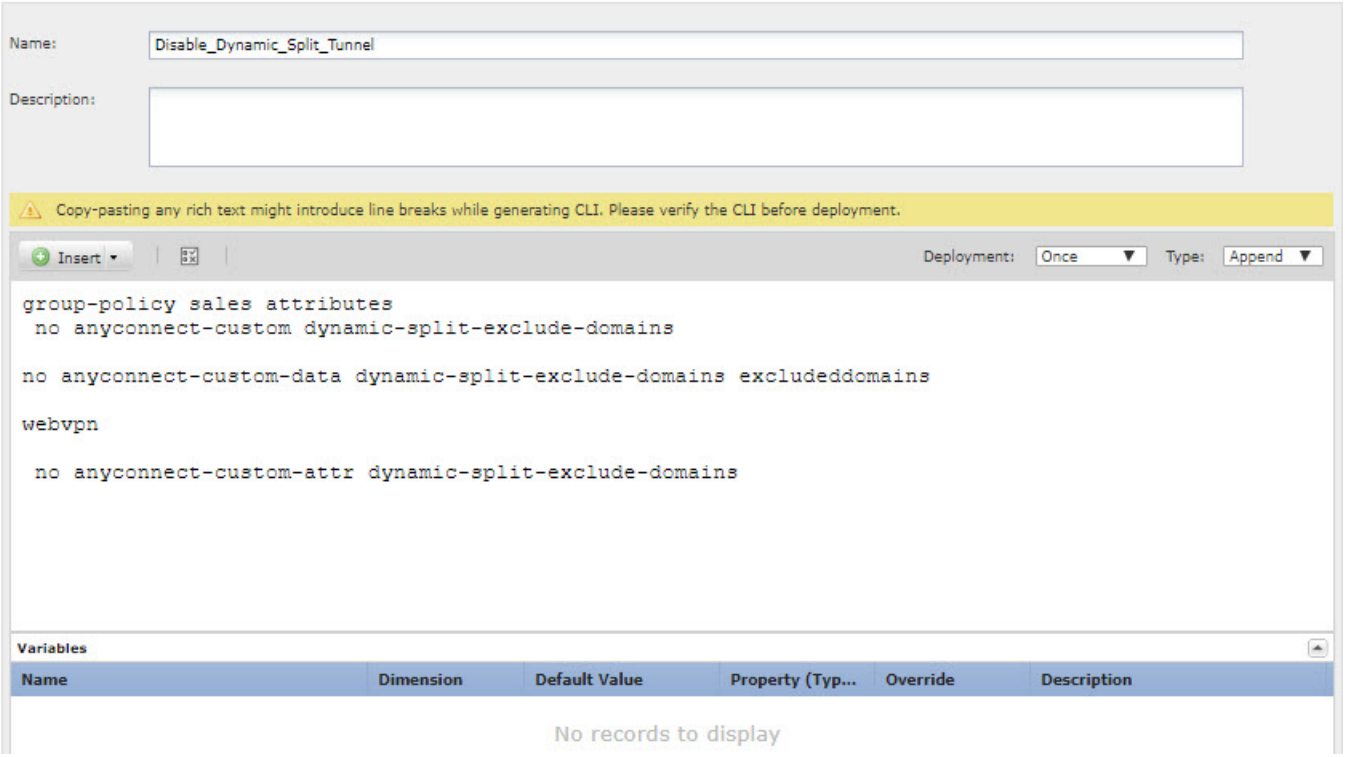
- **Name** : nom de l'objet. Par exemple, Disable_Dynamic_Split_Tunnel.
- **Deployment** (Déploiement) : sélectionnez **Once** (une fois). Ces commandes doivent être configurées une seule fois.
- **Type** : conservez la valeur par défaut, **Append** (Ajouter). Les commandes sont envoyées à l'appareil après les commandes des fonctionnalités directement prises en charge.
- **Object body** (Corps de l'objet): dans le corps de l'objet, tapez les commandes requises pour supprimer l'attribut personnalisé de chaque politique de groupe qui l'utilise, puis supprimez l'attribut personnalisé. Par exemple, si l'attribut personnalisé est utilisé par les politiques de groupes de ventes et que l'attribut est excludeddomains, les commandes seraient les suivantes :

```
group-policy sales attributes
 no anyconnect-custom dynamic-split-exclude-domains

no anyconnect-custom-data dynamic-split-exclude-domains excludeddomains

webvpn
 no anyconnect-custom-attr dynamic-split-exclude-domains
```

Le corps de l'objet doit ressembler à ce qui suit :



Étape 2 Modifiez la politique FlexConfig pour retirer les objets de tunnellisation fractionnée dynamique et ajoutez l'objet qui retire la configuration.

a) Sélectionnez **Devices** > **FlexConfig** (Appareils, FlexConfig).

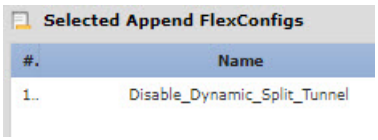
b) Modifiez la politique FlexConfig

c) Dans la liste **Selected Appended FlexConfigs** (FlexConfigs ajoutés sélectionnés), cliquez sur l'icône de suppression pour chacun des objets de tunnellisation fractionnée dynamique, ceux qui activent l'attribut personnalisé, puis l'ajoutent à l'attribut aux politiques de groupe.

d) Sélectionnez l'objet FlexConfig qui désactive la tunnellisation fractionnée dynamique dans le dossier **User Defined** (défini par l'utilisateur) dans la table des matières, puis cliquez sur > pour l'ajouter à la politique.

L'objet doit être ajouté à la liste **Selected Appended FlexConfigs** (FlexConfigs sélectionnées et ajoutées).

La liste devrait ressembler à ce qui suit :



e) Cliquez sur **Save** (Enregistrer).

f) Cliquez sur **Preview Config** (Aperçu de la configuration et dans la boîte de dialogue d'aperçu, sélectionnez l'un des périphériques attribués.

Le système génère un aperçu de l'interface de ligne de commande de configuration qui sera envoyée au périphérique. Vérifiez que les commandes générées à partir de l'objet semblent correctes. Celles-ci seront affichées à la fin de l'aperçu. Notez que vous verrez également les commandes générées à partir d'autres

modifications que vous avez apportées aux fonctionnalités gérées. Pour les commandes de tunnellisation fractionnée dynamique, vous devriez voir quelque chose de similaire à ce qui suit :

```
###Flex-config Appended CLI ###
group-policy sales attributes
 no anyconnect-custom dynamic-split-exclude-domains

no anyconnect-custom-data dynamic-split-exclude-domains excludeddomains

webvpn
 no anyconnect-custom-attr dynamic-split-exclude-domains
```

Étape 3 Déployez vos modifications.

Cartes d'attributs LDAP pour la configuration AnyConnect

Si vous utilisez Active Directory (AD)/LDAP pour authentifier les utilisateurs du VPN d'accès à distance, vous pouvez utiliser les mappages d'attributs LDAP pour ajuster la configuration et le comportement AnyConnect en fonction des attributs retournés par le serveur AD/LDAP.

À propos des cartes d'attribut LDAP

Une carte des attributs LDAP assimile les attributs qui existent dans Active Directory (AD) ou le serveur LDAP avec des noms d'attribut Cisco. Lorsque le serveur AD ou LDAP renvoie l'authentification à l'appareil FTD lors de l'établissement de la connexion VPN d'accès à distance, le périphérique FTD peut utiliser les informations pour ajuster la façon dont le client AnyConnect termine la connexion.

Par exemple, vous pouvez mapper l'attribut AD/LDAP **memberOf** à l'attribut Cisco **Group-Policy**. Vous devez ensuite associer les valeurs que vous obtenez d'AD/LDAP aux noms des politiques de groupe du VPN d'accès à distance que vous avez définies pour le VPN. Si l'appareil FTD trouve un attribut de politique de groupe pour un utilisateur, AnyConnect tentera d'établir la connexion VPN d'accès à distance en utilisant ce nom de politique de groupe.

Après avoir créé une mise en correspondance d'attributs LDAP, vous l'associez à la configuration du serveur AD/LDAP. Ainsi, vous pouvez avoir différentes cartes pour différents serveurs AD/LDAP : les cartes ne sont pas liées directement au profil de connexion VPN d'accès à distance ni aux politiques de groupe.

Vous pouvez trouver une liste des attributs Cisco pris en charge pour l'autorisation LDAP dans le Guide de configuration ASA 8.4/8.6, https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/ref_extserver.html#pgfId-1773708.

Vous pouvez configurer cette fonctionnalité en utilisant l'IU de FMC à partir des versions 6.7 ou ultérieures. Pour en savoir plus, consultez Configurer le VPN d'accès à distance avec l'authentification et l'autorisation LDAP pour FTD. Pour les anciennes versions de FMC, vous devez le configurer à l'aide de FlexConfig, comme indiqué dans Contrôler l'utilisation de la politique de groupe avec les cartes d'attribut LDAP, à la page 9.

Contrôler l'utilisation de la politique de groupe avec les cartes d'attribut LDAP

Une utilisation typique des cartes d'attributs LDAP consiste à contrôler la politique de groupe qui est affectée à un utilisateur en fonction de l'appartenance au groupe AD/LDAP de l'utilisateur. Pour ce faire, vous mappez les valeurs de l'attribut **memberOf** AD/LDAP aux valeurs de l'attribut Cisco **Group-Policy**.

En tant qu'aperçu, pour utiliser une carte LDAP, vous devez :

1. Créez la carte à l'aide de la commande **ldap attribute-map** *name*, où *name* est le nom de la carte, et non le nom d'un attribut.
2. Mappez un attribut AD/LDAP à un attribut Cisco, par nom, à l'aide de la commande **map-name** *ldap_attribute_name Cisco_attribute_name*.
3. Mappez les valeurs que vous vous attendez à voir dans l'attribut AD/LDAP aux valeurs pertinentes dans l'attribut Cisco, à l'aide de la commande **map-value** *ldap_attribute_name ldap_value Cisco_value*.
4. Associez la carte d'attributs LDAP à un ou plusieurs serveurs AD/LDAP à l'aide de la commande **ldap-attribute-map** *name*. Remarquez la différence subtile entre la commande qui ajoute une carte au serveur AD/LDAP et la commande qui crée la carte elle-même. La seule différence est que la commande complète est mise en tiret, tandis que la commande de base qui crée la carte est simplement **ldap**. Notez que vous devez utiliser la commande **aaa-server** *name* **host** *server_address* pour entrer dans le bon mode et associer la carte.

La procédure suivante explique le processus de bout en bout.

Avant de commencer

Cette procédure devrait fonctionner avec toutes les versions AnyConnect.

Cet exemple suppose que vous ayez déjà configuré le VPN d'accès à distance et qu'il fonctionne correctement. Le VPN doit utiliser AD/LDAP comme serveur d'authentification, et cela doit être configuré. Vous devez également configurer toutes les politiques de groupe : ne les configurez pas dans FlexConfig.

L'objectif est de mapper les utilisateurs aux politiques de groupe de VPN d'accès à distance suivantes :

- Les utilisateurs des gestionnaires APP-SSL-VPN (AD/LDAP) doivent utiliser la politique de groupe nommée LabAdminAccessGroupPolicy.
- Les utilisateurs d'ingénierie (AD/LDAP) doivent utiliser la politique de groupe nommée VPNAccessGroupPolicy.

Procédure

Étape 1 Créez l'objet FlexConfig deploy-once/append qui crée la carte LDAP, y compris les mappages d'attributs/valeurs. Cet objet crée la carte uniquement, il n'affecte pas la carte à un serveur AD/LDAP.

a) Choisissez **Objects** > **Object Management** (Objets, Gestion des objets).
b) Choisissez **FlexConfig** > **FlexConfig Object** (FlexConfig, Objets FlexConfig) dans la table des matières.
c) Cliquez sur **Add FlexConfig Object** (Ajouter un objet FlexConfig), configurez les propriétés suivantes, puis cliquez sur **Save** (Enregistrer).

- **Name** : nom de l'objet. Par exemple, Create_LDAP_Map_for_VPN_Access.
- **Deployment** (Déploiement) : sélectionnez **Once** (une fois). Ces commandes doivent être configurées une seule fois.
- **Type** : conservez la valeur par défaut, **Append** (Ajouter). Les commandes sont envoyées à l'appareil après les commandes des fonctionnalités directement prises en charge.

- **Object body** (Corps de l'objet) : dans le corps de l'objet, tapez les commandes requises pour créer la carte LDAP, mapper l'attribut AD/LDAP à un attribut Cisco, puis mapper les valeurs de cet attribut (comme retourné par AD/LDAP) aux valeurs qui sont significatifs de l'attribut Cisco.

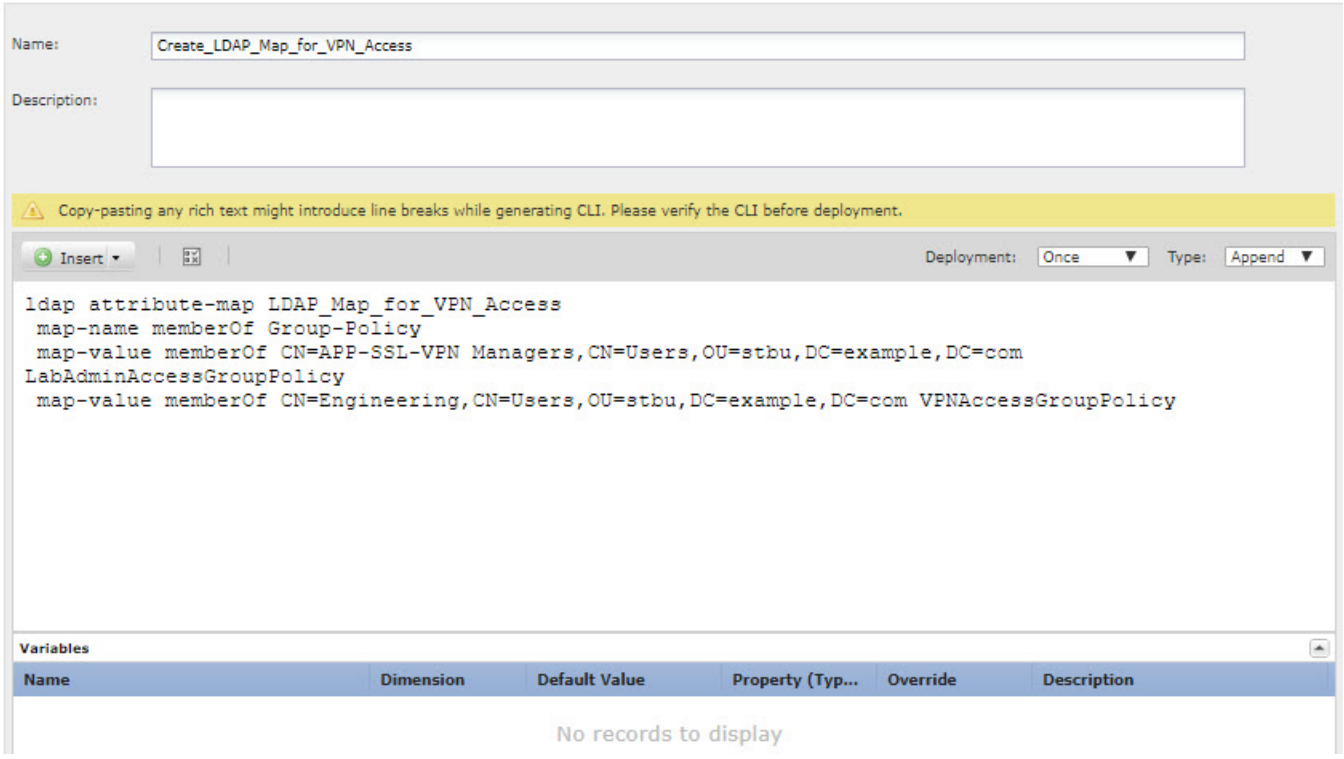
  Dans l'exemple suivant :

  - **LDAP_Map_for_VPN_Access** est le nom de la carte d'attributs LDAP. Il peut s'agir du nom que vous souhaitez.
  - **memberOf** est le nom d'un attribut AD/LDAP, qui est défini dans le serveur lui-même. Ceci n'est pas une chaîne aléatoire.
  - **Group-Policy** est le nom d'un attribut Cisco et n'est pas non plus une chaîne aléatoire.
  - **CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=example,DC=com** est une valeur que vous attendez d'AD/LDAP dans l'attribut **memberOf** lors de l'authentification. Cette chaîne est basée sur la configuration de votre serveur AD/LDAP. Cette chaîne indique que l'utilisateur est membre du groupe d'utilisateurs APP-SSL-VPN Managers.
  - **LabAdminAccessGroupPolicy** est le nom d'une politique de groupe que vous avez définie dans FMC et que vous utilisez dans le profil de connexion VPN d'accès à distance. Cette chaîne doit correspondre au nom d'une politique de groupe existante.
  - **CN=Engineering,CN=Users,OU=stbu,DC=example,DC=com** est une valeur que vous vous attendez à renvoyer dans l'attribut **memberOf**. Cette chaîne indique que l'utilisateur est membre du groupe d'utilisateurs d'ingénierie.
  - **VPNAccessGroupPolicy** est le nom d'une politique de groupe qui existe déjà et est utilisée dans le VPN d'accès à distance.

  Les commandes pour cette configuration seraient les suivantes :

```
ldap attribute-map LDAP_Map_for_VPN_Access
 map-name memberOf Group-Policy
 map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=example,DC=com
LabAdminAccessGroupPolicy
 map-value memberOf CN=Engineering,CN=Users,OU=stbu,DC=example,DC=com
VPNAccessGroupPolicy
```

Le corps de l'objet doit ressembler à ce qui suit :



Étape 2 Créez l'objet FlexConfig deploy-everytime/append qui affecte la carte à un serveur AD/LDAP.

Comme vous définissez le domaine AD/LDAP directement dans le centre de gestion Cisco Firepower Management Center, vos modifications FlexConfig apportées au domaine seront supprimées lors de chaque déploiement. Par conséquent, vous devez les configurer à nouveau à la fin de chaque tâche de déploiement.

Sur la page des objets FlexConfig, Cliquez sur **Add FlexConfig Object** (Ajouter un objet FlexConfig), configurez les propriétés suivantes, puis cliquez sur **Save** (Enregistrer).

- **Name** : nom de l'objet. Par exemple, Attach_LDAP_Map_for_VPN_Access.
- **Deployment** (déploiement) : sélectionnez **Anytime** (À tout moment).
- **Type** : conservez la valeur par défaut, **Append** (Ajouter).
- **Object body** (Corps de l'objet) : dans le corps de l'objet, tapez les commandes requises pour affecter la carte au serveur AD utilisé pour le VPN d'accès à distance.

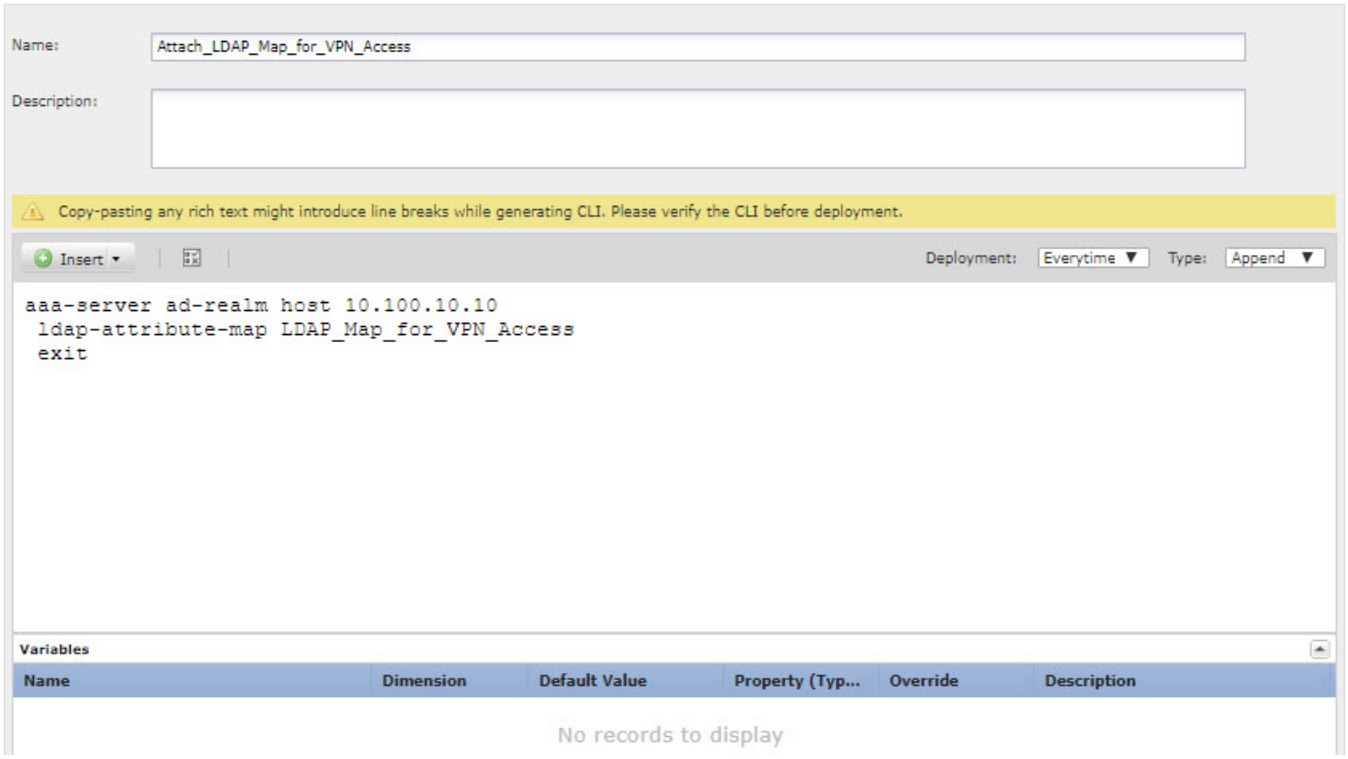
  Dans l'exemple suivant :

  - **LDAP_Map_for_VPN_Access** est le nom de la carte d'attributs LDAP que vous avez créée dans l'objet FlexConfig précédent.
  - **ad_realm** est le nom du domaine AD/LDAP que vous utilisez dans le VPN d'accès à distance, et **10.100.10.10** est l'adresse IP d'un serveur du domaine. Dans cet exemple, nous supposons qu'il n'y a qu'un seul serveur. S'il y en a d'autres, vous devez relancer les commandes **aaa-server** et **ldap-attribute-map** ultérieures pour chaque serveur. Notez que le nom de domaine peut être ce que vous choisissez, mais pour cette commande, il doit correspondre exactement au nom du domaine que vous avez créé et utilisé dans la connexion VPN d'accès à distance que vous modifiez. De même, l'adresse du serveur doit en être une actuellement configurée dans le domaine.

Les commandes pour cette configuration seraient les suivantes :

```
aaa-server ad-realm host 10.100.10.10
 ldap-attribute-map LDAP_Map_for_VPN_Access
 exit
```

Le corps de l'objet doit ressembler à ce qui suit :



Étape 3 Créez la politique FlexConfig qui déploie ces objets.

a) Sélectionnez **Devices** > **FlexConfig** (Appareils, FlexConfig).

b) Cliquez sur **New Policy** (Nouvelle politique) ou si une politique FlexConfig existante doit être affectée (ou est déjà affectée) aux appareils cibles, modifiez simplement cette dernière.

Lors de la création d'une nouvelle politique, affectez les appareils cibles à la politique dans la boîte de dialogue où vous nommez la politique.

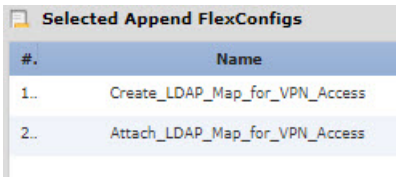
c) Utilisez Ctrl+clic pour sélectionner l'objet FlexConfig dans le dossier **User Defined** (Défini par l'utilisateur) dans la table des matières, puis cliquez sur **>** pour l'ajouter à la politique.

Les objets doivent être ajoutés à la liste **Selected Appended FlexConfigs** (FlexConfigs sélectionnées et ajoutées).

d) Utilisez le glisser-déposer pour vous assurer que les objets sont dans le bon ordre.

L'objet qui crée la carte d'attributs LDAP doit venir avant l'objet qui affecte la carte à un serveur AD/LDAP. Sinon, si vous essayez d'attribuer une carte d'attributs LDAP qui n'existe pas encore, vous obtiendrez une erreur.

La liste devrait ressembler à ce qui suit :



e) Cliquez sur **Save** (Enregistrer).

f) Si vous n'avez pas encore affecté tous les périphériques ciblés à la politique, cliquez sur le lien **Policy Affectations** (Affectations de politiques) ci-dessous Save and make the assignments now (Enregistrer et effectuer les affectations maintenant).

g) Cliquez sur **Preview Config** (Aperçu de la configuration et dans la boîte de dialogue d'aperçu, sélectionnez l'un des périphériques attribués.

Le système génère un aperçu de l'interface de ligne de commande de configuration qui sera envoyée au périphérique. Vérifiez que les commandes générées à partir de l'objet semblent correctes. Celles-ci seront affichées à la fin de l'aperçu. Notez que vous verrez également les commandes générées à partir d'autres modifications que vous avez apportées aux fonctionnalités gérées. Pour les commandes d'attribut LDAP, vous devriez voir quelque chose de similaire à ce qui suit :

```
###Flex-config Appended CLI ######Flex-config Appended CLI ###
ldap attribute-map LDAP_Map_for_VPN_Access

 map-name memberOf Group-Policy

 map-value memberOf CN=APP-SSL-VPN Managers,CN=Users,OU=stbu,DC=example,DC=com
LabAdminAccessGroupPolicy

 map-value memberOf CN=Engineering,CN=Users,OU=stbu,DC=example,DC=com VPNAccessGroupPolicy

aaa-server ad-realm host 10.100.10.10

 ldap-attribute-map LDAP_Map_for_VPN_Access

 exit
```

Étape 4 Déployez vos modifications.

Étape 5 Vérifiez la configuration.

Vous pouvez vérifier que les commandes ont été configurées sur chaque appareil FTD. Utilisez une session SSH avec l'appareil ou avec l'outil CLI dans FMC (**System** > **Health** > **Monitor** [Système, Intégrité, Vérifier], cliquez sur l'appareil, puis sur **Advanced Troubleshooting** [Dépannage avancé], puis sélectionnez l'onglet **Threat Defense CLI**). Voici les commandes qui afficheront la configuration.

- **show running-config aaa-server** affiche la configuration du serveur AD/LDAP.
- **show running-config ldap** affiche la carte des attributs.

Retirer les cartes d'attribut LDAP

Si vous ne souhaitez plus utiliser la mise en correspondance d'attributs LDAP, vous devez créer un objet FlexConfig pour retirer la configuration des appareils sur lesquels vous avez déployé la fonctionnalité. Le simple retrait des objets FlexConfig de la politique FlexConfig n'est pas suffisante.

Cependant, pour résoudre rapidement un problème, vous pouvez simplement supprimer l'objet FlexConfig qui attribue la carte au serveur AD/LDAP et déployer les modifications. Le processus de déploiement retire toutes les modifications apportées aux fonctionnalités gérées, de sorte que la commande **ldap-attribute-map** qui attribue la carte au serveur sera supprimée. Cela signifie que la carte continuera d'exister dans la configuration de l'appareil, mais elle ne sera utilisée par aucun serveur AD/LDAP.

La procédure suivante explique comment retirer la carte.

Procédure

Étape 1 Créez l'objet FlexConfig Deploy-once/append qui supprime la carte d'attributs LDAP.

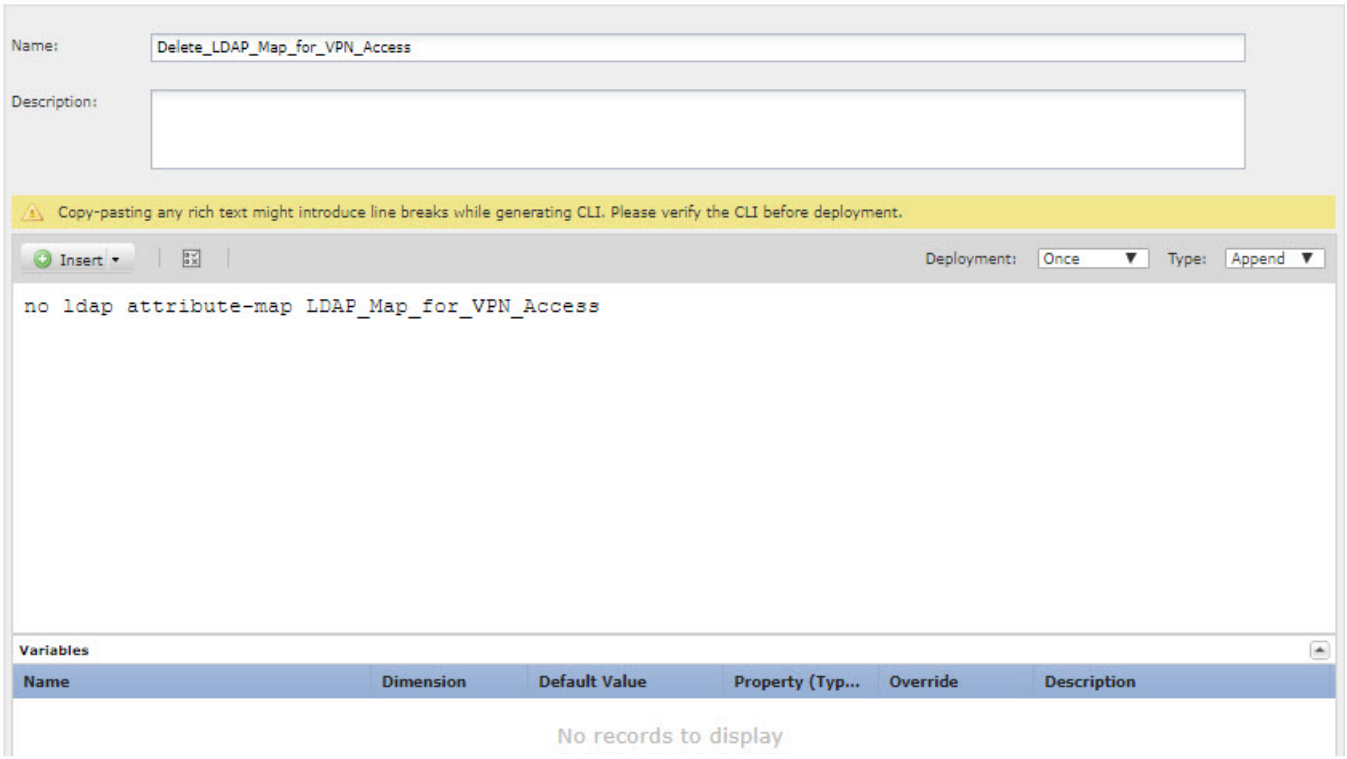
Normalement, vous devez d'abord supprimer toutes les commandes qui utilisent un objet avant de supprimer l'objet. Cependant, comme le domaine AD/LDAP est une fonctionnalité gérée, la tâche de déploiement aura déjà supprimé ces commandes. Ainsi, vous devez simplement supprimer la carte d'attributs.

a) Choisissez **Objects** > **Object Management** (Objets, Gestion des objets).
b) Choisissez **FlexConfig** > **FlexConfig Object** (FlexConfig, Objets FlexConfig) dans la table des matières.
c) Cliquez sur **Add FlexConfig Object** (Ajouter un objet FlexConfig), configurez les propriétés suivantes, puis cliquez sur **Save** (Enregistrer).

- **Name** : nom de l'objet. Par exemple, Delete_LDAP_Map_for_VPN_Access.
- **Deployment** (Déploiement) : sélectionnez **Once** (une fois). Ces commandes doivent être configurées une seule fois.
- **Type** : conservez la valeur par défaut, **Append** (Ajouter). Les commandes sont envoyées à l'appareil après les commandes des fonctionnalités directement prises en charge. Cela est particulièrement important, car vous dépendez de la tâche de déploiement pour supprimer les commandes qui utilisent la mise en correspondance des attributs LDAP.
- **Object body** (Corps de l'objet) : dans le corps de l'objet, tapez la commande requise pour supprimer la carte d'attributs LDAP. Notez que vous n'avez pas besoin de supprimer le contenu de la carte. Vous supprimez simplement la carte et son contenu est également supprimé. Par exemple, si la carte s'intitule LDAP_Map_for_VPN_Access, la commande serait la suivante :

```
no ldap attribute-map LDAP_Map_for_VPN_Access
```

Le corps de l'objet doit ressembler à ce qui suit :



Étape 2 Modifiez la politique FlexConfig pour supprimer les objets qui créent et attribuent la carte d'attributs LDAP, et ajoutez l'objet qui supprime la carte.

a) Sélectionnez **Devices** > **FlexConfig** (Appareils, FlexConfig).

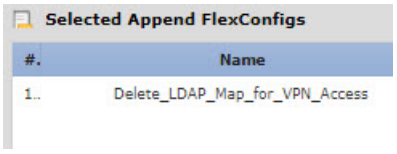
b) Modifiez la politique FlexConfig

c) Dans la liste **Selected Appended FlexConfigs** (FlexConfigs sélectionnées et ajoutées), cliquez sur l'icône de suppression des objets qui créent et attribuent la carte d'attributs LDAP.

d) Sélectionnez l'objet FlexConfig qui supprime la carte dans le dossier **User Defined** (Défini par l'utilisateur) dans la table des matières, puis cliquez sur > pour l'ajouter à la politique.

L'objet doit être ajouté à la liste **Selected Appended FlexConfigs** (FlexConfigs sélectionnées et ajoutées).

La liste devrait ressembler à ce qui suit :



e) Cliquez sur **Save** (Enregistrer).

f) Cliquez sur **Preview Config** (Aperçu de la configuration et dans la boîte de dialogue d'aperçu, sélectionnez l'un des périphériques attribués.

Le système génère un aperçu de l'interface de ligne de commande de configuration qui sera envoyée au périphérique. Vérifiez que les commandes générées à partir de l'objet semblent correctes. Celles-ci seront affichées à la fin de l'aperçu. Notez que vous verrez également les commandes générées à partir d'autres modifications que vous avez apportées aux fonctionnalités gérées. Pour cet exemple, vous devriez voir quelque chose de semblable à ce qui suit :

```
###Flex-config Appended CLI ###
no ldap attribute-map LDAP_Map_for_VPN_Access
```

Étape 3 Déployez vos modifications.

Personnaliser l'icône et le logo AnyConnect

Vous pouvez personnaliser l'icône et le logo de l'application AnyConnect sur les machines clients Windows et Linux. Les noms des icônes sont prédéfinis et il existe des limites précises au type de fichier et à la taille des images que vous téléversez.

Bien que vous puissiez utiliser n'importe quel nom de fichier si vous déployez votre propre exécutable pour personnaliser l'interface graphique, cet exemple suppose que vous échangez simplement des icônes et des logos sans déployer une structure entièrement personnalisée.

Il existe un certain nombre d'images que vous pouvez remplacer, et leurs noms de fichiers varient selon la plateforme. Pour des renseignements complets sur les options de personnalisation, les noms de fichiers, les types et les tailles, consultez le chapitre sur la personnalisation et la localisation du client AnyConnect dans le *Guide de l'administrateur du client Cisco AnyConnect Secure Mobility* . Par exemple, le chapitre du client 4.8 est disponible à l'adresse :

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect48/administration/guide/b_AnyConnect_Administrator_Guide_4-8/customize-localize-anyconnect.html

Remarque Vous pouvez effectuer cette personnalisation avec n'importe quel appareil FTD, quel que soit l'outil que vous utilisez pour le gérer. Cependant, FlexConfig ne fonctionnera pour ces commandes que dans le FMC.

Avant de commencer

Aux fins de cet exemple, nous remplacerons les images suivantes pour les clients Windows. Notez que si votre image est de taille différente de la taille maximale, le système la redimensionnera automatiquement au maximum et étendra automatiquement l'image au besoin.

- app_logo.png

  Cette image de logo d'application est l'icône de l'application. Elle peut avoir une taille maximale de 128 x 128 pixels.

- company_logo.png

  Cette image de logo d'entreprise apparaît dans le coin supérieur gauche des commandes déroulantes du tiroir et des boîtes de dialogue Advanced (Avancé). La taille maximale est de 97 x 58 pixels.

- company_logo_alt.png

  L'autre image de logo d'entreprise apparaît dans le coin inférieur droit de la boîte de dialogue À propos de. La taille maximale est de 97 x 58 pixels.

Pour téléverser ces fichiers, vous devez les placer sur un serveur auquel l'appareil FTD peut accéder. Vous pouvez utiliser un serveur TFTP, FTP, HTTP, HTTPS ou SCP. Les URL pour obtenir des images de ces

fichiers peuvent inclure des chemins d'accès et un nom d'utilisateur/mot de passe, comme requis par la configuration de votre serveur. Cet exemple utilisera TFTP.

Procédure

Étape 1 Chargez les fichiers image sur chaque appareil FTD qui agit en tant que tête de réseau VPN d'accès à distance qui doit utiliser les icônes et les logos personnalisés.

a) Connectez-vous à l'interface de ligne de commande (CLI) de l'appareil à l'aide d'un client SSH.

b) Dans l'interface de ligne de commande, saisissez la commande **system support diagnostic-cli** pour passer en mode de diagnostic de l'interface de ligne de commande.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftdv1>
```

Remarque
Lisez le message! Vous devez appuyer sur **Ctrl + a, puis sur d**, pour sortir de l'interface de commande en ligne de diagnostic et revenir en mode d'interface de commande en ligne FTD normal.

c) Notez l'invite de commande. La CLI normale utilise uniquement les >, tandis que le mode EXEC de l'interface de diagnostic en ligne de diagnostic utilise le nom d'hôte plus >. Dans cet exemple, ftdv1>. Vous devez passer en mode d'exécution privilégié, qui utilise # comme caractère de fin, par exemple, ftdv1#. Si votre invite contient déjà le numéro, ignorez cette étape. Sinon, saisissez la commande enable, puis appuyez simplement sur Enter (Entrée) à l'invite de mot de passe, et ce, sans saisir de mot de passe.

```
ftdv1> enable
Password:
ftdv1#
```

d) Utilisez la commande **copy** pour copier chaque fichier du serveur d'hébergement dans le disk0 (disque0) de l'appareil FTD. Vous pouvez les placer dans un sous-répertoire, tel que disk0:/anyconnect-images/. Vous pouvez créer un nouveau dossier en utilisant la commande **mkdir**.

Par exemple, si l'adresse IP du serveur TFTP est 10.7.0.80 et que vous souhaitez créer un nouveau répertoire, les commandes seront semblables aux suivantes. Notez que les réponses à la commande **copy** sont omis après le premier exemple.

```
ftdv1# mkdir disk0:anyconnect-images

Create directory filename [anyconnect-images]? yes

Created dir disk0:/anyconnect-images

ftdv1# copy /noconfirm tftp://10.7.0.80/app_logo.png
disk0:/anyconnect-images/app_logo.png

Accessing tftp://10.7.0.80/app_logo.png...!!!!!!
Writing file disk0:/anyconnect-images/app_logo.png...
!!!!!!
12288 bytes copied in 1.000 secs (12288 bytes/sec)

ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo.png
```

```
disk0:/anyconnect-images/company_logo.png
ftdv1# copy /noconfirm tftp://10.7.0.80/company_logo_alt.png
disk0:/anyconnect-images/company_logo_alt.png
```

Étape 2 Utilisez la commande **import webvpn** dans l'interface de ligne de commande de diagnostic pour demander à AnyConnect de télécharger ces images lors de son installation sur les machines clientes.

import webvpn AnyConnect-customization type resource platform win name *filename* **disk0:**/*directoryname/filename*

Cette commande concerne Windows. Pour Linux, remplacez le mot-clé **win** par **linux** ou **linux-64**, selon le cas pour vos clients.

Par exemple, pour importer les fichiers téléchargés à l'étape précédente, et en supposant que nous sommes toujours dans l'interface de ligne de commande de diagnostic :

```
ftdv1# import webvpn AnyConnect-customization type resource platform win
name app_logo.png disk0:/anyconnect-images/app_logo.png

ftdv1# import webvpn AnyConnect-customization type resource platform win
name company_logo.png disk0:/anyconnect-images/company_logo.png

ftdv1# import webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png disk0:/anyconnect-images/company_logo_alt.png
```

Remarque
Vous pouvez effectuer cette étape à l'aide de FlexConfig, en entrant les commandes **import webvpn** dans un objet FlexConfig deploy-once/append, en ajoutant l'objet à une politique FlexConfig, puis en attribuant les politiques FlexConfig aux appareils FTD concernés. Cependant, comme vous devez passer en mode d'exécution privilégié de la CLI de diagnostic sur chaque appareil pour téléverser les images, il est pratique de les importer en même temps.

Étape 3 Vérifiez la configuration.

- Pour vérifier les fichiers importés, utilisez la commande **show import webvpn AnyConnect-customization** en mode d'exécution privilégié de la CLI de diagnostic.
- Pour vérifier que les images ont été téléchargées sur un client, elles doivent apparaître lorsque l'utilisateur exécute le client. Vous pouvez également vérifier le dossier suivant sur les clients Windows, où %PROGRAMFILES% se résout généralement en c:\Program Files.

  %PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\res

Prochaine étape

Si vous souhaitez revenir aux images par défaut, utilisez la commande **revert webvpn** (en mode d'exécution privilégié de la CLI de diagnostic) pour chaque image que vous avez personnalisée. Vous pouvez le faire dans un FlexConfig deploy-once/append, ce qui a plus de sens, car vous devriez probablement le faire après avoir exécuté le VPN d'accès à distance pendant un certain temps. FlexConfig vous économiserait l'effort d'établir des connexions SSH avec chaque appareil et vous permettra d'effectuer la tâche en une seule tâche de déploiement. La commande est :

revert webvpn AnyConnect-customization type resource platform win name *nom de fichier*

Comme pour **import webvpn**, remplacez **win** par **linux** ou **linux-64** si vous avez personnalisé ces plateformes clientes, et exécutez la commande séparément pour chaque nom de fichier d'image que vous avez importé. Par exemple :

```
ftdv1# revert webvpn AnyConnect-customization type resource platform win
name app_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo.png

ftdv1# revert webvpn AnyConnect-customization type resource platform win
name company_logo_alt.png
```

Configurer les modules et profils AnyConnect à l'aide de FlexConfig

Le paquet AnyConnect comprend des modules pour une variété de fonctionnalités, telles que l'activateur AMP, que vous pouvez éventuellement utiliser pour fournir des services supplémentaires aux connexions VPN d'accès à distance. Chaque module comprend un profil que vous pouvez modifier pour le faire fonctionner selon vos besoins. Pour activer ces modules et ces profils sur FTD, vous devez utiliser FlexConfig.

Vous ne devez configurer que les modules que vous avez l'intention d'utiliser. Chaque module a son propre éditeur de profil, qui est inclus dans le paquet AnyConnect Profile Editor que vous pouvez télécharger et installer sur un système Windows.

Comme le fichier de paquet AnyConnect comprend tous les modules, vous ne téléversez pas les modules eux-mêmes. Il vous suffit de téléverser les profils utilisés par les modules afin de personnaliser le comportement du module afin qu'il fonctionne dans votre configuration VPN d'accès à distance.

Vous pouvez configurer cette fonctionnalité en utilisant l'IU de FMC à partir des versions 6.7 ou ultérieures. Pour en savoir plus, consultez Configurer les modules Secure Client sur un Threat Defense à l'aide de Cisco Secure Firewall Management Center.

Dans les versions 6.4 à 6.6, vous pouvez activer le VPN par application sur un FTD à l'aide de FlexConfig. Utilisez la procédure suivante pour cette configuration :

Avant de commencer

Avant de pouvoir téléverser des profils client, vous devez effectuer les opérations suivantes.

- Téléchargez et installez l'outil d'installation autonome AnyConnect « Profile Editor - Windows / Standalone installer (MSI) ». Le fichier d'installation est destiné à Windows uniquement, et il est intitulé tools-anyconnect-profileeditor-win-<version>-k9.msi, où <version> est la version d'AnyConnect. Par exemple, tools-anyconnect-win-4.8.03036-profileeditor-k9.msi. Vous devez également installer Java JRE 1.6 (ou une version ultérieure) avant d'installer l'éditeur de profils. Obtenez l'éditeur de profil AnyConnect sur software.cisco.com dans la catégorie AnyConnect Secure Mobility Client.
- Utilisez les éditeurs de profils AnyConnect appropriés basés sur l'interface graphique pour créer les profils dont vous avez besoin. Pour des informations détaillées, consultez l'aide en ligne de l'éditeur.

Dans cet exemple, nous allons téléverser des profils et activer tous les modules. Dans l'exemple, vous avez déjà un VPN d'accès à distance opérationnel et vous avez créé toutes les politiques de groupe à l'aide de FMC.

Procédure

Étape 1 Chargez les profils sur chaque appareil FTD qui agit en tant que tête de réseau VPN d'accès à distance qui doit utiliser les profils de module personnalisés.

a) Connectez-vous à l'interface de ligne de commande (CLI) de l'appareil à l'aide d'un client SSH.

b) Dans l'interface de ligne de commande, saisissez la commande **system support diagnostic-cli** pour passer en mode de diagnostic de l'interface de ligne de commande.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftdv1>
```

Remarque
Lisez le message! Vous devez appuyer sur **Ctrl + a, puis sur d**, pour sortir de l'interface de commande en ligne de diagnostic et revenir en mode d'interface de commande en ligne FTD normal.

c) Notez l'invite de commande. La CLI normale utilise uniquement les >, tandis que le mode EXEC de l'interface de diagnostic en ligne de diagnostic utilise le nom d'hôte plus >. Dans cet exemple, ftdv1>. Vous devez passer en mode d'exécution privilégié, qui utilise # comme caractère de fin, par exemple, ftdv1#. Si votre invite contient déjà le numéro, ignorez cette étape. Sinon, saisissez la commande enable, puis appuyez simplement sur Enter (Entrée) à l'invite de mot de passe, et ce, sans saisir de mot de passe.

```
ftdv1> enable
Password:
ftdv1#
```

d) Utilisez la commande **copy** pour copier chaque fichier du serveur d'hébergement dans le disk0 (disque0) de l'appareil FTD. Vous pouvez les placer dans un sous-répertoire, tel que disk0:/modules/. Vous pouvez créer un nouveau dossier en utilisant la commande **mkdir**.

Par exemple, si l'adresse IP du serveur TFTP est 10.7.0.80 et que vous souhaitez créer un nouveau répertoire, les commandes seront semblables aux suivantes. Notez que les réponses à la commande **copy** sont omises après le premier exemple.

```
ftdv1# mkdir disk0:modules

Create directory filename [modules]? yes

Created dir disk0:/modules

ftdv1# copy /noconfirm tftp://10.7.0.80/amp.asp
disk0:/modules/amp.asp

Accessing tftp://10.7.0.80/amp.asp...!!!
Writing file disk0:/modules/amp.asp...
!
676 bytes copied in 0.0 secs (812800 bytes/sec)

ftdv1# copy /noconfirm tftp://10.7.0.80/ACManifestUmbrella-01.xml
disk0:/modules/ACManifestUmbrella-01.xml
ftdv1# copy /noconfirm tftp://10.7.0.80/feedback.fsp
disk0:/modules/feedback.fsp
```

```
ftdv1# copy /noconfirm tftp://10.7.0.80/iseposture.isp
disk0:/modules/iseposture.isp
ftdv1# copy /noconfirm tftp://10.7.0.80/nam.nsp
disk0:/modules/nam.nsp
ftdv1# copy /noconfirm tftp://10.7.0.80/networkvisibility.nvmsp
disk0:/modules/networkvisibility.nvmsp
ftdv1# copy /noconfirm tftp://10.7.0.80/websecurity.wso
disk0:/modules/websecurity.wso
ftdv1# copy /noconfirm tftp://10.7.0.80/vpn.xml
disk0:/modules/vpn.xml
```

Étape 2 Créez l'objet FlexConfig deploy-once/append qui identifie les profils pour chaque module et active les modules pour chaque profil de groupe dans le VPN d'accès à distance.

a) Choisissez **Objects** > **Object Management** (Objets, Gestion des objets).

b) Choisissez **FlexConfig** > **FlexConfig Object** (FlexConfig, Objets FlexConfig) dans la table des matières.

c) Cliquez sur **Add FlexConfig Object** (Ajouter un objet FlexConfig), configurez les propriétés suivantes, puis cliquez sur **Save** (Enregistrer).

- **Name** : nom de l'objet. Par exemple, Enable_AnyConnect_Module_Profiles.
- **Deployment** (déploiement) : sélectionnez **Anytime** (À tout moment). Comme vous modifiez des fonctionnalités gérées activement par FMC, vos modifications seront retirée pendant chaque tâche de déploiement. Ainsi, vous devez les reconfigurer chaque fois que vous déployez des modifications.
- **Type** : conservez la valeur par défaut, **Append** (Ajouter).
- **Object body** (Corps de l'objet) : dans le corps de l'objet, saisissez les commandes requises pour identifier les profils, activer les modules et appliquer les profils pour chaque politique de groupe qui doit les utiliser. Les commandes que vous devez configurer sont les suivantes :
  - **anyconnect profiles** *profile_name file_location*

    Cette commande, en mode de configuration webvpn, indique le nom du profil ainsi que le chemin d'accès complet et le nom de fichier du profil sur le disque de l'appareil FTD. Cette commande rend le profil disponible pour une utilisation par AnyConnect et ses modules.
  - **anyconnect modules value** *module_names*

    Cette commande, en mode de configuration de la politique de groupe webvpn, spécifie les modules AnyConnect que vous souhaitez activer pour la politique de groupe. Vous devez utiliser cette commande sur chaque politique de groupe qui doit utiliser les modules. Vous pouvez définir plusieurs modules en les séparant par des virgules, mais sans espaces.
  - Les noms de modules possibles sont :
    - **dart**— Outil de diagnostic et de rapport AnyConnect (DART)
    - **nam**— Gestionnaire d'accès au réseau de AnyConnect
    - **vpngina**—AnyConnect Start Before Logon (SBL)
    - **websecurity**—AnyConnect Web Security Module
    - **telemetry**—AnyConnect Telemetry Module
    - **posture**—AnyConnect Posture Module
    - **ampenabler**—AnyConnect AMP Enabler

- **iseposture**—AnyConnect ISE Posture
- **umbrella**—AnyConnect Umbrella

- **anyconnect profiles value** *profile_name* **type** *module_name*

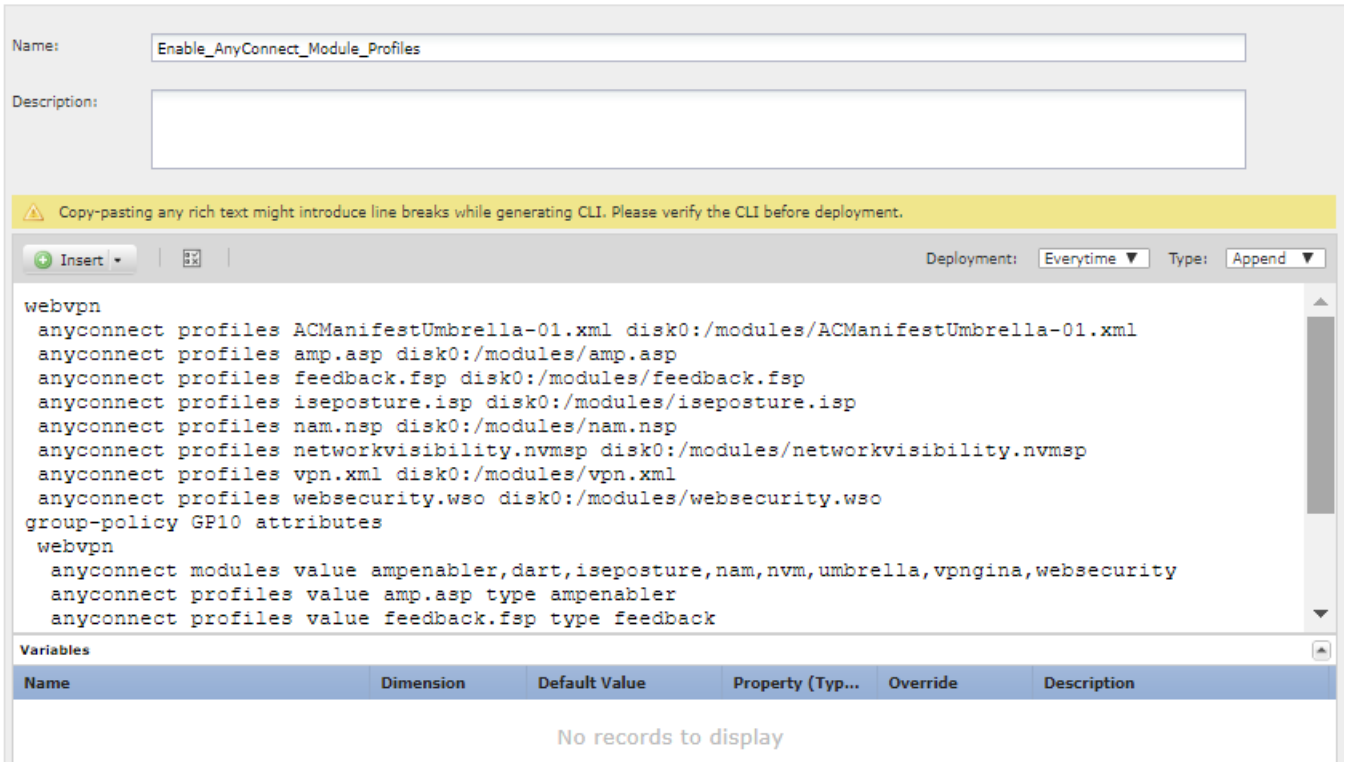
  Cette commande, en mode de configuration de la politique de groupes webvpn, précise le profil à utiliser pour le module que vous avez activé avec la commande **anyconnect modules**. L'exception est le module **feedback**, qui n'a pas besoin d'être activé au préalable. Les noms de module sont les mêmes que ceux utilisés dans la commande **anyconnect modules**, à l'exception de **vpngina**, dont le type est **user**.

Par exemple, les commandes suivantes configurent les modules que nous avons précédemment téléversés pour la politique de groupe nommée G10. Si vous avez des politiques de groupe supplémentaires, vous devez relancer l'ensemble de commandes qui commence par la commande group-policy pour chaque politique de groupe.

```
webvpn
 anyconnect profiles ACManifestUmbrella-01.xml
disk0:/modules/ACManifestUmbrella-01.xml
 anyconnect profiles amp.asp disk0:/modules/amp.asp
 anyconnect profiles feedback.fsp disk0:/modules/feedback.fsp
 anyconnect profiles iseposture.isp disk0:/modules/iseposture.isp
 anyconnect profiles nam.nsp disk0:/modules/nam.nsp
 anyconnect profiles networkvisibility.nvmsp disk0:/modules/networkvisibility.nvmsp

 anyconnect profiles vpn.xml disk0:/modules/vpn.xml
 anyconnect profiles websecurity.wso disk0:/modules/websecurity.wso
group-policy GP10 attributes
 webvpn
  anyconnect modules value
ampenabler,dart,iseposture,nam,nvm,umbrella,vpngina,websecurity
  anyconnect profiles value amp.asp type ampenabler
  anyconnect profiles value feedback.fsp type feedback
  anyconnect profiles value iseposture.isp type iseposture
  anyconnect profiles value nam.nsp type nam
  anyconnect profiles value networkvisibility.nvmsp type nvm
  anyconnect profiles value ACManifestUmbrella-01.xml type umbrella
  anyconnect profiles value websecurity.wso type websecurity
  anyconnect profiles value vpn.xml type user
```

Le corps de l'objet doit ressembler à ce qui suit :



Étape 3 Créez la politique FlexConfig qui déploie cet objet.

a) Sélectionnez **Devices** > **FlexConfig** (Appareils, FlexConfig).

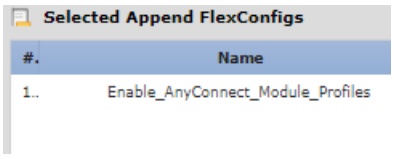
b) Cliquez sur **New Policy** (Nouvelle politique) ou si une politique FlexConfig existante doit être affectée (ou est déjà affectée) aux appareils cibles, modifiez simplement cette dernière.

Lors de la création d'une nouvelle politique, affectez les appareils cibles à la politique dans la boîte de dialogue où vous nommez la politique.

c) Sélectionnez l'objet FlexConfig dans le dossier **User Defined** (défini par l'utilisateur) dans la table des matières, puis cliquez sur **>** pour l'ajouter à la politique.

L'objet doit être ajouté à la liste **Selected Appended FlexConfigs** (FlexConfigs sélectionnées et ajoutées).

La liste devrait ressembler à ce qui suit :



d) Cliquez sur **Save** (Enregistrer).

e) Si vous n'avez pas encore affecté tous les périphériques ciblés à la politique, cliquez sur le lien **Policy Affectations** (Affectations de politiques) ci-dessous Save and make the assignments now (Enregistrer et effectuer les affectations maintenant).

f) Cliquez sur **Preview Config** (Aperçu de la configuration et dans la boîte de dialogue d'aperçu, sélectionnez l'un des périphériques attribués.

Le système génère un aperçu de l'interface de ligne de commande de configuration qui sera envoyée au périphérique. Vérifiez que les commandes générées à partir de l'objet semblent correctes. Celles-ci seront affichées à la fin de l'aperçu. Notez que vous verrez également les commandes générées à partir d'autres modifications que vous avez apportées aux fonctionnalités gérées. En ce qui concerne ces commandes, le résultat devrait ressembler à ce qui suit :

```
###Flex-config Appended CLI ###
webvpn

 anyconnect profiles ACManifestUmbrella-01.xml disk0:/modules/ACManifestUmbrella-01.xml


 anyconnect profiles amp.asp disk0:/modules/amp.asp

 anyconnect profiles feedback.fsp disk0:/modules/feedback.fsp

 anyconnect profiles iseposture.isp disk0:/modules/iseposture.isp

 anyconnect profiles nam.nsp disk0:/modules/nam.nsp

 anyconnect profiles networkvisibility.nvmsp disk0:/modules/networkvisibility.nvmsp

 anyconnect profiles vpn.xml disk0:/modules/vpn.xml

 anyconnect profiles websecurity.wso disk0:/modules/websecurity.wso

group-policy GP10 attributes

 webvpn

  anyconnect modules value ampenabler,dart,iseposture,nam,nvm,umbrella,vpngina,websecurity


  anyconnect profiles value amp.asp type ampenabler

  anyconnect profiles value feedback.fsp type feedback

  anyconnect profiles value iseposture.isp type iseposture

  anyconnect profiles value nam.nsp type nam

  anyconnect profiles value networkvisibility.nvmsp type nvm

  anyconnect profiles value ACManifestUmbrella-01.xml type umbrella

  anyconnect profiles value websecurity.wso type websecurity

  anyconnect profiles value vpn.xml type user
```

Étape 4 Déployez vos modifications.

Prochaine étape

Puisque vous apportez des modifications à des fonctionnalités gérées, pour supprimer la configuration du module, supprimez simplement l'objet FlexConfig de la politique FlexConfig, puis redéployez la configuration. La tâche de déploiement supprimera les modifications de configuration.

Si vous souhaitez supprimer les profils des appareils, vous devez vous connecter à l'interface de ligne de commande de chaque appareil et utiliser la commande **delete** en mode d'exécution privilégié dans l'interface de ligne de commande de diagnostic.

VPN d'accès à distance fondé sur les applications (par application) sur les appareils portables

Lorsque vous prenez en charge des appareils portables, tels que les téléphones exécutant Android ou iOS, vous pouvez utiliser les applications du gestionnaire de périphériques mobiles (MDM) pour ajuster l'accès VPN afin que seules les applications prises en charge soient autorisées à utiliser le tunnel VPN. En limitant le VPN d'accès à distance aux applications approuvées, vous pouvez réduire la charge sur la tête de réseau VPN et protéger le réseau d'entreprise contre les applications malveillantes installées sur ces appareils portables.

Pour utiliser le VPN d'accès distant par application, vous devez installer et configurer une application tierce de gestion des appareils mobiles (MDM). C'est dans le gestionnaire des appareils mobiles que vous définissez la liste des applications approuvées qui peuvent être utilisées sur le tunnel VPN. L'explication de la configuration et de l'utilisation du gestionnaire des appareils mobiles tiers que vous sélectionnez n'entre pas dans le cadre de ce document.

Vous pouvez configurer cette fonctionnalité en utilisant l'IU de FMC à partir des versions 7.0 ou ultérieures. Pour en savoir plus, consultez Configurer le VPN d'accès à distance basé sur les applications (VPN par application) sur les appareils portables à l'aide de Cisco Secure Firewall Management Center.

Dans les versions 6.4 à 6.7, vous pouvez activer le VPN par application sur un FTD à l'aide de FlexConfig. Les rubriques suivantes expliquent comment activer le VPN par application sur la tête de réseau FTD à l'aide de FlexConfig, afin que votre gestionnaire de périphériques mobiles puisse appliquer vos politiques sur les appareils portables.

À propos des VPN basés sur les applications (par application)

Lorsque vous utilisez AnyConnect pour établir une connexion VPN à partir d'un appareil portable , tout le trafic, y compris le trafic des applications personnelles, est acheminé par le VPN.

Si vous souhaitez plutôt acheminer les applications d'entreprise uniquement par le VPN, de sorte que le trafic non entreprise est exclu du VPN, vous pouvez utiliser le VPN par application pour sélectionner les applications qui doivent être tunnellisées par le VPN.

Vous configurez le VPN par application à l'aide de l'attribut personnalisé **perapp** AnyConnect. L'ajout de cet attribut à un profil de groupe VPN d'accès à distance limite automatiquement le tunnel aux applications explicitement identifiées. Le trafic de toutes les autres applications est automatiquement exclu du tunnel.

La configuration du VPN par application présente les principaux avantages suivants :

- **Performance** : elle limite le trafic dans le VPN au trafic qui doit être acheminé au réseau d'entreprise. Ainsi, vous libèrez des ressources à la tête de réseau du VPN d'accès à distance.
- **Protection** : Puisque seul le trafic des applications approuvées est autorisé, elle protège le tunnel d'entreprise des applications malveillantes non approuvées qu'un utilisateur pourrait installer involontairement sur l'appareil portable. Étant donné que ces applications ne sont pas incluses dans le tunnel, le trafic provenant de celles-ci n'est jamais envoyé à la tête de réseau.

Le gestionnaire de périphériques mobiles (MDM) s'exécutant sur le terminal mobile applique la politique VPN par appareil sur les applications.

Détermination des identifiants d'application des applications mobiles

Avant de configurer la tête de réseau FTD pour autoriser le VPN basé sur les applications à partir des appareils portables, vous devez déterminer quelles applications doivent être autorisées dans le tunnel.

Nous vous recommandons fortement de configurer la politique par application dans le gestionnaire de périphéques mobiles (MDM) sur l'appareil portable de l'utilisateur. Cela simplifie vraiment la configuration de la tête de réseau.

Si vous décidez à la place de configurer la liste des applications autorisées sur la tête de réseau, vous devez déterminer les identifiants d'application pour chaque application sur chaque type de terminal.

L'ID de l'application, appelé ID de lot dans iOS, est un nom DNS inversé. Vous pouvez utiliser un astérisque comme caractère générique. Par exemple, *.* indique toutes les applications et com.cisco.* indique toutes les applications Cisco.

Pour déterminer les ID d'application :

- **Android** : accédez à Google Play dans un navigateur Web et sélectionnez la catégorie Apps. Cliquez sur (ou passez le curseur sur) une application que vous souhaitez autoriser, puis regardez l'URL. L'ID de l'application se trouve dans l'URL, dans le paramètre **id=**. Par exemple, l'URL suivante concerne Facebook Messenger, donc l'ID de l'application est com.facebook.orca.

  https://play.google.com/store/apps/details?id=com.facebook.orca

  Pour les applications qui ne sont pas disponibles sur Google Play, comme les vôtres, téléchargez une application de visualisation de nom de paquet pour extraire l'ID de l'application. Plusieurs de ces applications sont disponibles, l'une d'entre elles devrait fournir ce dont vous avez besoin, mais Cisco n'approuve aucune d'entre elles.

- **iOS** : Il n'y a aucun moyen simple d'obtenir l'ID d'offre groupée. Voici une façon de le déterminer :

  1. Utilisez un navigateur Web de poste de travail tel que Chrome pour rechercher le nom de l'application.
  2. Dans les résultats de la recherche, cherchez le lien pour télécharger l'application sur l'App Store d'Apple. Par exemple, Facebook Messager ressemblerait à :

     https://apps.apple.com/us/app/messenger/id454638411
  3. Copiez le numéro après la chaîne d' **id**. Dans cet exemple, **454638411**.
  4. Ouvrez une nouvelle fenêtre de navigateur et ajoutez le numéro à la fin de l'URL suivante :

     https://itunes.apple.com/lookup?id=

     Pour cet exemple : https://itunes.Apple.com/lookup?id=454638411
  5. Vous serez invité à télécharger un fichier texte, généralement nommé 1.txt. Téléchargez le fichier.
  6. Ouvrez le fichier dans un éditeur de texte tel que Wordpad et recherchez le bundleid. Par exemple :

     "bundleId":"com.facebook.Messenger",

     Dans cet exemple, l'ID de lot est com.facebook.Messenger. Utilisez-le comme ID d'application.

Une fois que vous avez votre liste d'identifiants d'application, vous pouvez configurer la politique comme expliqué dans la section. Configurer les tunnels VPN basés sur les applications (par application), à la page 28

Configurer les tunnels VPN basés sur les applications (par application)

Après avoir installé et configuré votre logiciel gestionnaire de périphériques mobiles, vous pouvez activer le VPN par application sur l'appareil de tête de réseau FTD. Une fois activé sur la tête de réseau, votre logiciel MDM commencera à contrôler quelles applications sont acheminées par tunnellisation du VPN vers le réseau d'entreprise.

Avant de commencer

Cette fonctionnalité nécessite la licence AnyConnect Plus ou Apex. Elle fonctionne uniquement sur les appareils Android et iOS.

Cet exemple suppose que vous ayez déjà configuré le VPN d'accès à distance et qu'il fonctionne correctement.

Vous devez également avoir déjà installé et configuré un gestionnaire de périphériques mobiles tiers. Vous configurez les applications qui seront autorisées dans le VPN sur le gestionnaire des appareils mobiles, et non sur l'appareil de tête de réseau FTD. Au lieu de cela, la meilleure pratique consiste simplement à activer le VPN par application dans FTD, puis à utiliser le gestionnaire des appareils mobiles pour configurer et mettre en œuvre votre politique par application. L'exemple suivant suppose que vous utilisiez cette approche plutôt que de préciser les applications sur la tête de réseau FTD.

Procédure

Étape 1 Téléchargez le **sélecteur d'applications Cisco AnyConnect Enterprise** du site software.cisco.com. Vous pouvez trouver cette application dans la catégorie **AnyConnect Secure Mobility Client v4.x.**

Vous devez exécuter Java 7 pour exécuter le fichier jar d'application.

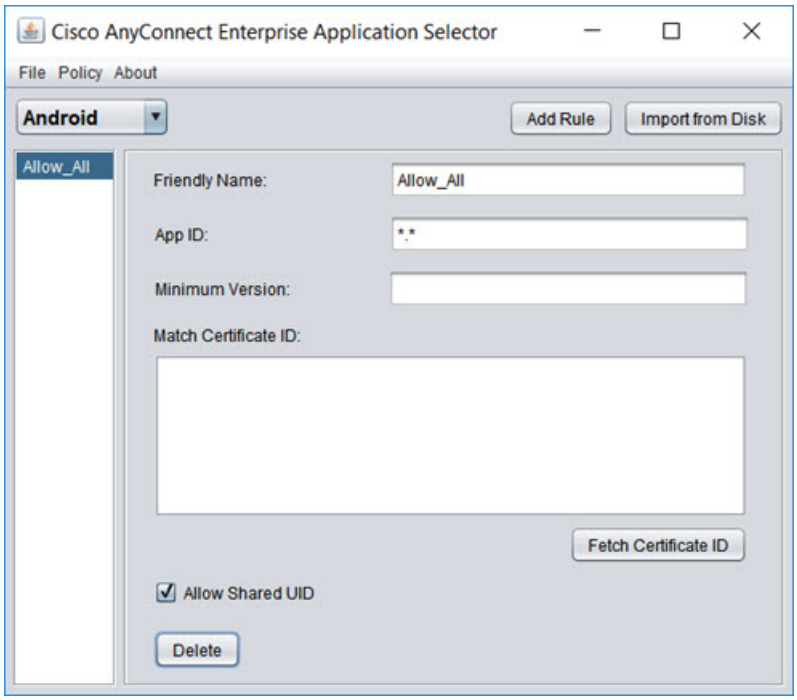
Étape 2 Définissez la politique VPN par application en utilisant le sélecteur d'application AnyConnect Enterprise.

Nous vous recommandons de créer une politique Allow All (Tout autoriser) simple et de définir les applications autorisées dans le gestionnaire de périphériques mobiles (MDM). Cependant, vous pouvez spécifier une liste d'applications à autoriser et contrôler la liste à partir de la tête de réseau. Si vous souhaitez inclure des applications spécifiques, créez une règle distincte pour chaque application en utilisant un nom convivial unique et l'identifiant d'application de l'application. Pour en savoir plus sur l'obtention des identifiants d'application, consultez Détermination des identifiants d'application des applications mobiles, à la page 27.

La procédure suivante explique comment créer une politique Allow All (Autoriser tout) qui prend en charge les plateformes Android et iOS.

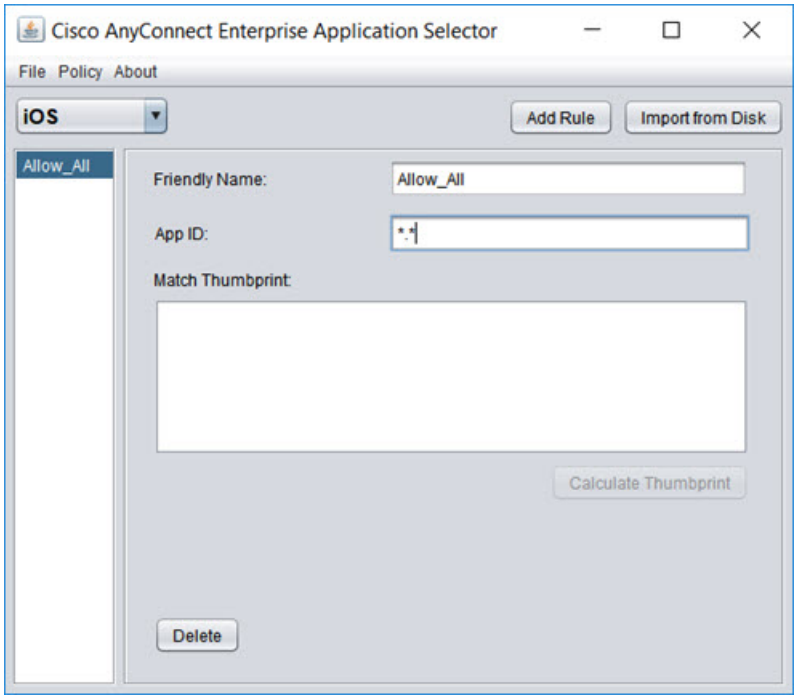
a) Dans le sélecteur d'application AnyConnect Enterprise, sélectionnez **Android** comme type de plateforme, puis complétez les options suivantes :

- **Friendly Name** (Nom convivial) : quelque chose de pertinent, comme **Allow_All** (Tout_permettre).
- **App ID** (Identifiant de l'application) : Entrer ***.*** pour correspondre à toutes les applications possibles.
- Ignorez tous les autres champs. Celles-ci sont utilisées pour définir une stratégie sur des applications et des versions exactes.



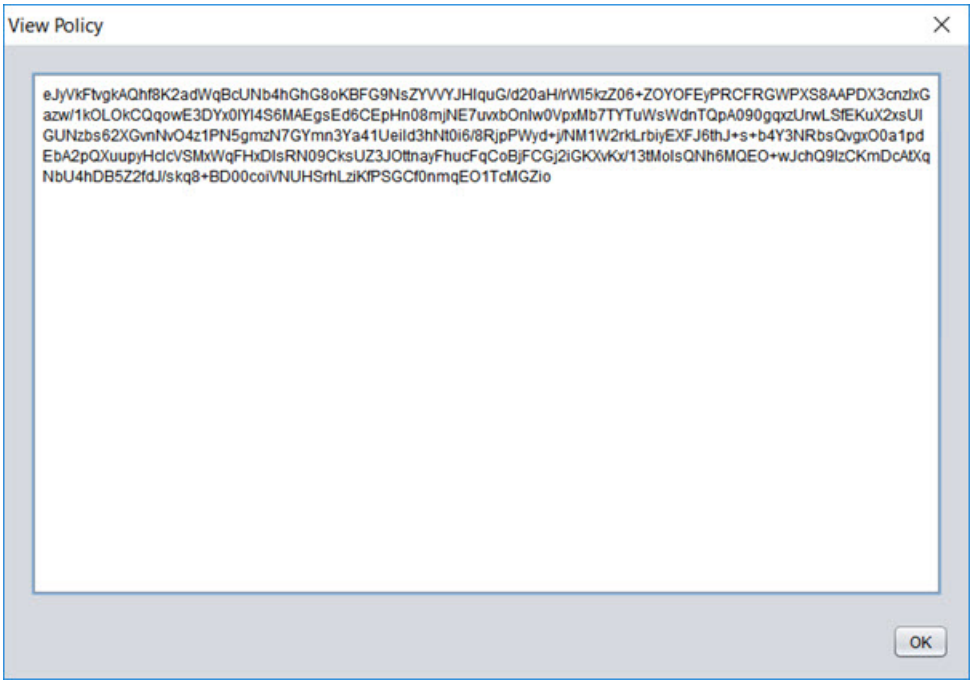
b) Sélectionnez **iOS** comme type de plateforme, puis complétez les options suivantes :

- **Friendly Name** (Nom convivial) : quelque chose de pertinent, comme **Allow_All** (Tout_permettre).
- **App ID** (Identifiant de l'application) : Entrer ***.*** pour correspondre à toutes les applications possibles.
- Ignorez tous les autres champs.



c) Sélectionnez **Policy** > **View Policy** (Politique, Afficher la politique).

Vous obtiendrez une chaîne base64 non lisible. Cette chaîne contient en fait un fichier XML chiffré que le système FTD décompressera pour afficher les politiques que vous avez créées. Vous utiliserez une copie de cette chaîne dans les étapes ultérieures.



Étape 3 Créez l'objet FlexConfig deploy-once/append qui crée l'attribut personnalisé perapp et affecte à l'attribut la politique par application base64 créée dans le sélecteur d'application AnyConnect Enterprise.

a) Choisissez **Objects** > **Object Management** (Objets, Gestion des objets).

b) Choisissez **FlexConfig** > **FlexConfig Object** (FlexConfig, Objets FlexConfig) dans la table des matières.

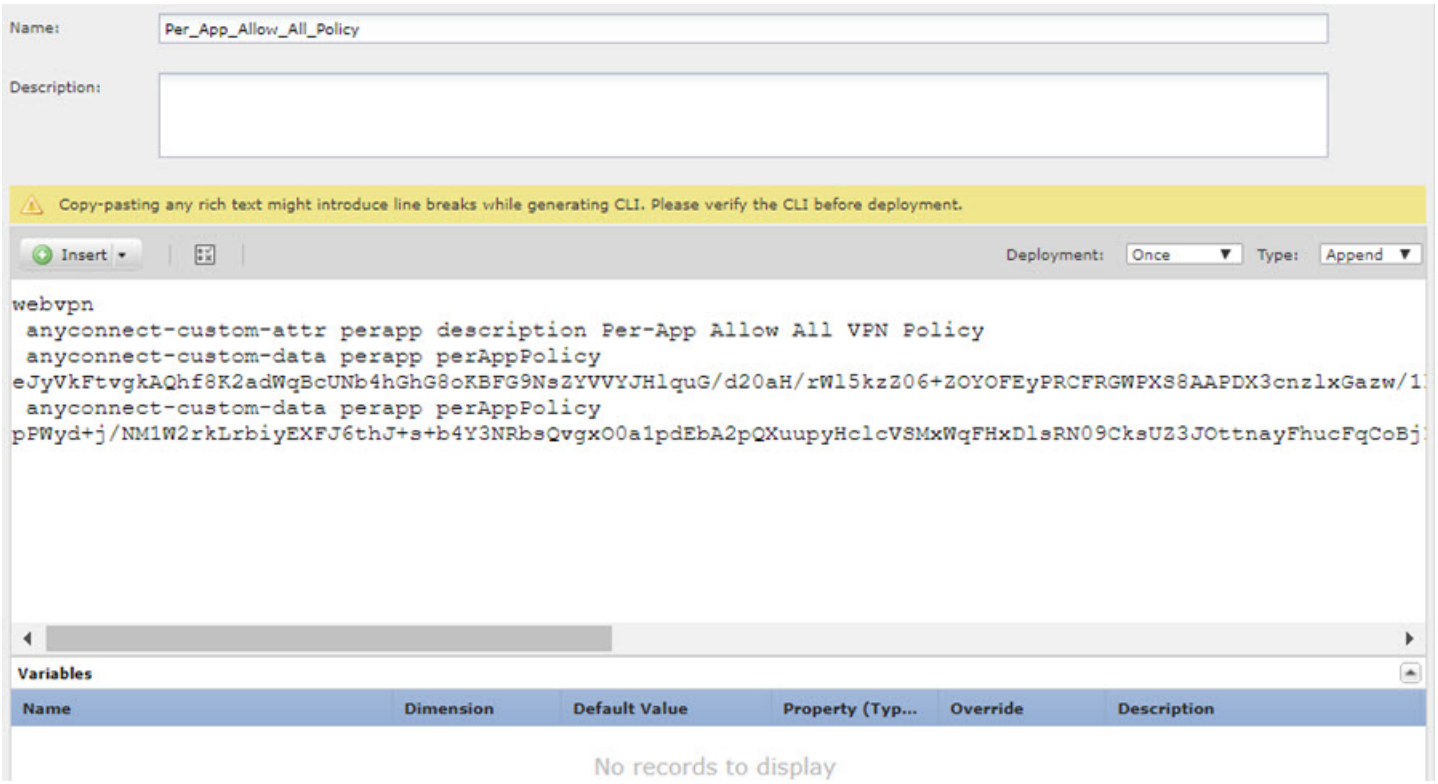
c) Cliquez sur **Add FlexConfig Object** (Ajouter un objet FlexConfig), configurez les propriétés suivantes, puis cliquez sur **Save** (Enregistrer).

- **Name** : nom de l'objet. Par exemple, Per_App_Allow_All_Policy.
- **Deployment** (Déploiement) : sélectionnez **Once** (une fois). Ces commandes doivent être configurées une seule fois.
- **Type** : conservez la valeur par défaut, **Append** (Ajouter). Les commandes sont envoyées à l'appareil après les commandes des fonctionnalités directement prises en charge.
- **Object body** (Corps de l'objet) : dans le corps de l'objet, tapez les commandes requises pour créer un attribut de type **perapp**, puis ajoutez les données, qui sont un nom d'attribut et la chaîne de politique base64. Notez que l'élément de données est limité à 420 caractères, donc si la chaîne base64 est plus longue que cela, vous devez la diviser et utiliser plusieurs commandes **anyconnect-custom-data**. Lorsque vous utilisez plusieurs commandes de données pour une variable donnée, la deuxième et les commandes suivantes sont simplement ajoutées à la chaîne de données initiale. Vous pouvez soit couper précisément la chaîne base64 à 420 caractères, soit la couper simplement en fragments faciles à gérer. Par exemple, pour créer un attribut nommé perAppPolicy et utiliser votre politique Allow_All, les commandes seront les suivantes. Notez que la description est facultative, mais si elle est incluse, il ne s'agit pas d'une commande distincte, mais fait partie de

la commande **anyconnect-custom-attr**. (Notez que dans cet exemple, les retours de ligne sont ajoutés pour améliorer la lecture.)

```
webvpn
 anyconnect-custom-attr perapp description Per-App Allow All VPN Policy
 anyconnect-custom-data perapp perAppPolicy
eJyVkFtvgkAQhf8K2adWqBcUNb4hGhG8oKBFG9NsZYVVYJHlquG/d20aH/rWl5kzZ06+
ZOYOFEyPRCFRGWPXS8AAPDX3cnzlxGazw/1kOLOkCQqowE3DYx0IYI4S6MAEgsEd6CEp
Hn08mjNE7uvxbOnIw0VpxMb7TYTuWsWdnTQpA090gqxzUrwLSfEKuX2xsUlGUNzbs62X
GvnNvO4z1PN5gmzN7GYmn3Ya41Ueild3hNt0i6/8Rj
 anyconnect-custom-data perapp perAppPolicy
pPWyd+j/NM1W2rkLrbiyEXFJ6thJ+s+b4Y3NRbsQvgxO0a1pdEbA2pQXuupyHclcVSMxW
qFHxDlsRN09CksUZ3JOttnayFhucFqCoBjFCGj2iGKXvKx/13tMoIsQNh6MQEO+wJchQ9
IzCKmDcAtXqNbU4hDB5Z2fdJ/skq8+BD00coiVNUHSrhLziKfPSGCf0nmqEO1TcMGZio
```

Le corps de l'objet doit ressembler à ce qui suit :



Étape 4 Si vous utilisez des politiques de groupe personnalisées, créez un objet FlexConfig deploy-once/append pour configurer l'attribut personnalisé de tunnellisation fractionnée dynamique dans les politiques de groupe.

Si vous utilisez la politique de groupe par défaut, nommée DfltGrpPolicy, créez un objet FlexConfig deploy-everytime/append pour configurer l'attribut personnalisé de tunnellisation fractionnée dynamique dans la politique de groupe. Vous devez déployer cet objet à chaque fois, car lors de chaque déploiement, le système annulera toute modification personnalisée de la politique par défaut.

Pour les politiques de groupe personnalisées, contrairement à la politique de groupe par défaut, le système n'annulera pas les modifications que vous apportez. Vous devez donc déployer les modifications une seule fois. Si vous utilisez plusieurs politiques de groupe, vous pouvez utiliser un seul objet FlexConfig pour ajouter l'attribut personnalisé à chaque politique à tour de rôle. Vous pouvez également créer un objet FlexConfig

par politique de groupe. Le résultat sera le même, le choix dépendra donc de vos propres exigences pour la modularisation de votre politique FlexConfig.

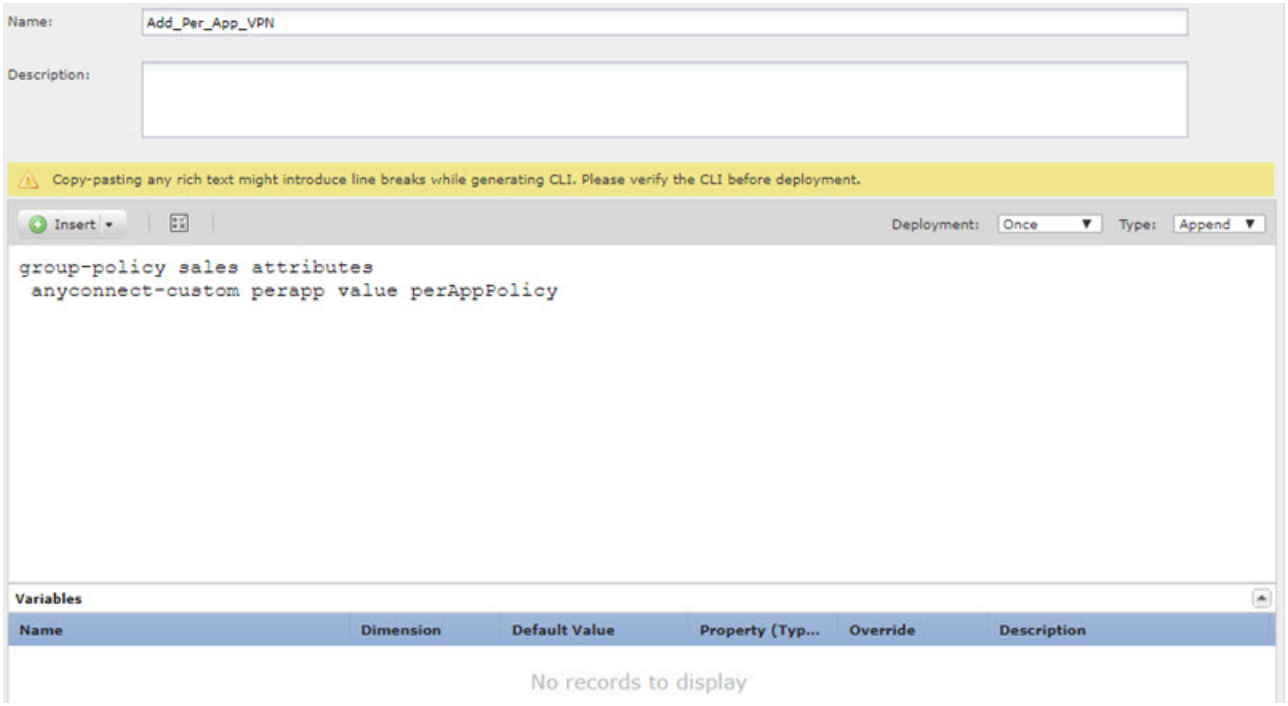
La procédure suivante concerne la politique de groupe personnalisée « sales » (ventes). Nous vous recommandons d'utiliser des groupes personnalisés plutôt que le groupe par défaut.

a) Choisissez **Objects** > **Object Management** (Objets, Gestion des objets).
b) Choisissez **FlexConfig** > **FlexConfig Object** (FlexConfig, Objets FlexConfig) dans la table des matières.
c) Cliquez sur **Add FlexConfig Object** (Ajouter un objet FlexConfig), configurez les propriétés suivantes, puis cliquez sur **Save** (Enregistrer).

- **Name** : nom de l'objet. Par exemple, Add_Per_App_VPN.
- **Deployment** (Déploiement) : sélectionnez **Once** (une fois).
- **Type** : conservez la valeur par défaut, **Append** (Ajouter).
- **Object body** (Corps de l'objet) : dans le corps de l'objet, tapez les commandes requises pour ajouter l'attribut personnalisé à la politique de groupe. Par exemple, si l'attribut que vous avez créé s'intitule perAppPolicy et que la politique de groupe s'intitule « sales » (ventes), les commandes sont les suivantes :

```
group-policy sales attributes
 anyconnect-custom perapp value perAppPolicy
```

Le corps de l'objet doit ressembler à ce qui suit :



Étape 5 Créez la politique FlexConfig qui déploie ces objets.

a) Sélectionnez **Devices** > **FlexConfig** (Appareils, FlexConfig).
b) Cliquez sur **New Policy** (Nouvelle politique) ou si une politique FlexConfig existante doit être affectée (ou est déjà affectée) aux appareils cibles, modifiez simplement cette dernière.

Lors de la création d'une nouvelle politique, affectez les appareils cibles à la politique dans la boîte de dialogue où vous nommez la politique.

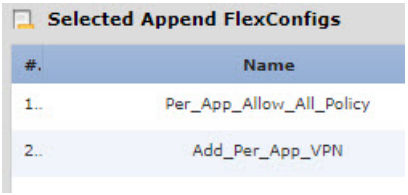
c) Utilisez Ctrl+clic pour sélectionner l'objet FlexConfig dans le dossier **User Defined** (Défini par l'utilisateur) dans la table des matières, puis cliquez sur > pour l'ajouter à la politique.

Les objets doivent être ajoutés à la liste **Selected Appended FlexConfigs** (FlexConfigs sélectionnées et ajoutées).

d) Utilisez le glisser-déposer pour vous assurer que les objets sont dans le bon ordre.

L'objet qui crée l'objet d'attribut personnalisé doit venir avant les objets qui attribuent cet attribut aux politiques de groupe. Sinon, si vous essayez d'ajouter un attribut personnalisé qui n'existe pas encore, vous obtiendrez une erreur.

La liste devrait ressembler à ce qui suit si vous avez un seul objet qui configure vos politiques de groupe personnalisées :



e) Cliquez sur **Save** (Enregistrer).

f) Si vous n'avez pas encore affecté tous les périphériques ciblés à la politique, cliquez sur le lien **Policy Affectations** (Affectations de politiques) ci-dessous Save and make the assignments now (Enregistrer et effectuer les affectations maintenant).

g) Cliquez sur **Preview Config** (Aperçu de la configuration et dans la boîte de dialogue d'aperçu, sélectionnez l'un des périphériques attribués.

Le système génère un aperçu de l'interface de ligne de commande de configuration qui sera envoyée au périphérique. Vérifiez que les commandes générées à partir de l'objet semblent correctes. Celles-ci seront affichées à la fin de l'aperçu. Notez que vous verrez également les commandes générées à partir d'autres modifications que vous avez apportées aux fonctionnalités gérées. En ce qui concerne ces commandes, le résultat devrait ressembler à ce qui suit :

```
###Flex-config Appended CLI ###
webvpn

 anyconnect-custom-attr perapp description Per-App Allow All VPN Policy

 anyconnect-custom-data perapp perAppPolicy eJyVkFtvgkAQhf8K2adWqBcUNb4hGh

 anyconnect-custom-data perapp perAppPolicy pPWyd+j/NM1W2rkLrbiyEXFJ6thJ+s

group-policy sales attributes

 anyconnect-custom perapp value perAppPolicy
```

Étape 6 Déployez vos modifications.

Étape 7 Vérifiez la configuration.

- Vous pouvez vérifier que les commandes ont été configurées sur chaque appareil FTD. Utilisez une session SSH avec l'appareil ou avec l'outil CLI dans FMC (**System** > **Health** > **Monitor** [Système,

Intégrité, Vérifier], cliquez sur l'appareil, puis sur **Advanced Troubleshooting** [Dépannage avancé], puis sélectionnez l'onglet **Threat Defense CLI**). Voici les commandes qui afficheront la configuration.

- **show running-config webvpn**
- **show running-config anyconnect-custom-data**
- **show running-config group-policy** *name*, (nom), où vous remplacez *name* par un nom de politique de groupe tel que sales (ventes).

- Vous pouvez vérifier que le système se comporte correctement à partir d'un client AnyConnect. Ouvrez les statistiques du client et recherchez les éléments suivants :
  - **Le mode du tunnel** doit indiquer « Application Tunnel » (Tunnel d'application) plutôt que « Tunnel All Traffic » (Tunnel tout le trafic).

  - **Tunneled Apps** (Applications tunnelisées) répertorie les applications que vous avez activées pour la tunnellisation dans le gestionnaire de périphérique mobile MDM.

Prochaine étape

Si vous ne souhaitez plus utiliser le VPN par application, vous devez créer un objet FlexConfig pour supprimer la configuration des appareils FTD. En outre, vous devrez retirer le gestionnaire des appareils mobiles; consultez la documentation du gestionnaire des appareils mobiles pour obtenir des instructions.

Pour la tête de réseau FTD, créez un objet FlexConfig Deploy-once/append qui contient les commandes nécessaires pour supprimer l'attribut personnalisé de chaque politique de groupe qui l'utilise, puis supprimez l'attribut personnalisé. Par exemple, si l'attribut personnalisé est utilisé par deux politiques de groupe, DfltGrpPolicy et sales (ventes), et que l'attribut est nommé perAppPolicy, les commandes seraient les suivantes :

```
group-policy DfltGrpPolicy attributes
 no anyconnect-custom perapp
```

```
group-policy sales attributes
 no anyconnect-custom perapp

no anyconnect-custom-data perapp perAppPolicy

webvpn
 no anyconnect-custom-attr perapp
```

Ensuite, dans la politique FlexConfig, supprimez les objets qui créent et attribuent l'attribut, puis ajoutez ce nouvel objet. Déployez la configuration et la fonctionnalité par application sera supprimée des politiques de groupe.

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.