VPN d'accès à distance

Le réseau privé virtuel (VPN) d'accès à distance permet aux utilisateurs individuels de se connecter à votre réseau à partir d'un emplacement distant à l'aide d'un ordinateur ou d'autres périphériques pris en charge connectés à Internet. Cela permet aux collaborateurs mobiles de se connecter à partir de leur réseau domestique ou d'un réseau Wi-Fi public, par exemple.

Les rubriques suivantes expliquent comment configurer le VPN d'accès à distance pour votre réseau.

Aperçu du VPN d'accès à distance

Vous pouvez utiliser FDM pour configurer le VPN d'accès à distance sur SSL à l'aide du logiciel client AnyConnect.

Lorsque le client AnyConnect client négocie une connexion SSL VPN avec le FTD périphérique, il se connecte à l'aide de Transport Layer Security (TLS) ou de Datagram Transport Layer Security (DTLS). L'utilisation de DTLS évite les problèmes de latence et de bande passante associés à certaines connexions SSL et améliore la performance des applications en temps réel sensibles aux retards de paquets. Le client et le périphérique FTD négocient la version TLS/DTLS à utiliser. DTLS est utilisé si le client le prend en charge.

Nombre maximal de sessions VPN simultanées par modèle de périphérique

Il y a une limite maximale au nombre de sessions VPN d'accès à distance simultanées autorisées sur un périphérique en fonction du modèle de périphérique. Cette limite est conçue pour que les performances du système ne se dégradent pas à des niveaux inacceptables. Utilisez ces limites pour la planification de la capacité.

Modèle du périphérique	Maximum de sessions VPN d'accès à distance simultanées
Firepower 1010	75

Modèle du périphérique	Maximum de sessions VPN d'accès à distance simultanées
Firepower 1120	150
Firepower 1140	400
Firepower de la série 2110	1 500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10 000
Secure Firewall 3110	3 000
Secure Firewall 3120	6000
Secure Firewall 3130	15 000
Secure Firewall 3140	20 000
Firepower 4100, tous les modèles	10 000
Appareils Cisco Firepower de série 9300, tous les modèles	20 000
FTDv: FTDv5	50
FTDv: FTDv10, FTDv20, FTDv30	250
FTDv: FTDv50	750
FTDv: FTDv100	10 000
ISA 3000	25

Téléchargement du logiciel client AnyConnect

Avant de pouvoir configurer un VPN d'accès à distance, vous devez télécharger le logiciel client AnyConnect sur votre ordinateur. Vous devrez charger ces paquets lors de la définition du VPN.

Vous devez télécharger la dernière version client AnyConnect pour vous assurer de disposer des dernières fonctionnalités, des corrections de bogues et des correctifs de sécurité. Mettez régulièrement à jour les paquets sur le périphérique Cisco Firepower Threat Defense.

Remarque Vous pouvez charger un paquet client AnyConnect par système d'exploitation : Windows, Mac et Linux. Vous ne pouvez pas charger plusieurs versions pour un type de système d'exploitation donné.

Obtenez les paquets de logiciels client AnyConnect depuis software.cisco.com. Vous devez télécharger les versions « Full Installation Package » (ensemble d'installation complet) des clients.

Comment les utilisateurs peuvent installer le logiciel client AnyConnect

Pour établir une connexion VPN, vos utilisateurs doivent installer le logiciel client AnyConnect. Vous pouvez utiliser vos méthodes de distribution de logiciels existantes pour installer le logiciel directement. Vous pouvez également faire en sorte que les utilisateurs installent client AnyConnect directement à partir du périphérique FTD.

Les utilisateurs doivent avoir des droits d'administrateur sur leur poste de travail pour installer le logiciel.

Une fois le client AnyConnect installé, si vous chargez de nouvelles versions client AnyConnect sur le système, le client AnyConnect détectera la nouvelle version lors de la prochaine connexion VPN effectuée par l'utilisateur. Le système invitera automatiquement l'utilisateur à télécharger et à installer le logiciel client mis à jour. Cette automatisation simplifie la distribution des logiciels pour vous et vos clients.

Si vous décidez que les utilisateurs installent initialement le logiciel à partir du périphérique FTD, demandez aux utilisateurs de procéder comme suit.

Remarque Les utilisateurs d'Android et d'iOS doivent télécharger client AnyConnect à partir de l'App Store approprié.

Procédure

Étape 1 À l'aide d'un navigateur Web, ouvrez **https://***ravpn-address*, où *ravpn-address* est l'adresse IP ou le nom d'hôte de l'interface externe sur laquelle vous autorisez les connexions VPN.

Vous identifiez cette interface lorsque vous configurez le VPN d'accès à distance. Le système invite l'utilisateur à se connecter.

Si vous avez modifié le port pour les connexions VPN d'accès à distance, les utilisateurs doivent inclure le port personnalisé dans l'URL. Par exemple : si vous avez changé le port en 4443 : https://ravpn.example.com:4443

Étape 2 Connectez-vous au site.

Les utilisateurs sont authentifiés à l'aide du serveur de répertoire configuré pour le VPN d'accès à distance. La connexion doit être réussie pour continuer.

Si la connexion a réussi, le système détermine si l'utilisateur dispose déjà de la version requise de client AnyConnect. Si client AnyConnect est absent de l'ordinateur de l'utilisateur ou s'il est de niveau inférieur, le système commence automatiquement l'installation du logiciel client AnyConnect.

Lorsque l'installation est terminée, client AnyConnect termine la connexion VPN d'accès à distance.

Contrôle des autorisations et des attributs des utilisateurs à l'aide de RADIUS et des stratégies de groupe

Vous pouvez appliquer des attributs d'autorisation d'utilisateur (également appelés droits ou autorisations d'utilisateur) aux connexions VPN RA à partir d'un serveur RADIUS externe ou d'une politique de groupe définie sur le périphérique Cisco Firepower Threat Defense. Si le périphérique Cisco Firepower Threat Defense

reçoit des attributs du serveur AAA externe qui sont en conflit avec ceux configurés dans la politique de groupe, les attributs du serveur AAA prévalent toujours.

Le périphérique Cisco Firepower Threat Defense applique les attributs dans l'ordre suivant :

1. Attributs de l'utilisateur sur le serveur AAA externe : le serveur renvoie ces attributs une fois l'authentification ou l'autorisation de l'utilisateur réussie.
2. Politique de groupe configurée sur le périphérique Cisco Firepower Threat Defense : si un serveur RADIUS renvoie la valeur de l'attribut de classe RADIUS IETF-Class-25 (OU= group-policy) pour l'utilisateur, le périphérique place l'utilisateur dans la politique de groupe du même nom et applique les attributs de la politique de groupe qui ne sont pas renvoyés par le serveur.Cisco Firepower Threat Defense
3. Politiques de groupe affectées par le profil de connexion (également appelé groupes de tunnels) : le profil de connexion contient les paramètres préliminaires pour la connexion et comprend une politique de groupe par défaut appliquée à l'utilisateur avant l'authentification. Tous les utilisateurs se connectant au périphérique Cisco Firepower Threat Defense appartiennent initialement à ce groupe, qui fournit tous les attributs manquants dans les attributs d'utilisateur renvoyés par le serveur AAA ou dans la politique de groupe attribuée à l'utilisateur.

Les périphériques FTD prennent en charge les attributs avec l'ID de fournisseur 3076. Si le serveur RADIUS que vous utilisez ne comporte pas ces attributs définis, vous devez les définir manuellement. Pour définir un attribut, utilisez le nom ou le numéro d'attribut, le type, la valeur et le code du fournisseur (3076).

Les rubriques suivantes expliquent les attributs pris en charge selon que les valeurs sont définies dans le serveur RADIUS ou s'il s'agit de valeurs que le système envoie au serveur RADIUS.

Attributs envoyés au serveur RADIUS

Les attributs RADIUS 146 et 150 sont envoyés du périphérique Cisco Firepower Threat Defense au serveur RADIUS pour les demandes d'authentification et d'autorisation. Tous les attributs suivants sont envoyés du périphérique Cisco Firepower Threat Defense au serveur RADIUS pour les demandes de démarrage, de mise à jour provisoire et d'arrêt de gestion.

Tableau 1 : Attributs FTD envoyés à RADIUS

Attribut	Numéro de l'attribut	Syntaxe, type	Valeur unique ou valeurs multiples	Description ou valeur
Type de client	150	nombre entier	Unique	Le type de client qui se connecte au VPN : 2 = client AnyConnect VPN SSL
Type de séance	151	nombre entier	Unique	Le type de connexion : 1 = client AnyConnect VPN SSL
Tunnel Group Name	146	Chaîne	Unique	Le nom du profil de connexion qui a été utilisé pour établir la session, tel qu'il est défini sur le périphérique Cisco Firepower Threat Defense. Ce nom peut comporter de 1 à 253 caractères.

Attributs reçus du serveur RADIUS

Les attributs d'autorisation utilisateur suivants sont envoyés au périphérique Cisco Firepower Threat Defense par le serveur RADIUS.

Tableau 2 : Attributs RADIUS envoyés à FTD

Attribut	Numéro de l'attribut	Syntaxe, type	Valeur unique ou valeurs multiples	Description ou valeur
Liste d'accès entrant	86	Chaîne	Unique	Les deux attributs Access-List (Liste d'accès) prennent le nom d'une ACL configurée sur le périphérique Cisco Firepower Threat Defense. Créez ces ACLs en utilisant le type d'objet Smart CLI Extended Access List (liste d'accès étendue Smart CLI) (sélectionnez **Device (périphérique)** > **Advanced Configuration (configuration avancée)** > **Smart CLI** > **Objects (objets)**). Ces listes de contrôle d'accès contrôlent le flux du trafic dans le sens entrant (trafic entrant sur le périphérique Cisco Firepower Threat Defense) ou sortant (trafic sortant du périphérique Cisco Firepower Threat Defense.
Liste d'accès sortante	87	Chaîne	Unique	
Ensembles des adresses	217	Chaîne	Unique	Le nom d'un objet réseau défini sur le périphérique Cisco Firepower Threat Defense qui identifie un sous-réseau, qui sera utilisé comme groupement d'adresses pour les clients se connectant au VPN d'accès à distance. Définissez l'objet réseau dans la page **Objects** (objets).
Banner1	15	Chaîne	Unique	Bannière à afficher lorsque l'utilisateur se connecte.
Banner2	36	Chaîne	Unique	La deuxième partie de la bannière à afficher lorsque l'utilisateur se connecte. Bannière2 est ajouté à Bannière1.
Politique de groupe	25	Chaîne	Unique	La politique de groupe à utiliser dans la connexion. Vous devez créer la politique de groupe sur la page **Group Policy** (politique de groupe) du VPN d'accès à distance. Vous pouvez utiliser l'un des formats suivants : • *nom de la politique de groupe* • OU=*nom de la politique de groupe* • OU=*nom de la politique de groupe*;
Connexions simultanées	2	nombre entier	Unique	Nombre de connexions simultanées distinctes que l'utilisateur est autorisé à établir, 0 à 2147483647.

Attribut	Numéro de l'attribut	Syntaxe, type	Valeur unique ou valeurs multiples	Description ou valeur
VLAN	140	nombre entier	Unique	Le VLAN dans lequel limiter la connexion de l'utilisateur, 0 à 4094. Vous devez également configurer ce VLAN sur une sous-interface du périphérique Cisco Firepower Threat Defense.

Authentification à deux facteurs

Vous pouvez configurer l'authentification à deux facteurs pour le VPN RA. Avec l'authentification à deux facteurs, l'utilisateur doit fournir un nom d'utilisateur et un mot de passe statiques, ainsi qu'un élément supplémentaire comme un jeton RSA ou un code d'accès Duo. L'authentification à deux facteurs diffère de l'utilisation d'une deuxième source d'authentification en ce sens que l'authentification à deux facteurs est configurée sur une source d'authentification unique, la relation avec le serveur RSA/Duo étant liée à la source d'authentification principale. L'exception est Duo LDAP, où vous configurez le serveur LDAP Duo comme source d'authentification secondaire.

Le système a été testé avec des jetons RSA et des codes d'accès Duo envoyés à Duo Mobile pour le deuxième facteur, conjointement avec tout serveur RADIUS ou AD comme premier facteur dans le processus d'authentification à deux facteurs.

Authentification à deux facteurs RSA

Vous pouvez configurer RSA en utilisant l'une des approches suivantes. Consultez la documentation de RSA pour obtenir des renseignements sur la configuration côté RSA.

- Définissez le serveur RSA directement dans FDM en tant que serveur RADIUS, et utilisez ce serveur comme source d'authentification principale dans le VPN d'accès à distance.

  Lorsqu'il utilise cette approche, l'utilisateur doit s'authentifier à l'aide d'un nom d'utilisateur configuré sur le serveur RADIUS RSA, puis concaténer le mot de passe avec le jeton RSA temporaire à usage unique, en séparant le mot de passe et le jeton par une virgule : *password*,*token*.

  Dans cette configuration, il est courant d'utiliser un serveur RADIUS distinct (comme celui fourni dans Cisco ISE) pour fournir les services d'autorisation. Vous devez configurer le deuxième serveur RADIUS en tant qu'autorisation et, éventuellement, serveur de comptabilité.

- Intégrer le serveur RSA avec un serveur RADIUS ou AD qui prend en charge l'intégration directe, et configurer le VPN d'accès à distance pour utiliser le serveur RADIUS ou AD non RSA comme source d'authentification principale. Dans ce cas, le serveur RADIUS/AD utilise RSA-SDI pour déléguer et orchestrer l'authentification à deux facteurs entre le client et le serveur RSA.

  Lorsqu'il utilise cette approche, l'utilisateur doit s'authentifier à l'aide d'un nom d'utilisateur configuré sur le serveur RADIUS ou AD, et concaténer le mot de passe avec le jeton RSA à usage unique temporaire, en séparant le mot de passe et le jeton par une virgule : *password*,*token*.

  Dans cette configuration, vous utilisez également le serveur RADIUS non RSA comme serveur d'autorisation et, éventuellement, serveur de comptabilité.

Authentification à deux facteurs Duo au moyen de RADIUS

Vous pouvez configurer le serveur RADIUS Duo comme source d'authentification principale. Cette approche utilise le serveur mandataire d'authentification RADIUS Duo.

Pour les étapes détaillées de la configuration de Duo, consultez https://duo.com/docs/cisco-firepower.

Vous devez ensuite configurer Duo pour transférer les demandes d'authentification dirigées vers le serveur mandataire pour utiliser un autre serveur RADIUS, ou un serveur AD, comme premier facteur d'authentification et le service en nuage Duo comme deuxième facteur.

Lorsqu'il utilise cette approche, l'utilisateur doit s'authentifier à l'aide d'un nom d'utilisateur configuré sur le mandataire d'authentification Duo et le serveur RADIUS/AD associé, et le mot de passe pour le nom d'utilisateur configuré dans le serveur RADIUS/AD, suivi de l'un des codes Duo suivants :

- *Duo-passcode*. Par exemple, *my-password*,**12345**.
- **push**. Par exemple, *mon-motdepasse*,**push**. Utilisez **push** pour demander à Duo d'envoyer une authentification push à l'application Duo Mobile, que l'utilisateur doit déjà avoir installée et enregistrée.
- **sms**. Par exemple, *mon-motdepasse*,**sms**. Utilisez **sms** pour demander à Duo d'envoyer un message SMS avec un nouveau lot de codes d'authentification au périphérique mobile de l'utilisateur. La tentative d'authentification de l'utilisateur échouera lors de l'utilisation de **sms**. L'utilisateur doit ensuite s'authentifier de nouveau et saisir le nouveau mot de passe comme facteur secondaire.
- **phone**. Par exemple, *mon-motdepasse*,**phone**. Utilisez **phone** pour demander à Duo d'effectuer l'authentification par rappel téléphonique.

Si le nom d'utilisateur/mot de passe est authentifié, le mandataire d'authentification Duo contacte le service en nuage Duo, qui valide que la demande provient d'un appareil mandataire configuré valide, puis envoie un code d'accès temporaire au périphérique mobile de l'utilisateur, comme indiqué. Lorsque l'utilisateur accepte ce code d'accès, la session est marquée comme authentifiée par Duo et le VPN d'accès à distance est établi.

Authentification à deux facteurs Duo avec LDAP

Vous pouvez utiliser le serveur LDAP Duo comme source d'authentification secondaire en conjonction avec un serveur Microsoft Active Directory (AD) ou RADIUS comme source principale. Avec Duo LDAP, l'authentification secondaire valide l'authentification principale avec un code d'accès Duo, une notification poussée ou un appel téléphonique.

Le périphérique Cisco Firepower Threat Defense communique avec Duo LDAP à l'aide de LDAPS sur le port TCP/636.

Notez que le serveur LDAP Duo fournit des services d'authentification uniquement, il ne fournit pas de services d'identité. Ainsi, si vous utilisez Duo LDAP comme source d'authentification principale, vous ne verrez pas les noms d'utilisateurs associés aux connexions VPN d'accès à distance dans les tableaux de bord, et vous ne pourrez pas écrire de règles de contrôle d'accès pour ces utilisateurs.

Lorsqu'il utilise cette approche, l'utilisateur doit s'authentifier à l'aide d'un nom d'utilisateur configuré à la fois sur le serveur RADIUS/AD et sur le serveur LDAP Duo. Lorsqu'il est invité à se connecter par le client AnyConnect, l'utilisateur fournit le mot de passe RADIUS/AD dans le champ **Password** (Mot de passe) principal et, dans **Secondary Password** (Mot de passe secondaire), fournit l'un des éléments suivants pour s'authentifier auprès de Duo. Pour en savoir plus, consultez https://guide.duo.com/anyconnect.

- *Duo passcode* (Code d'accès Duo) : authentifiez-vous à l'aide d'un code d'accès, généré avec Duo Mobile, envoyé par SMS, généré par votre jeton matériel ou fourni par un administrateur. Par exemple, 1234567.

- **push** (Notification poussée) : envoyez une demande de connexion à votre téléphone, si vous avez installé et activé l'application Duo Mobile. Passez en revue la demande et appuyez sur **Approve** (Approuver) pour vous connecter.
- **Téléphone** : authentifiez-vous à l'aide d'un rappel téléphonique.
- **SMS** : demandez un code d'accès Duo dans un message texte. La tentative de connexion échouera. Connectez-vous à nouveau en utilisant le nouveau code d'accès.

Pour une explication détaillée et un exemple d'utilisation de Duo LDAP, consultez Comment configurer l'authentification à deux facteurs à l'aide de Duo LDAP, à la page 43.

Exigences de licence pour le VPN d'accès à distance

Votre licence de périphérique de base doit respecter les exigences d'exportation avant que vous puissiez configurer le VPN d'accès à distance. Lorsque vous enregistrez le périphérique, vous devez le faire avec un compte Smart Software Manager qui est activé pour les fonctionnalités d'exportation contrôlée. Vous ne pouvez pas non plus configurer la fonctionnalité à l'aide de la licence d'évaluation.

En outre, vous devez acheter et activer une licence VPN d'accès à distance, l'une des licences suivantes : AnyConnect Plus, AnyConnect Apex, ou VPN AnyConnect . Ces licences sont traitées de la même manière pour les périphériques FTD, même si elles sont conçues pour permettre différents ensembles de fonctionnalités lorsqu'elles sont utilisées avec des têtes de réseau ASA basées sur le logiciel.

Pour activer la licence, sélectionnez **Device (Périphérique)** > **Smart License (Licence Smart)** > **View Configuration (Afficher la configuration)**, puis sélectionnez la licence appropriée dans le groupe de licences RA VPN License (Licence VPN RA). La licence doit être disponible dans votre compte Smart Software Manager. Pour en savoir plus sur l'activation des licences, consultez Activation ou désactivation des licences facultatives.

Pour plus d'informations, voir le *Guide de commande Cisco AnyConnect*, http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf. D'autres fiches techniques sont également disponibles sur http://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/datasheet-listing.html.

Consignes et limites pour le VPN d'accès à distance

Veuillez tenir compte des consignes et limitations suivantes lors de la configuration du VPN d'accès à distance.

- Vous ne pouvez pas configurer à la fois l'accès (accès HTTPS dans la liste d'accès de gestion) FDM et le VPN SSL d'accès à distance sur la même interface, pour le même port TCP. Par exemple, si vous configurez le VPN SSL d'accès distant sur l'interface externe, vous ne pouvez pas ouvrir aussi l'interface externe pour les connexions HTTPS sur le port 443. Si vous configurez les deux fonctionnalités sur la même interface, veillez à modifier le port HTTPS d'au moins l'un de ces services pour éviter un conflit.
- L'interface externe du VPN d'accès à distance est un paramètre global. Vous ne pouvez pas configurer des profils de connexion distincts sur différentes interfaces.
- Vous ne pouvez pas utiliser des adresses qui se chevauchent dans l'adresse source d'une règle NAT et d'un ensemble d'adresses VPN d'accès à distance.
- Si vous configurez l'authentification à deux facteurs à l'aide des tokens RADIUS et RSA, le délai d'expiration d'authentification par défaut de 12 secondes est trop court pour permettre une authentification

réussie dans la plupart des cas. Vous pouvez augmenter la valeur du délai d'expiration d'authentification en créant un profil client AnyConnect personnalisé et en l'appliquant au profil de connexion VPN d'accès à distance (RA VPN), comme décrit dans Configurer et charger les profils client AnyConnect, à la page 11. Nous recommandons un délai d'authentification d'au moins 60 secondes, afin que les utilisateurs aient suffisamment de temps pour s'authentifier, puis coller le token RSA, et pour la vérification aller-retour du token.

- L'émission de commandes telles que **curl** sur la tête de réseau du VPN d'accès à distance n'est pas directement prise en charge et pourrait ne pas donner les résultats souhaitables. Par exemple, la tête de réseau ne répond pas aux requêtes HTTP HEAD.

Configuration du VPN d'accès à distance

Pour activer le VPN d'accès à distance pour vos clients, vous devez configurer un certain nombre d'éléments distincts. La procédure suivante explique le processus de bout en bout.

Procédure

Étape 1 Configurer les licenses.

Vous devez activer deux licences :

- Lorsque vous enregistrez le périphérique, vous devez le faire avec un compte Smart Software Manager qui est activé pour les fonctionnalités d'exportation contrôlée. La licence de base doit respecter les exigences de contrôle des exportations avant de pouvoir configurer le VPN d'accès à distance. Vous ne pouvez pas non plus configurer la fonctionnalité à l'aide de la licence d'évaluation. Pour la procédure d'enregistrement du périphérique, consultez Enregistrement de l'appareil.
- Une licence VPN d'accès à distance. Pour de plus amples renseignements, consultez la section Exigences de licence pour le VPN d'accès à distance, à la page 8. Pour activer la licence, consultez Activation ou désactivation des licences facultatives.

Étape 2 Configurer les certificats.

Les certificats sont requis pour authentifier les connexions SSL entre les clients et le périphérique. Vous pouvez utiliser le DefaultInternalCertificate (Certificat interne par défaut) prédéfini pour le VPN, ou créer le vôtre.

Si vous utilisez une connexion chiffrée pour le domaine de répertoire utilisé pour l'authentification, vous devez charger un certificat d'autorité de certification de confiance.

Pour en savoir plus sur les certificats et la façon de les charger, consultez Configuration des certificats.

Étape 3 (Facultatif) Configurer les paramètres TLS/SSL.

Par défaut, le système permettra aux utilisateurs distants de se connecter au VPN d'accès à distance en utilisant toute version TLS et tout chiffrement pris en charge par le système. Cependant, vous pouvez limiter les versions TLS/DTLS, les chiffrements et les groupes Diffie-Hellman autorisés pour appliquer une connexion plus sécurisée. Consultez Configuration des paramètres de chiffrement TLS/SSL.

Étape 4 (Facultatif) Configurer et charger les profils client AnyConnect, à la page 11.

Étape 5 Configurer la source d'identité utilisée pour l'authentification des utilisateurs distants.

Vous pouvez utiliser les sources suivantes pour les comptes utilisateurs autorisés à se connecter au VPN d'accès à distance. Vous pouvez également utiliser des certificats clients pour l'authentification, seuls ou associés à une source d'identité.

- Active Directory identity realm (Domaine d'identité Active Directory) : en tant que source d'authentification principale. Les comptes d'utilisateur sont définis dans votre serveur Active Directory (AD). Consultez Configuration des domaines d'identité AD.
- RADIUS server group (Groupe de serveurs RADIUS) : en tant que source d'authentification principale ou secondaire, ainsi que pour l'autorisation et la comptabilité. Consultez Configuration des groupes de serveurs RADIUS.
- LocalIdentitySource (Base de données locale des utilisateurs) : en tant que source principale ou de repli. Vous pouvez définir des utilisateurs directement sur le périphérique et ne pas utiliser de serveur externe. Si vous utilisez la base de données locale comme source de secours, veillez à définir les mêmes noms d'utilisateur/mots de passe locaux que ceux définis dans le serveur externe. Consultez Configurer les utilisateurs locaux.
- Duo LDAP server (Serveur LDAP Duo) : en tant que source d'authentification principale ou secondaire. Bien que vous puissiez utiliser un serveur LDAP Duo comme source principale, il ne s'agit pas de la configuration normale. Vous l'utilisez normalement comme source secondaire pour fournir une authentification à deux facteurs en conjonction avec un serveur Active Directory ou RADIUS principal. Pour de plus amples renseignements, consultez la section Comment configurer l'authentification à deux facteurs à l'aide de Duo LDAP, à la page 43.

Étape 6 (Facultatif) Configurer les politiques de groupe pour le VPN d'accès à distance, à la page 25

La politique de groupe définit les attributs liés à l'utilisateur. Vous pouvez configurer des politiques de groupe pour fournir un accès différentiel aux ressources en fonction de l'appartenance au groupe. Vous pouvez également utiliser la politique par défaut pour toutes les connexions.

Étape 7 Configurer un profil de connexion VPN d'accès à distance, à la page 16.

Étape 8 Autoriser le trafic par le VPN d'accès à distance, à la page 13.

Étape 9 Vérifier la configuration VPN d'accès à distance, à la page 14.

Si vous rencontrez des problèmes pour effectuer une connexion, consultez Dépannage des VPN d'accès à distance, à la page 32.

Étape 10 (Facultatif) Activez la politique d'identité et configurez une règle pour l'authentification passive.

Si vous activez l'authentification passive des utilisateurs, les utilisateurs qui se sont connectés par le biais du VPN d'accès à distance seront affichés dans les tableaux de bord et ils seront également disponibles en tant que critères de correspondance de trafic dans les politiques. Si vous n'activez pas l'authentification passive, les utilisateurs de VPN d'accès à distance ne seront disponibles que s'ils correspondent à une politique d'authentification active. Vous devez activer la politique d'identité pour obtenir des informations de nom d'utilisateur dans les tableaux de bord ou pour la correspondance du trafic.

Configurer et charger les profils client AnyConnect

Les profils client AnyConnect sont téléchargés sur les clients avec le logiciel client AnyConnect. Ces profils définissent de nombreuses options liées au client, telles que la connexion automatique au démarrage et la reconnexion automatique, et si l'utilisateur final peut modifier l'option à partir des client AnyConnect préférences et des paramètres avancés.

Si vous configurez un nom d'hôte complet (FQDN) pour l'interface externe lors de la configuration de la connexion VPN d'accès à distance, le système crée un profil client pour vous. Ce profil active les paramètres par défaut. Vous ne devez créer et téléverser des profils client que si vous souhaitez un comportement autre que celui par défaut. Notez que les profils clients sont facultatifs : si vous n'en chargez pas, client AnyConnect utilisera les paramètres par défaut pour toutes les options contrôlées par profil.

Remarque Vous devez inclure l'interface externe du périphérique FTD dans la liste des serveurs du profil VPN pour que le client AnyConnect affiche tous les paramètres contrôlables par l'utilisateur lors de la première connexion. Si vous n'ajoutez pas l'adresse ou le nom de domaine complet (FQDN) en tant qu'entrée d'hôte dans le profil, les filtres ne s'appliquent pas à la session. Par exemple, si vous créez une correspondance de certificat et que le certificat correspond correctement aux critères, mais que vous n'ajoutez pas le périphérique en tant qu'entrée d'hôte dans ce profil, la correspondance de certificat est ignorée.

Vous pouvez créer des profils pour le client AnyConnect ainsi que pour une variété de modules que vous pouvez éventuellement utiliser avec client AnyConnect, comme l'activateur AMP. Bien que vous puissiez charger des profils pour n'importe lequel de ces modules, le FDM prend en charge la création du profil client AnyConnect uniquement. Cependant, vous pouvez charger n'importe quel type de profil par l'intermédiaire de FDM, puis utiliser l'API FTD (à partir d'API Explorer) pour modifier le type de profil de l'objet. La page des profils affiche tous les profils de tout type, bien que la liste n'indique pas le type de profil. La procédure explique comment procéder.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de profil client AnyConnect tout en modifiant une propriété de profil en cliquant sur le lien **Create New AnyConnect Client Profile (Créer un nouveau profil client AnyConnect)** affiché dans la liste des objets.

Avant de commencer

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

- Téléchargez et installez l'installateur autonome « Profile Editor - Windows / Standalone installer (MSI) ».client AnyConnect Le fichier d'installation est destiné à Windows uniquement et il est intitulé anyconnect-profileeditor-win-<version>-k9.msi, où <version> correspond à la version d'AnyConnect (le nom de fichier peut être modifié).client AnyConnect Par exemple, anyconnect-profileeditor-win-4.3.04027-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 client AnyConnect auprès de software.cisco.com. Notez que ce paquet contient tous les éditeurs de profils, pas seulement celui du client VPN.
- Utilisez l'éditeur de profils pour créer les profils dont vous avez besoin. Vous devez préciser le nom d'hôte ou l'adresse IP de l'interface externe dans le profil. Pour des informations détaillées, consultez l'aide en ligne de l'éditeur.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **AnyConnect Client Profiles (Profils client AnyConnect)** dans la table des matières.

Étape 2 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton **+**.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.
- Pour télécharger le profil associé à un objet, cliquez sur l'icône de téléchargement ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 3 Saisissez un nom et, facultativement, une description pour l'objet.

Si vous chargez un profil de module, utilisez le nom de l'objet pour indiquer le type de module afin de vous permettre de le différencier plus facilement des profils client AnyConnect.

Étape 4 Cliquez sur **Upload** (Charger) et sélectionnez le fichier que vous avez créé à l'aide de l'éditeur de profil.

Étape 5 Cliquez sur **Open** (ouvrir) pour téléverser le profil.

Étape 6 Cliquez sur **OK** pour ajouter l'objet.

Étape 7 Si le profil que vous avez créé est en fait d'un type différent du profil client AnyConnect, procédez comme suit pour modifier le type de profil de l'objet.

a) Cliquez sur le bouton des autres options ( ) et choisissez **API Explorer** (Explorateur d'interface de protocole d'application).

Le système ouvre l'explorateur d'interface de protocole d'application dans un onglet ou une fenêtre distincte, en fonction des paramètres de votre navigateur.

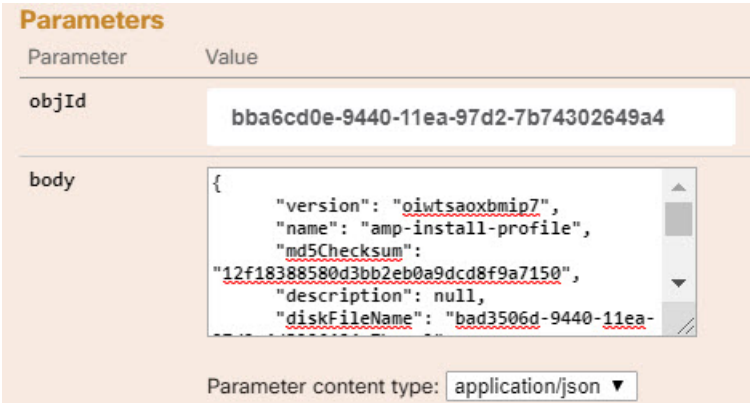
b) Ouvrez la ressource AnyConnectClientProfile.

c) Sélectionnez la méthode GET /object/anyconnectclientprofiles et cliquez sur le bouton **Try It Out!** (Essayez-le !).

Chaque objet de profil sera représenté comme suit. L'attribut en surbrillance est celui que vous devez modifier.

```
{
      "version": "oiwtsaoxbmip7",
      "name": "amp-install-profile",
      "md5Checksum": "12f18388580d3bb2eb0a9dcd8f9a7150",
      "description": null,
      "diskFileName": "bad3506d-9440-11ea-97d2-4d3296494e7b.xml",
      "anyConnectModuleType": "ANY_CONNECT_CLIENT_PROFILE",
      "id": "bba6cd0e-9440-11ea-97d2-7b74302649a4",
      "type": "anyconnectclientprofile",
      "links": {
        "self": "https://10.89.5.38/api/fdm/v6/object/
anyconnectclientprofiles/bba6cd0e-9440-11ea-97d2-7b74302649a4"
      }
```

d) Recherchez votre objet dans la sortie, sélectionnez le code et utilisez la touche Ctrl + cliquez pour le copier dans le presse-papier.
e) Sélectionnez la méthode PUT /object/anyconnectclientprofiles/{objId}, puis collez le contenu dans le champ **body** (corps).
f) Copiez la valeur **id** et collez-la dans la zone d'édition **objId** au-dessus du body (corps). Vous pouvez également trouver l'ID d'objet à la fin de l'URL « self ».



g) Dans le body (corps) de l'objet, recherchez le champ **anyConnectModuleType**, puis remplacez sa valeur par celle correspondant à votre type de profil. Choisissez parmi DART, FEEDBACK, WEB_SECURITY, ANY_CONNECT_CLIENT_PROFILE, AMP_ENABLER, NETWORK_ACCESS_MANAGER, NETWORK_VISIBILITY, START_BEFORE_LOGIN, ISE_POSTURE, UMBRELLA.
h) Toujours dans le **body** (corps), supprimez l'attribut **links**, y compris la virgule après la valeur **type**.

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

```
{
      "version": "oiwtsaoxbmip7",
      "name": "amp-install-profile",
      "md5Checksum": "12f18388580d3bb2eb0a9dcd8f9a7150",
      "description": null,
      "diskFileName": "bad3506d-9440-11ea-97d2-4d3296494e7b.xml",
      "anyConnectModuleType": "AMP_ENABLER",
      "id": "bba6cd0e-9440-11ea-97d2-7b74302649a4",
      "type": "anyconnectclientprofile"
      }
```

i) Cliquez sur **Try It Out!** (Essayez-le!) Examinez la réponse afin de vérifier que l'objet a été correctement modifié. Vous devriez obtenir un code réponse de 200 et un corps de réponse qui reflète vos modifications. Vous pouvez utiliser la méthode GET pour vérifier davantage les résultats.

Autoriser le trafic par le VPN d'accès à distance

Vous pouvez utiliser l'une des techniques suivantes pour activer la circulation du trafic dans le tunnel VPN d'accès à distance.

- Configurez la commande **sysopt connection permit-vpn**, qui exempte le trafic qui correspond à la connexion VPN de la politique de contrôle d'accès. La valeur par défaut pour cette commande est **no sysopt connection permit-vpn**, ce qui signifie que le trafic VPN doit également être autorisé par la politique de contrôle d'accès.

Il s'agit de la méthode la plus sécurisée pour autoriser le trafic dans le VPN, car les utilisateurs externes ne peuvent pas falsifier des adresses IP dans l'ensemble d'adresses VPN d'accès à distance. L'inconvénient est que le trafic VPN ne sera pas inspecté, ce qui signifie que la protection contre les intrusions et les fichiers, le filtrage des URL ou d'autres fonctions avancées ne seront pas appliqués au trafic. Cela signifie également qu'aucun événement de connexion ne sera généré pour le trafic, et donc les tableaux de bord statistiques ne refléteront pas les connexions VPN.

Pour configurer cette commande, sélectionnez l'option **de politique de contournement du contrôle d'accès pour le trafic déchiffré dans vos profils de connexion VPN d'accès à distance**.

- Créez des règles de contrôle d'accès pour autoriser les connexions à partir de l'ensemble d'adresses VPN d'accès à distance. Cette méthode garantit que le trafic VPN est inspecté et que des services avancés peuvent être appliqués aux connexions. L'inconvénient est que des utilisateurs externes ont alors la possibilité de falsifier les adresses IP et d'accéder ainsi à votre réseau interne.

Vérifier la configuration VPN d'accès à distance

Après avoir configuré le VPN d'accès à distance et déployé la configuration sur le périphérique, vérifiez que vous pouvez établir des connexions à distance.

Si vous rencontrez des problèmes, lisez les rubriques de dépannage pour aider à isoler et à corriger les problèmes. Consultez Dépannage des VPN d'accès à distance, à la page 32.

Procédure

Étape 1 À partir d'un réseau externe, établissez une connexion VPN à l'aide du protocole client AnyConnect.

À l'aide d'un navigateur Web, ouvrez **https://***ravpn-address*, où *ravpn-address* est l'adresse IP ou le nom d'hôte de l'interface externe sur laquelle vous autorisez les connexions VPN. Si nécessaire, installez le logiciel client et terminez la connexion. Consultez Comment les utilisateurs peuvent installer le logiciel client AnyConnect, à la page 3.

Si vous avez modifié le port pour les connexions VPN d'accès à distance, vous devez inclure le port personnalisé dans l'URL. Par exemple, si vous avez changé le port en 4443 : https://ravpn.example.com:4443

Si vous avez configuré des URL de groupe, essayez également ces URL.

Étape 2 Connectez-vous à l'interface de ligne de commande du périphérique comme expliqué dans Connexion avec l'interface de ligne de commande (CLI). Sinon, ouvrez la console CLI.

Étape 3 Utilisez la commande **show vpn-sessiondb** pour afficher les informations récapitulatives sur les sessions VPN actuelles.

Les statistiques doivent afficher votre session client AnyConnect active et des informations sur les sessions cumulatives, le nombre maximal de sessions simultanées et les sessions inactives. Voici un exemple de sortie de la commande :

```
> show vpn-sessiondb
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                           ------------------------------------------------
AnyConnect Client           :      1 :         49 :           3 :        0
```

```
  SSL/TLS/DTLS               :      1 :         49 :           3 :        0
Clientless VPN               :      0 :          1 :           1
  Browser                    :      0 :          1 :           1
-----------------------------------------------------------------------------
Total Active and Inactive    :      1             Total Cumulative :     50
Device Total VPN Capacity    :  10000
Device Load                  :     0%
-----------------------------------------------------------------------------

-----------------------------------------------------------------------------
Tunnels Summary
-----------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ----------------------------------------------
Clientless                   :      0 :          1 :               1
AnyConnect-Parent            :      1 :         49 :               3
SSL-Tunnel                   :      1 :         46 :               3
DTLS-Tunnel                  :      1 :         46 :               3
-----------------------------------------------------------------------------
Totals                       :      3 :        142
-----------------------------------------------------------------------------

-----------------------------------------------------------------------------
IPv6 Usage Summary
-----------------------------------------------------------------------------
                              Active : Cumulative : Peak Concurrent
                             ----------------------------------------------
AnyConnect SSL/TLS/DTLS      :        :           :
  Tunneled IPv6              :      1 :         20 :           2
-----------------------------------------------------------------------------
```

Étape 4 Utilisez la commande **show vpn-sessiondb anyconnect** pour afficher des informations détaillées sur les sessions VPN actuelles.

Les informations détaillées comprennent le chiffrement utilisé, les octets transmis et reçus et d'autres statistiques. Si vous utilisez votre connexion VPN, vous devriez voir les nombres d'octets transmis/reçus changer à mesure que vous réexécutez cette commande.

```
> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : priya                  Index        : 4820
Assigned IP  : 172.18.0.1             Public IP    : 192.168.2.20
Assigned IPv6: 2009::1
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 27731                  Bytes Rx     : 14427
Group Policy : MyRaVpn|Policy         Tunnel Group : MyRaVpn
Login Time   : 21:58:10 UTC Mon Apr 10 2017
Duration     : 0h:51m:13s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a800fd012d400058ebfff2
Security Grp : none                   Tunnel Zone  : 0
```

Gestion de la configuration VPN d'accès à distance

Les profils de connexion VPN d'accès à distance définissent les caractéristiques qui permettent aux utilisateurs externes d'établir une connexion VPN avec le système à l'aide de client AnyConnect. Chaque profil définit les serveurs et les certificats AAA utilisés pour authentifier les utilisateurs, l'ensemble d'adresses pour attribuer des adresses IP aux utilisateurs et les politiques de groupe qui définissent une variété d'attributs axés sur l'utilisateur.

Vous créerez plusieurs profils si vous devez fournir des services variables à différents groupes d'utilisateurs ou si vous avez différentes sources d'authentification. Par exemple, si votre organisation fusionne avec une autre organisation qui utilise des serveurs d'authentification différents, vous pouvez créer un profil pour le nouveau groupe qui utilise ces serveurs d'authentification.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans le groupe **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)**.

Le groupe affiche des informations récapitulatives sur le nombre de profils de connexion et de politiques de groupe actuellement configurés.

Étape 2 Cliquez sur **Connection Profiles** (Profils de connexion) dans la table des matières si ce n'est déjà fait.

Étape 3 Effectuez l'une des actions suivantes :

- Cliquez sur le bouton + pour créer un nouveau profil de connexion. Pour plus de renseignements sur les instructions, consultez Configurer un profil de connexion VPN d'accès à distance, à la page 16.
- Cliquez sur le bouton d'affichage ( ) pour ouvrir un résumé du profil de connexion et des instructions de connexion. Dans le résumé, vous pouvez cliquer sur **Edit** (Modifier) pour apporter des modifications.
- Cliquez sur le bouton de suppression ( ) pour supprimer un profil de connexion dont vous n'avez plus besoin.
- Sélectionnez **Group Policies** (Politiques de groupe) dans la table des matières afin de définir les attributs axés sur l'utilisateur pour les profils de connexion. Consultez Configurer les politiques de groupe pour le VPN d'accès à distance, à la page 25.

Configurer un profil de connexion VPN d'accès à distance

Vous pouvez créer un profil de connexion VPN d'accès à distance pour permettre à vos utilisateurs de se connecter à vos réseaux internes lorsqu'ils se trouvent sur des réseaux externes, comme leur réseau local. Créez des profils distincts pour tenir compte des différentes méthodes d'authentification.

Avant de commencer

Avant de configurer la connexion VPN d'accès à distance (RA)

- Téléchargez les paquets de logiciels client AnyConnect requis à partir de software.cisco.com sur votre ordinateur.
- L'interface externe, celle qui met fin aux connexions VPN d'accès à distance, ne peut pas également avoir une liste d'accès de gestion qui autorise les connexions HTTPS sur le même port. Configurez un port différent pour l'accès de gestion (voir Configuration du port HTTPS pour l'accès de gestion sur les interfaces de données) ou configurez un port différent pour le profil de connexion. Les deux services utilisent le port 443 par défaut, il faut donc le modifier.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans le groupe **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)**.

Le groupe affiche des informations récapitulatives sur le nombre de profils de connexion et de politiques de groupe actuellement configurés.

Étape 2 Cliquez sur **Connection Profiles** (Profils de connexion) dans la table des matières si ce n'est déjà fait.

Étape 3 Effectuez l'une des opérations suivantes :

- Cliquez sur le bouton + pour créer un nouveau profil de connexion.
- Cliquez sur le bouton d'affichage () pour ouvrir un résumé du profil de connexion et des instructions de connexion. Dans le résumé, vous pouvez cliquer sur **Edit** (Modifier) pour apporter des modifications.

Étape 4 Configurez les attributs de connexion de base.

- **Connection Profile Name** (Nom du profil de connexion) : le nom de cette connexion, jusqu'à 50 caractères sans espaces. Par exemple, MainOffice. Vous ne pouvez pas utiliser une adresse IP comme nom.

  Remarque
  Le nom que vous saisissez ici est ce que les utilisateurs verront dans la liste des connexions du client AnyConnect. Choisissez un nom qui aura du sens pour vos utilisateurs.

- **Alias de groupe**, **URL de groupe** : les alias contiennent d'autres noms ou URL pour un profil de connexion spécifique. Les utilisateurs de VPN peuvent choisir un nom d'alias dans le client AnyConnect, dans la liste des connexions, lorsqu'ils se connectent au périphérique Cisco Firepower Threat Defense. Le nom de profil de connexion est automatiquement ajouté en tant qu'alias de groupe. Les alias peuvent comporter jusqu'à 31 caractères.

  Vous pouvez également configurer la liste des URL de groupe, que vos points terminaux peuvent sélectionner lors du lancement de la connexion VPN d'accès à distance. Si les utilisateurs se connectent à l'aide de l'URL de groupe, le système les connecte automatiquement en utilisant le profil de connexion qui correspond à cette dernière. Cette URL serait utilisée par les clients sur lesquels le client AnyConnect n'est pas encore installé.

  Ajoutez autant d'alias de groupe et d'URL que nécessaire. Ces alias et ces URL doivent être uniques pour tous les profils de connexion définis sur le périphérique. Les URL de groupe doivent commencer par **https://**.

  Par exemple, vous pouvez avoir l'alias Sous-traitant et l'URL de groupe https://ravpn.example.com/contractor. Une fois le client AnyConnect installé, l'utilisateur doit simplement sélectionner l'alias de groupe dans la liste déroulante de connexions VPN client AnyConnect.

Étape 5 Configurez les sources d'identité principales et, le cas échéant, secondaires.

Ces options déterminent la façon dont les utilisateurs distants s'authentifient sur le périphérique pour activer la connexion VPN d'accès à distance. L'approche la plus simple consiste à utiliser AAA uniquement, puis à sélectionner un domaine AD ou à utiliser LocalIdentitySource (LocalIdentitySource). Vous pouvez utiliser les approches suivantes pour **Authentication Type** (Type d'authentification) :

- **AAA Only** (AAA uniquement) : authentifie et autorise les utilisateurs en fonction du nom d'utilisateur et du mot de passe. Pour de plus amples renseignements, consultez la section Configurer AAA pour un profil de connexion, à la page 20.
- **Client Certificate Only** (Certificat client uniquement) : authentifie les utilisateurs en fonction du certificat d'identité du périphérique client. Pour de plus amples renseignements, consultez la section Configurer l'authentification par certificat pour un profil de connexion, à la page 24.
- **AAA et ClientCertificate** : utilise à la fois le nom d'utilisateur et le mot de passe ainsi que le certificat d'identité du périphérique client.
- **SAML** : utilise un serveur SAML comme source d'authentification principale. Lorsque vous utilisez SAML, vous ne pouvez pas configurer une source d'authentification de repli ou une source d'authentification secondaire. Pour de plus amples renseignements, consultez la section Configurer AAA pour un profil de connexion, à la page 20.

Étape 6 Configurez l'ensemble d'adresses pour les clients.

L'ensemble d'adresses définit les adresses IP que le système peut attribuer aux clients distants lorsqu'ils établissent une connexion VPN. Pour en savoir plus, consultez Configurer l'adressage client pour le VPN d'accès à distance, à la page 24.

Étape 7 Cliquez sur **Next** (suivant).

Étape 8 Sélectionnez la **Group Policy** (Politique de groupe) à utiliser pour ce profil.

La politique de groupe définit les conditions de connexion des utilisateurs après l'établissement du tunnel. Le système comprend une politique de groupe par défaut nommée « DfltGrpPolicy ». Vous pouvez créer des politiques de groupe supplémentaires pour fournir les services dont vous avez besoin.

Lorsque vous sélectionnez une politique de groupe, un résumé des caractéristiques du groupe s'affiche. Cliquez sur **Edit** (Modifier) dans le résumé pour apporter des modifications.

Si la politique de groupe dont vous avez besoin n'existe pas encore, cliquez sur **Create New Group Policy** (Créer une nouvelle politique de groupe) dans la liste déroulante.

Pour des informations détaillées sur les politiques de groupe, consultez Configurer les politiques de groupe pour le VPN d'accès à distance, à la page 25.

Étape 9 Cliquez sur **Next** (suivant).

Étape 10 Configurez les paramètres globaux.

Ces options s'appliquent à tous les profils de connexion. Après avoir créé le premier profil de connexion, ces options sont préconfigurées pour chaque profil suivant. Si vous apportez des modifications, vous modifiez tous les profils de connexion configurés.

- **Certificate of Device Identity** (Certificat d'identité du périphérique) : sélectionnez le certificat interne utilisé pour établir l'identité du périphérique. Les clients doivent accepter ce certificat pour établir une connexion VPN sécurisée. Si vous n'avez pas encore de certificat, cliquez sur **Create New Internal Certificate** (Créer un nouveau certificat interne) dans la liste déroulante. Vous devez configurer un certificat.

- **Outside Interface** (Interface externe) : l'interface à laquelle les utilisateurs se connectent lors de l'établissement de la connexion VPN d'accès à distance. Bien qu'il s'agisse normalement de l'interface externe (orientée Internet), choisissez l'interface située entre le périphérique et les utilisateurs finaux que vous prenez en charge.
- **Fully-qualified Domain Name for the Outside Interface** (Nom de domaine complet pour l'interface externe) : le nom de l'interface, par exemple, ravpn.exemple.com. Si vous spécifiez un nom, le système peut créer un profil client pour vous.

  Remarque
  Vous êtes responsable de vous assurer que les serveurs DNS utilisés dans le VPN et par les clients peuvent résoudre ce nom en l'adresse IP de l'interface externe. Ajoutez le nom de domaine complet aux serveurs DNS concernés.

- **Port** : le port TCP à utiliser pour les connexions VPN d'accès à distance. La valeur par défaut est 443. Si vous devez vous connecter à FDM sur la même interface utilisée pour le VPN d'accès à distance, vous devez modifier le numéro de port soit pour le profil de connexion, soit pour FDM. Les deux services utilisent le port 443 par défaut. Notez que les utilisateurs devront inclure le numéro de port dans l'URL si vous modifiez le port pour les connexions VPN d'accès à distance.
- **Bypass Access Control policy for decrypted traffic** (Contourner la politique de contrôle d'accès pour le trafic déchiffré) (sysopt permit-vpn) : indique si le trafic VPN est soumis à la politique de contrôle d'accès. Le trafic VPN déchiffré est soumis par défaut à l'inspection de la stratégie de contrôle d'accès. L'activation de l'option **Bypass Access Control policy for decrypted traffic** (Contourner la politique de contrôle d'accès pour le trafic déchiffré) contourne la politique de contrôle d'accès, mais pour le VPN d'accès à distance, le filtre ACL VPN et l'ACL d'autorisation téléchargée à partir du serveur AAA sont toujours appliqués au trafic VPN.

  Notez que si vous sélectionnez cette option, le système configure la commande **sysopt connection permit-vpn**, qui est un paramètre global. Cela aura également une incidence sur le comportement des connexions VPN de site à site. De plus, vous ne pouvez pas effectuer de sélections différentes pour cette option dans vos profils de connexion : la fonctionnalité est activée ou désactivée pour tous les profils.

  Si vous ne sélectionnez pas cette option, il pourrait être possible pour les utilisateurs externes d'usurper les adresses IP dans votre ensemble d'adresses VPN d'accès à distance et ainsi obtenir l'accès à votre réseau. Cela peut se produire parce que vous devrez créer des règles de contrôle d'accès qui permettent à votre ensemble d'adresses d'accéder aux ressources internes. Si vous utilisez des règles de contrôle d'accès, considérez l'utilisation des spécifications de l'utilisateur pour contrôler l'accès, plutôt que l'adresse IP source seule.

  L'inconvénient de sélectionner cette option est que le trafic VPN ne sera pas inspecté, ce qui signifie que la protection contre les intrusions et les fichiers, le filtrage des URL ou d'autres fonctions avancées ne seront pas appliqués au trafic. Cela signifie également qu'aucun événement de connexion ne sera généré pour le trafic, et donc les tableaux de bord statistiques ne refléteront pas les connexions VPN.
- **NAT Exempt** (Exemption NAT) : activez l'exemption NAT pour exempter de la traduction NAT le trafic vers et depuis les terminaux VPN d'accès à distance. Si vous n'exemptez pas le trafic VPN de la NAT, assurez-vous que les règles NAT existantes pour les interfaces externe et interne ne s'appliquent pas au bassin d'adresses du VPN d'accès à distance. Les règles d'exemption de NAT sont des règles NAT d'identité statique manuelle pour une combinaison interface source/destination et réseau donnée, mais elles ne sont pas reflétées dans la politique NAT, elles sont masquées. Si vous activez NAT exempté, vous devez également configurer les éléments suivants.

Notez qu'il s'agit d'une option globale; elle s'applique à tous les profils de connexion. Ainsi, ajoutez simplement des interfaces et des réseaux internes, ne les remplacez pas, sinon vous modifierez les paramètres d'exemption NAT pour tous les autres profils de connexion que vous avez déjà définis.

- **Inside Interfaces** (Interfaces internes) : sélectionnez les interfaces des réseaux internes auxquels les utilisateurs distants accéderont. Les règles NAT sont créées pour ces interfaces.
- **Inside Networks** (Réseaux internes) : sélectionnez les objets réseau qui représentent les réseaux internes auxquels les utilisateurs distants accèdent. La liste des réseaux doit contenir les mêmes types d'adresses IP que les ensembles d'adresses que vous prenez en charge.

- **AnyConnect Packages** (Paquets Secure Client / AnyConnect) : les images logicielles d'installation complète client AnyConnect que vous prendrez en charge sur les connexions VPN d'accès à distance. Pour chaque paquet, le nom de fichier, y compris les extensions, ne peut pas dépasser 60 caractères. Pour chaque paquet, le nom de fichier, y compris les extensions, ne doit pas dépasser 60 caractères. Cependant, vous ne pouvez pas configurer différents paquets pour différents profils de connexion. Si vous avez déjà configuré un paquet pour un autre profil, le paquet est présélectionné. La modification de ce dernier le modifiera pour tous les profils.

  Téléchargez les paquets à partir de software.cisco.com. Si le terminal n'est pas déjà doté du bon paquet, le système invite l'utilisateur à télécharger et à installer le paquet après l'authentification de l'utilisateur.

Étape 11 Cliquez sur **Next** (suivant).

Étape 12 Examinez le résumé.

Tout d'abord, vérifiez que le résumé est correct.

Ensuite, cliquez sur **Instructions** pour voir ce que doivent faire les utilisateurs finaux pour installer initialement le logiciel client AnyConnect et vérifier qu'ils peuvent établir une connexion VPN. Cliquez sur **Copy** (Copier) pour copier ces instructions dans le presse-papiers, puis les distribuer à vos utilisateurs.

Étape 13 Cliquez sur **Terminer**.

Prochaine étape

Assurez-vous que le trafic est autorisé dans le tunnel VPN, comme expliqué dans la section Autoriser le trafic par le VPN d'accès à distance, à la page 13.

Configurer AAA pour un profil de connexion

Les serveurs d'authentification, d'autorisation et de comptabilité (AAA) utilisent un nom d'utilisateur et un mot de passe pour déterminer si un utilisateur est autorisé à accéder au VPN d'accès à distance. Si vous utilisez des serveurs RADIUS, vous pouvez différencier les niveaux d'autorisation des utilisateurs authentifiés afin de fournir un accès différentiel aux ressources protégées. Vous pouvez également utiliser les services de comptabilité RADIUS pour suivre l'utilisation.

Lors de la configuration de AAA, vous devez configurer une source d'identité principale. Les sources secondaires et de repli sont facultatives. Utilisez une source secondaire si vous souhaitez mettre en œuvre la double authentification, par exemple, à l'aide de jetons RSA ou de DUO.

Options de source d'identité principale

- **Primary Identity Source for User Authentication** (Source d'identité principale pour l'authentification de l'utilisateur) : la source d'identité principale utilisée pour authentifier les utilisateurs distants. Les utilisateurs finaux doivent être définis dans cette source ou la source de repli facultative pour terminer une connexion VPN. Sélectionnez l'une des options suivantes :
  - Un domaine d'identité Active Directory (AD) Si le domaine dont vous avez besoin n'existe pas encore, cliquez sur **Create New Identity Realm** (créer un nouveau domaine d'identité).
  - Un groupe de serveurs RADIUS.
  - LocalIdentitySource (la base de données des utilisateurs locaux) : vous pouvez définir des utilisateurs directement sur le périphérique et ne pas utiliser de serveur externe.
  - Un serveur LDAP Duo. Cependant, il est préférable de l'utiliser comme source d'authentification secondaire pour fournir une authentification à deux facteurs, comme décrit dans Comment configurer l'authentification à deux facteurs à l'aide de Duo LDAP, à la page 43. Si vous l'utilisez comme source principale, vous n'obtiendrez pas d'informations sur l'identité de l'utilisateur, et vous ne verrez pas les informations sur les utilisateurs dans les tableaux de bord, et vous ne pourrez pas non plus écrire de règles de contrôle d'accès basées sur l'utilisateur.
  - Un serveur SAML. Si vous utilisez un serveur SAML, vous ne pouvez pas configurer une source d'authentification de repli ou secondaire. Vous pouvez utiliser RADIUS comme serveur d'autorisation, mais vous devez configurer le serveur RADIUS pour que l'authentification ne soit pas requise. Autrement dit, le serveur RADIUS fournira les informations d'autorisation après l'authentification de la connexion par SAML.
- **SAML Login Experience** (Expérience de connexion SAML) : si vous sélectionnez SAML comme source d'authentification principale, vous devez sélectionner le navigateur client à utiliser pour terminer l'authentification Web :
  - **VPN Client embedded browser** (navigateur intégré du client VPN) : le client VPN utilise son navigateur intégré pour l'authentification Web, donc l'authentification s'applique uniquement à la connexion VPN. Il s'agit de la configuration par défaut et ne nécessite aucune configuration supplémentaire.
  - **Default OS Browser** (navigateur du système d'exploitation par défaut) : le client VPN utilise le navigateur par défaut du système pour l'authentification Web. Cette option active la connexion unique (SSO) entre votre authentification VPN et d'autres connexions d'entreprise. Choisissez également cette option si vous souhaitez prendre en charge des méthodes d'authentification web, telles que l'authentification biométrique, qui ne peuvent pas être exécutées dans le navigateur intégré.

    Vous devez charger un progiciel qui active l'authentification Web dans le navigateur. Obtenez les paquets sur le site de software.cisco.com. Notez que le paquet que vous chargez est utilisé par tous les profils de connexion qui utilisent SAML avec le navigateur du système d'exploitation par défaut; les paquets sont globaux et non spécifiques à un profil de connexion.
- **Fallback Local Identity Source** (Source d'identité locale de secours) : si la source principale est un serveur externe, vous pouvez sélectionner LocalIdentitySource comme solution de secours au cas où le serveur principal ne serait pas disponible. Si vous utilisez la base de données locale comme source de secours, veillez à définir les mêmes noms d'utilisateur/mots de passe locaux que ceux définis dans le serveur externe.

Advanced Options (Options avancées) : cliquez sur le lien **Advanced** (Avancé) et configurez les options suivantes :

- **Strip options** (Options de suppression) : un domaine est un domaine administratif. L'activation des options suivantes permet à l'authentification d'être basée sur le nom d'utilisateur uniquement. Vous pouvez activer n'importe quelle combinaison de ces options. Cependant, vous devez cocher les deux cases si votre serveur ne peut pas analyser les délimiteurs.
  - **Strip Identity Source Server from Username (Supprimer le serveur de source d'identité du nom d'utilisateur)** : que ce soit pour supprimer le nom de la source d'identité du nom d'utilisateur avant de transmettre ce nom au serveur AAA. Par exemple, si vous sélectionnez cette option et que l'utilisateur entre domaine\nom d'utilisateur comme nom d'utilisateur, le domaine est supprimé du nom d'utilisateur et envoyé au serveur AAA pour authentification. Par défaut, cette fonction est désactivée.
  - **Strip Group from Username** (Supprimer le groupe du nom d'utilisateur) : permet de supprimer le nom du groupe du nom d'utilisateur avant de transmettre ce nom au serveur AAA. Cette option s'applique aux noms donnés au format nomdutilisateur@domaine ; l'option supprime le domaine et le signe @. Par défaut, cette fonction est désactivée.
- **Enable Password Management** (Activer la gestion des mots de passe) : permet à l'utilisateur de modifier le mot de passe à son expiration. Si vous ne sélectionnez pas cette option, à l'expiration du mot de passe de l'utilisateur, le client AnyConnect refusera la connexion et l'utilisateur devra modifier le mot de passe sur le serveur AAA. Si vous sélectionnez cette option, client AnyConnect invite l'utilisateur à modifier le mot de passe à son expiration, ce qui est beaucoup plus pratique pour l'utilisateur. Sélectionnez l'une des options suivantes : Assurez-vous également d'activer MSCHAPv2 sur le serveur AAA.
  - **Notify user x days prior to password expiration (LDAP only)** (Avertir l'utilisateur x jours avant l'expiration du mot de passe [LDAP uniquement]) : à partir du nombre de jours que vous spécifiez, avertissez l'utilisateur de l'expiration prochaine du mot de passe. Vous pouvez définir l'avertissement de 1 à 180 jours, 14 étant la valeur par défaut.
  - **Notify user on the day of password expiration** (Avertir l'utilisateur le jour de l'expiration du mot de passe) : l'utilisateur ne reçoit pas d'avertissement, mais il est toujours invité à modifier le mot de passe à l'expiration de ce dernier. Même si vous définissez une période d'avertissement, les utilisateurs RADIUS obtiennent toujours ce comportement.

Source d'identité secondaire

- **Secondary Identity Source for User Authorization** (Source d'identité secondaire pour l'autorisation de l'utilisateur) : la deuxième source d'identité facultative. Si l'utilisateur s'authentifie avec succès auprès de la source principale, il est invité à s'authentifier auprès de la source secondaire. Vous pouvez sélectionner un domaine AD, un groupe de serveurs RADIUS, un serveur LDAP Duo, ou la source d'identité locale.
- **Advanced options** (Options avancées) : cliquez sur le lien **Advanced** (Avancé) et configurez les options suivantes
  - **Fallback Local Identity Source for Secondary** (Source d'identité locale de secours pour la source secondaire) : si la source secondaire est un serveur externe, vous pouvez sélectionner LocalIdentitySource comme solution de secours au cas où le serveur secondaire ne serait pas disponible. Si vous utilisez la base de données locale comme source de secours, veillez à définir les mêmes noms d'utilisateur/mots de passe locaux que ceux définis dans le serveur externe secondaire.

- **Use Primary Username for Secondary Login** (Utiliser le nom d'utilisateur principal pour la connexion secondaire) : par défaut, lors de l'utilisation d'une source d'identité secondaire, le système vous demande de saisir le nom d'utilisateur et le mot de passe pour la source secondaire. Si vous sélectionnez cette option, le système invite uniquement à saisir le mot de passe secondaire et utilise pour la source secondaire le même nom d'utilisateur que celui authentifié auprès de la source d'identité principale. Sélectionnez cette option si vous configurez les mêmes noms d'utilisateur dans les sources d'identité principale et secondaire.
- **Username for Session Server** (Nom d'utilisateur pour le serveur de session) : une fois l'authentification réussie, le nom d'utilisateur s'affiche dans les événements et les tableaux de bord statistiques, est utilisé pour déterminer les correspondances pour les règles de déchiffrement SSL et de contrôle d'accès basées sur l'utilisateur ou le groupe, et sert à la comptabilité. Comme vous utilisez deux sources d'authentification, vous devez indiquer au système s'il doit utiliser le nom d'utilisateur principal ou secondaire comme identité de l'utilisateur. Par défaut, le nom principal est utilisé.
- **Password Type** (Type de mot de passe) : indique comment obtenir le mot de passe pour le serveur secondaire. Ce champ s'applique uniquement si vous sélectionnez **AAA et Client Certificate (certificat client)** pour le type d'authentification et pour les options de certificat, vous sélectionnez à la fois **Prefill username from certificate on user login window** (Préremplir le nom d'utilisateur à partir du certificat dans la fenêtre de connexion) et **Hide username in login window** (Masquer le nom d'utilisateur dans la fenêtre de connexion). La valeur par défaut est **Prompt** (Invite), ce qui signifie que l'utilisateur est invité à saisir le mot de passe.

  Sélectionnez **Primary Identity Source Password** (Mot de passe de la source d'identité principale) pour utiliser automatiquement le mot de passe saisi lors de l'authentification de l'utilisateur sur le serveur principal.

  Sélectionnez **Common Password** (Mot de passe commun) pour utiliser le même mot de passe pour chaque utilisateur, puis saisissez ce mot de passe dans le champ **Common Password** (Mot de passe commun).

Options supplémentaires

- **Authorization Server** (Serveur d'autorisation) : le groupe de serveurs RADIUS qui a été configuré pour autoriser les utilisateurs du VPN d'accès à distance.

  Une fois l'authentification terminée, l'autorisation contrôle les services et les commandes disponibles pour chaque utilisateur authentifié. L'autorisation consiste à rassembler un ensemble d'attributs qui décrivent ce que l'utilisateur est autorisé à faire, ses capacités réelles et ses restrictions. Si vous n'utilisez pas l'autorisation, l'authentification à elle seule fournit le même accès à tous les utilisateurs authentifiés. Pour en savoir plus sur la configuration de RADIUS pour l'autorisation, consultez Contrôle des autorisations et des attributs des utilisateurs à l'aide de RADIUS et des stratégies de groupe, à la page 3.

  Notez que si le système obtient des attributs d'autorisation du serveur RADIUS qui chevauchent ceux définis dans la group policy (stratégie de groupe), les attributs RADIUS remplacent les attributs de la stratégie de groupe.

- **Accounting Server** (Serveur de comptabilité) : (facultatif). Le groupe de serveurs RADIUS à utiliser pour prendre en compte la session VPN d'accès à distance.

  La fonction de traçabilité est utilisée pour suivre les services auxquels les utilisateurs accèdent et la quantité de ressources réseau qu'ils consomment. Le périphérique Cisco Firepower Threat Defense signale l'activité de l'utilisateur au serveur RADIUS. Les renseignements de comptabilité comprennent

les heures de début et de fin des sessions, les noms d'utilisateur, le nombre d'octets transitant par le périphérique pour chaque session, le service utilisé et la durée de chaque session. Ces données peuvent ensuite être analysées pour la gestion du réseau, la facturation client ou l'audit. Vous pouvez utiliser la comptabilité seule ou conjointement avec l'authentification et l'autorisation.

Configurer l'authentification par certificat pour un profil de connexion

Vous pouvez utiliser les certificats installés sur le périphérique client pour authentifier les connexions VPN d'accès à distance. Lors de l'authentification par certificat, assurez-vous que le certificat d'autorité de certification de confiance utilisé pour valider les connexions utilisateur d'accès à distance comprend l'option **SSL Client** (client SSL) pour **Validation Usage** (utilisation de validation).

Lorsque vous utilisez des certificats clients, vous pouvez toujours configurer une source d'identité secondaire, une source de repli et des serveurs d'autorisation et de comptabilité. Il s'agit d'options AAA ; pour en savoir plus, consultez Configurer AAA pour un profil de connexion, à la page 20.

Voici les attributs spécifiques au certificat. Vous pouvez configurer ces attributs séparément pour les sources d'identité principale et secondaire. La configuration d'une source secondaire est facultative.

- **Username from Certificate** (Nom d'utilisateur à partir du certificat) : sélectionnez l'une des options suivantes :
  - **Map Specific Field** (Mapper un champ spécifique) : utilisez les éléments de certificat dans l'ordre du **Primary Field** (Champ principal) et **Secondary Field** (Champ secondaire). Les valeurs par défaut sont CN (Common Name) et OU (Organizational Unit). Sélectionnez les options qui fonctionnent pour votre organisation. Les champs sont combinés pour fournir le nom d'utilisateur, et il s'agit du nom utilisé dans les événements, les tableaux de bord et, à des fins de correspondance, dans les règles de déchiffrement SSL et de contrôle d'accès.
  - **Utiliser le DN entier (nom distinctif) comme nom d'utilisateur** : le système dérive automatiquement le nom d'utilisateur des champs DN.
- **Options avancées** : cliquez sur le lien **Advanced** (Avancé) et configurez les options suivantes
  - **Préremplir le nom d'utilisateur à partir du certificat lors de la connexion de l'utilisateur** : indique s'il faut remplir le champ du nom d'utilisateur avec le nom récupéré lorsque l'utilisateur est invité à s'authentifier.
  - **Masquer le nom d'utilisateur dans la fenêtre de connexion** : si vous sélectionnez l'option **Prefill** (Préremplirt), vous pouvez masquer le nom d'utilisateur, ce qui signifie que l'utilisateur ne peut pas le modifier dans l'invite de mot de passe.

Configurer l'adressage client pour le VPN d'accès à distance

Le système doit pouvoir fournir une adresse IP aux points terminaux qui se connectent au VPN d'accès à distance. Ces adresses peuvent être fournies par le serveur AAA, un serveur DHCP, un ensemble d'adresses IP configuré dans la politique de groupe ou un ensemble d'adresses IP configuré dans le profil de connexion. Le système teste ces ressources dans cet ordre et s'arrête lorsqu'il obtient une adresse disponible, qu'il attribue ensuite au client. Ainsi, vous pouvez configurer plusieurs options pour créer un mode à sécurité intégrée en cas d'un nombre peu commun de connexions simultanées.

Utilisez une ou plusieurs des méthodes suivantes pour configurer l'ensemble d'adresses d'un profil de connexion.

- **Serveur AAA** : d'abord, configurez un objet réseau sur le périphérique FTD qui spécifie un sous-réseau pour l'ensemble d'adresses. Ensuite, dans le serveur RADIUS, configurez l'attribut Address-Pools (217) pour l'utilisateur portant le nom de l'objet. Précisez également le serveur RADIUS pour l'authentification dans le profil de connexion.
- **DHCP** : d'abord, configurez un serveur DHCP avec une ou plusieurs plages d'adresses IPv4 pour le VPN d'accès à distance (vous ne pouvez pas configurer les regroupements IPv6 à l'aide de DHCP). Créez ensuite un objet réseau d'hôte avec l'adresse IP du serveur DHCP. Vous pouvez ensuite sélectionner cet objet dans l'attribut **Serveurs DHCP** du profil de connexion. Vous pouvez configurer jusqu'à 10 serveurs DHCP.

  Si le serveur DHCP dispose de plusieurs ensembles d'adresses, vous pouvez utiliser l'attribut **de portée DHCP** dans la politique de groupe que vous ajoutez au profil de connexion pour sélectionner l'ensemble à utiliser. Créez un objet réseau hôte avec l'adresse réseau de l'ensemble. Par exemple, si l'ensemble DHCP contient 192.168.15.0/24 et 192.168.16.0/24, la définition de la portée de DHCP à 192.168.16.0 garantira qu'une adresse du sous-réseau 192.168.16.0/24 sera sélectionnée.
- **Ensembles d'adresses IP locales** : d'abord, créez jusqu'à six objets réseau qui précisent les sous-réseaux. Vous pouvez configurer des ensembles distincts pour IPv4 et IPv6. Ensuite, sélectionnez ces objets dans les options **IPv4 Address Pool** et **IPv6 Address Pool**, soit dans la politique de groupe, soit dans le profil de connexion. Vous n'avez pas besoin de configurer IPv4 et IPv6, configurez simplement le schéma d'adresse que vous souhaitez prendre en charge.

  Vous n'avez pas non plus besoin de configurer l'ensemble dans la politique de groupe et le profil de connexion. La politique de groupe remplace les paramètres de profil de connexion. Par conséquent, si vous configurez les ensembles dans la politique de groupe, laissez les options vides dans le profil de connexion.

  Notez que les ensembles sont utilisés dans l'ordre dans lequel vous les listez.

Configurer les politiques de groupe pour le VPN d'accès à distance

Une politique de groupe est un ensemble de paires d'attributs/valeurs axées sur l'utilisateur pour les connexions VPN d'accès à distance. Le profil de connexion utilise une politique de groupe qui définit les conditions des connexions d'utilisateur après l'établissement du tunnel. Les politiques de groupe vous permettent d'appliquer des ensembles complets d'attributs à un utilisateur ou à un groupe d'utilisateurs, plutôt que d'avoir à spécifier chaque attribut individuellement pour chaque utilisateur.

Le système comprend une politique de groupe par défaut nommée « DfltGrpPolicy ». Vous pouvez créer des politiques de groupe supplémentaires pour fournir les services dont vous avez besoin.

Procédure

Étape 1 Cliquez sur **View Configuration** (Afficher la configuration) dans le groupe **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)**.

Le groupe affiche des informations récapitulatives sur le nombre de profils de connexion et de politiques de groupe actuellement configurés.

Étape 2 Cliquez sur **Group Policies** (Politiques de groupe) dans la table des matières.

Étape 3 Effectuez l'une des actions suivantes :

- Cliquez sur le bouton + pour créer un nouveau groupe. Consultez les rubriques suivantes pour obtenir des explications sur les attributs des pages de la politique de groupe :
  - Attributs généraux, à la page 26
  - Attributs des paramètres de session, à la page 27
  - Attributs d'attribution d'adresse, à la page 27
  - Attributs de tunnellisation fractionnée, à la page 28
  - Attributs client AnyConnect , à la page 29
  - Attributs des filtres de trafic, à la page 30
  - Attributs de mandataire de navigateur Windows, à la page 31
- Cliquez sur le bouton de modification ( ) pour modifier une politique existante.
- Cliquez sur le bouton de suppression ( ) pour supprimer un groupe dont vous n'avez plus besoin. Le groupe ne peut pas être actuellement utilisé dans un profil de connexion.

Attributs généraux

Les attributs généraux d'une politique de groupe définissent le nom du groupe et certains autres paramètres de base. L'attribut Name (Nom) est le seul attribut obligatoire.

- **Name** (Nom) : le nom de la politique de groupe. Le nom peut comporter jusqu'à 64 caractères. Les espaces sont autorisés.
- **Description** : une description de la politique de groupe. La description peut comporter jusqu'à 1 024 caractères.
- **Serveur DNS** : sélectionnez le groupe de serveurs DNS qui définit les serveurs DNS que les clients doivent utiliser pour la résolution de noms de domaine lorsqu'ils sont connectés au VPN. Si le groupe dont vous avez besoin n'est pas encore défini, cliquez sur **Create DNS Group** (créer un groupe DNS) et créez-le maintenant.
- **Bannière** : texte de la bannière, ou message de bienvenue, à présenter aux utilisateurs lors de la connexion. La valeur par défaut est Sans bannière. La longueur peut aller jusqu'à 496 caractères. La client AnyConnect ne prend en charge que le HTML partiel. Pour vous assurer que la bannière s'affiche correctement pour les utilisateurs distants, utilisez la balise
 pour indiquer les sauts de ligne.
- **Default Domain** (domaine par défaut) : le nom de domaine par défaut pour les utilisateurs de de VPN d'accès à distance. Par exemple, exemple.com. Ce domaine est ajouté aux noms d'hôte qui ne sont pas complets, par exemple, serverA au lieu de serverA.example.com.
- **AnyConnect Client Profiles (Profils de client AnyConnect)** : cliquez sur + et sélectionnez les client AnyConnect profils à utiliser pour ce groupe. Si vous configurez un nom de domaine complet pour l'interface extérieure (dans le profil de connexion), un profil par défaut sera créé pour vous. Sinon, vous pouvez charger votre propre profil client. Créez ces profils à l'aide de l'éditeur de profils client AnyConnect autonome, que vous pouvez télécharger et installer à partir de software.cisco.com. Si vous ne sélectionnez pas de profil client, le client AnyConnect utilise les valeurs par défaut pour toutes les options. Les éléments de cette liste sont des objets Profil client AnyConnect plutôt que les profils

eux-mêmes. Vous pouvez créer (et charger) de nouveaux profils en cliquant sur **Create New AnyConnect Client Profile (Créer un nouveau profil client AnyConnect)** dans la liste déroulante.

Vous pouvez sélectionner des client AnyConnect profils de module, tels que AMP Enabler, en plus du profil client AnyConnect. Vous pouvez sélectionner un profil par type de module.

Attributs des paramètres de session

Les paramètres de session d'une politique de groupe contrôlent la durée de connexion des utilisateurs au VPN et le nombre de connexions distinctes qu'ils peuvent établir.

- **Maximum Connection Time** (Durée maximale de connexion) : la durée maximale, en minutes, pendant laquelle les utilisateurs peuvent rester connectés au VPN sans se déconnecter et se reconnecter, de 1 à 4 473 924, ou laissez le champ vide. La valeur par défaut est illimitée (vide), mais le délai d'inactivité s'applique toujours.
- **Connection Time Alert Interval** (Intervalle d'alerte de connexion) : si vous spécifiez une durée de connexion maximale, l'intervalle d'alerte définit le temps avant que la durée maximale ne soit atteinte pour afficher un avertissement à l'utilisateur concernant la déconnexion automatique à venir. L'utilisateur peut choisir de mettre fin à la connexion et de se reconnecter pour redémarrer le minuteur. La valeur par défaut est de 1 minute . Vous pouvez spécifier une valeur comprise entre 1 et 30 minutes.
- **Idle Time** (Durée d'inactivité) : la durée, en minutes, pendant laquelle la connexion VPN peut être inactive avant d'être close automatiquement, de 1 à 35 791 394. S'il n'y a aucune activité de communication sur la connexion pendant ce nombre consécutif de minutes, le système arrête la connexion. La valeur par défaut est de 30 minutes.
- **Idle Time Alert Interval** (Intervalle d'alerte de temps d'inactivité) : la durée avant que le temps d'inactivité ne soit atteint pour afficher un avertissement à l'utilisateur concernant la déconnexion automatique à venir en raison d'une session inactive. Toute activité réinitialise la minuterie. La valeur par défaut est de 1 minute . Vous pouvez spécifier une valeur comprise entre 1 et 30 minutes.
- **Simultaneous Login Per User** (Connexions simultanées par utilisateur) : nombre maximal de connexions simultanées autorisées pour un utilisateur. La valeur par défaut est de 3. Vous pouvez spécifier de 1 à 2147483647 connexions. Autoriser de nombreuses connexions simultanées peut compromettre la sécurité et affecter les performances.

Attributs d'attribution d'adresse

Les attributs d'attribution d'adresse d'une politique de groupe définissent l'ensemble des adresses IP pour le groupe. L'ensemble défini ici remplace l'ensemble défini dans tout profil de connexion qui utilise ce groupe. Laissez ce paramètre vide si vous souhaitez utiliser l'ensemble défini dans le profil de connexion.

- **IPv4 Address Pool** (Ensemble d'adresses IPv4), **IPv6 Address Pool** (Ensemble d'adresses IPv6) : ces options définissent les ensembles d'adresses pour les points terminaux distants. Les clients reçoivent une adresse de ces ensembles en fonction de la version IP qu'ils utilisent pour établir la connexion VPN. Sélectionnez un objet réseau qui définit un sous-réseau pour chaque type d'adresse IP que vous souhaitez prendre en charge. Laissez la liste vide si vous ne souhaitez pas prendre en charge cette version IP. Par exemple, vous pouvez définir un ensemble d'adresses IPv4 comme 10.100.10.0/24. L'ensemble d'adresses ne peut pas se trouver sur le même sous-réseau que l'adresse IP pour l'interface externe.

  Vous pouvez spécifier une liste de six ensembles d'adresses maximum à utiliser pour l'attribution d'adresses locale. L'ordre dans lequel vous spécifiez les ensembles est important. Le système attribue les adresses de ces ensembles dans l'ordre dans lequel les ensembles apparaissent.

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

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

  Pour spécifier une portée, sélectionnez un objet réseau contenant 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. Cliquez sur **Create New Network** (créer un nouveau réseau) si l'objet n'existe pas. 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.

Attributs de tunnellisation fractionnée

Les attributs de tunnellisation fractionnée d'une politique de groupe définissent la façon dont le système doit gérer le trafic destiné au réseau interne par rapport au trafic acheminé de l'extérieur. La tunnellisation fractionnée dirige une partie du trafic réseau dans le tunnel VPN (chiffré) et le trafic réseau restant à l'extérieur du tunnel VPN (non chiffré ou en texte clair).

- **IPv4 Split Tunneling** (Tunnelisation fractionnée IPv4), **IPv6 Split Tunneling** (Tunnelisation fractionnée IPv6) : vous pouvez spécifier différentes options selon que le trafic utilise des adresses IPv4 ou IPv6, mais les options pour les deux sont identiques. Si vous souhaitez activer la tunnellisation fractionnée, spécifiez l'une des options qui vous obligent à sélectionner des objets réseau.
  - **Allow all traffic over tunnel** (autoriser tout le trafic via le tunnel) : ne pas diviser la tunnellisation. Une fois que l'utilisateur établit une connexion VPN d'accès à distance, tout le trafic de l'utilisateur passe par le tunnel protégé. Il s'agit du paramètre par défaut. Elle est également considérée comme l'option la plus sécurisée.
  - **Allow specified traffic over the tunnel** (Autoriser le trafic spécifié sur le tunnel) : sélectionnez les objets réseau qui définissent le réseau de destination et les adresses d'hôte. Tout trafic vers ces destinations passe par le tunnel protégé. Le client achemine le trafic vers toute autre destination vers les connexions à l'extérieur du tunnel (comme une connexion Wi-Fi locale ou un réseau).
  - **Exclude networks specified below** (Exclure les réseaux spécifiés ci-dessous) : sélectionnez les objets réseau qui définissent le réseau de destination ou les adresses d'hôte. Le client achemine tout trafic vers ces destinations vers des connexions à l'extérieur du tunnel. Le trafic vers toute autre destination passe par le tunnel.
- **Split DNS** (DNS fractionné) : vous pouvez configurer le système pour envoyer certaines requêtes DNS par l'intermédiaire de la connexion sécurisée tout en permettant au client d'envoyer d'autres requêtes DNS aux serveurs DNS configurés sur le client. Vous pouvez configurer les comportements DNS suivants :

- **Send DNS Request as per split tunnel policy** (envoi d'une requête DNS conformément à la politique du tunnel fractionné) : avec cette option, les demandes DNS sont traitées de la même manière que les options de séparation du tunnel sont définies. Si vous activez la tunnellisation fractionnée, les requêtes DNS sont envoyées en fonction des adresses de destination. Si vous n'activez pas la tunnellisation fractionnée, toutes les requêtes DNS passent par la connexion protégée.
- **Always send DNS requests over tunnel** (toujours envoyer les requêtes DNS via le tunnel) : sélectionnez cette option si vous activez la tunnellisation fractionnée, mais que vous souhaitez que toutes les requêtes DNS soient envoyées par la connexion protégée aux serveurs DNS définis pour le groupe.
- **Send only specified domains over tunnel** (envoyer uniquement les domaines spécifiés via le tunnel) : sélectionnez cette option si vous souhaitez que vos serveurs DNS protégés résolvent les adresses de certains domaines uniquement. Ensuite, spécifiez ces domaines en séparant les noms de domaines par des virgules. Par exemple, exemple.com, exemple1.com. Utilisez cette option si vous souhaitez que vos serveurs DNS internes résolvent les noms des domaines internes, tandis que les serveurs DNS externes gèrent tout le reste du trafic Internet.

Attributs client AnyConnect

Les attributs client AnyConnect d'une politique de groupe définissent certains paramètres SSL et de connexion utilisés par le client AnyConnect pour une connexion VPN d'accès à distance.

Paramètres SSL

- **Enable Datagram Transport Layer Security (DTLS)** (activer la sécurité de la couche de transport des datagrammes, ou DTLS) : s'il faut autoriser le client AnyConnect à utiliser deux tunnels simultanément, un tunnel SSL et un tunnel DTLS. L'utilisation de DTLS évite les problèmes de latence et de bande passante associés à certaines connexions SSL et améliore la performance des applications en temps réel sensibles aux retards de paquets. Si vous n'activez pas DTLS, les utilisateurs du client AnyConnect qui établissent des connexions SSL VPN se connectent uniquement à l'aide d'un tunnel SSL.
- **DTLS Compression** (compression DTLS) : s'il faut compresser les connexions DTLS (Datagram Transport Layer Security) pour ce groupe à l'aide de LZS. La compression DTLS est désactivée par défaut.
- **SSL Compression (Compression SSL)**: indique s'il faut activer la compression des données et, si oui, la méthode de compression de données à utiliser, **Deflate** ou **LZS**. La compression SSL est **désactivée** par défaut. La compression des données accélère les débits de transmission, mais augmente également les besoins en mémoire et l'utilisation du processeur pour chaque session utilisateur. Par conséquent, la compression SSL diminue le débit global du périphérique.
- **SSL Rekey Method (Méthode de renouvellement de clé SSL)**, **SSL Rekey Interval (Intervalle de renouvellement de clé SSL)** : permet au client de renouveler la clé de la connexion VPN en renégociant les clés de chiffrement et les vecteurs d'initialisation afin d'augmenter la sécurité de la connexion. Désactivez le renouvellement de clé en sélectionnant **Aucun**. Pour activer rekey, sélectionnez **New Tunnel** pour créer un nouveau tunnel à chaque fois. (L'option **Existing Tunnel** (Tunnel existant) entraîne la même action que **New Tunnel** (Nouveau tunnel).) Si vous activez le renouvellement de clé, définissez également l'intervalle de renouvellement, qui est de 4 minutes par défaut. Vous pouvez définir l'intervalle entre 4 et 10 080 minutes (1 semaine).

Paramètres de connexion

- **Ignore DF (Don't Fragment) Bit** (ignorer le bit Ne pas fragmenter DF : s'il faut ignorer le bit Ne pas fragmenter (DF) dans les paquets qui ont besoin de fragmentation. Sélectionnez cette option pour autoriser la fragmentation forcée des paquets dont le bit DF est activé, afin que ces paquets puissent passer par le tunnel.
- **Client Bypass Protocol** (protocole de contournement client) : vous permet de configurer la façon dont la passerelle sécurisée gère le trafic IPv4 (lorsqu'elle s'attend uniquement au trafic IPv6) ou la façon dont elle gère le trafic IPv6 (lorsqu'elle s'attend uniquement au trafic IPv4).

  Lorsque client AnyConnect établit une connexion VPN avec la tête de réseau, celle-ci lui attribue une adresse IPv4, IPv6 ou aux deux une adresse IPv4 et IPv6. Si la tête de réseau affecte uniquement une adresse IPv4 ou IPv6 à la connexion client AnyConnect, vous pouvez configurer le protocole de contournement du client pour abandonner le trafic réseau pour lequel la tête de réseau n'a pas attribué d'adresse IP (par défaut, désactivé, non coché), ou autoriser que ce trafic contourne la tête de réseau et soit envoyé par le client non chiffré ou « en clair » (activé, coché).

  Par exemple, supposons que la passerelle sécurisée attribue uniquement une adresse IPv4 à la connexion client AnyConnect et que le point terminal fonctionne à deux niveaux. Lorsque le point terminal tente d'atteindre une adresse IPv6, si le protocole de contournement des clients est désactivé, le trafic IPv6 est abandonné; cependant, si le protocole de contournement client est activé, le trafic IPv6 est envoyé par le client en clair.
- **MTU** : taille maximale d'unité de transmission (MTU) pour les connexions de VPN SSL établies par client AnyConnect. Par défaut, c'est de 1406 octets. La plage se situe entre 576 et 1 462 octets.
- **Messages Keepalive entre AnyConnect et la passerelle VPN** : s'il faut échanger des messages Keepalive entre les homologues pour démontrer qu'ils sont disponibles pour envoyer et recevoir des données dans le tunnel. Les messages Keepalive sont transmis à des intervalles définis. L'intervalle par défaut est de 20 secondes, et la plage valide est de 15 à 600 secondes.
- **Intervalle DPD côté passerelle**, **Intervalle DPD côté client** : activez la fonction DPD (Dead peer detection) pour vous assurer que la passerelle VPN ou le client VPN détecte rapidement lorsque l'homologue ne répond plus. Vous pouvez activer séparément la passerelle ou le client DPD. L'intervalle par défaut est de 30 secondes pour l'envoi de messages DPD. L'intervalle peut aller de 5 à 3 600 secondes.

Attributs des filtres de trafic

Les attributs de filtre de trafic d'une politique de groupe définissent les restrictions que vous souhaitez imposer aux utilisateurs affectés au groupe. Vous pouvez utiliser ces attributs au lieu de créer des règles de politique de contrôle d'accès pour restreindre les utilisateurs de VPN d'accès à distance à des ressources spécifiques, en fonction de l'adresse et du protocole d'hôte ou de sous-réseau, ou du VLAN.

Par défaut, les utilisateurs de VPN d'accès à distance ne sont pas empêchés par la politique de groupe d'accéder à toute destination sur votre réseau protégé.

- **Access List Filter** (Filtre de liste d'accès) : limitez l'accès à l'aide d'une liste de contrôle d'accès étendue (ACL). Sélectionnez l'objet Smart CLI Extended ACL (ACL étendue Smart CLI), ou cliquez sur **Create Extended Access List** (Créer une liste d'accès étendue) et créez-la maintenant.

  La liste de contrôle d'accès étendue vous permet de filtrer par adresse source, adresse de destination et protocole (comme IP ou TCP). Les ACL sont évaluées sur une base descendante, à la première correspondance, alors faites en sorte de placer les règles spécifiques avant les règles plus générales. Il y a une règle implicite « refuser tout » à la fin de la liste de contrôle d'accès. Par conséquent, si vous avez

l'intention de refuser l'accès à quelques sous-réseaux tout en autorisant tous les autres accès, assurez-vous d'inclure une règle « autoriser tout » à la fin de la liste de contrôle d'accès. Le filtre VPN s'applique aux connexions initiales uniquement. Il ne s'applique pas aux connexions secondaires, comme une connexion de support SIP, qui sont ouvertes en raison de l'action de l'inspection d'application.

Comme vous ne pouvez pas créer d'objets réseau lors de la modification d'un objet d'interface de ligne de commande intelligente d'ACL étendue, vous devez créer la liste de contrôle d'accès avant de modifier la politique de groupe. Sinon, vous devrez peut-être simplement créer l'objet, puis revenir ultérieurement pour créer les objets de réseau et toutes les entrées de contrôle d'accès dont vous avez besoin. Pour créer la liste de contrôle d'accès, allez à **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)** > **Smart CLI** > **Objects (Objets)**, créez un objet puis sélectionnez **Extended Access List** (Liste d'accès étendue) comme type d'objet. Pour obtenir un exemple, consultez Comment contrôler l'accès VPN RA par groupe, à la page 70.

- **Restrict VPN to VLAN** (Restreindre le VPN au VLAN) : aussi appelé « VLAN mapping (mappage VLAN) », cet attribut précise l'interface VLAN de sortie pour les sessions auxquelles s'applique cette politique de groupe. Le système transfère tout le trafic de ce groupe vers le VLAN sélectionné.

  Utilisez cet attribut pour affecter un VLAN à la politique de groupe pour simplifier le contrôle d'accès. L'affectation d'une valeur à cet attribut est une alternative à l'utilisation d'une liste de contrôle d'accès pour filtrer le trafic sur une session. Assurez-vous de spécifier un numéro de VLAN défini sur une sous-interface du périphérique. Les valeurs sont comprises entre 1 et 4 094.

Attributs de mandataire de navigateur Windows

Les attributs de mandataire du navigateur Windows d'une politique de groupe déterminent si et comment fonctionne un mandataire défini dans le navigateur de l'utilisateur.

Vous pouvez sélectionner l'une des valeurs suivantes pour le **mandataire du navigateur pendant la session VPN** :

- **No change in endpoint settings** (pas de modification des paramètres de point terminal) : permet à l'utilisateur de configurer (ou de ne pas configurer) un mandataire de navigateur pour HTTP et d'utiliser le mandataire s'il est configuré.
- **Disable browser proxy** (Désactiver le mandataire du navigateur) : n'utilisez pas le mandataire défini pour le navigateur, le cas échéant. Aucune connexion du navigateur ne passera par le serveur mandataire.
- **Auto detect settings** (Paramètres de détection automatique) : activez l'utilisation de la détection automatique du serveur mandataire dans le navigateur pour la machine cliente.
- **Use custom settings** (Utiliser les paramètres personnalisés) : définissez un serveur mandataire qui doit être utilisé par tous les périphériques clients pour le trafic HTTP. Configurez les paramètres suivants :
  - **Proxy Server IP or Hostname (Adresse IP ou nom d'hôte du serveur mandataire)**, **Port** : adresse IP, ou nom d'hôte, du serveur mandataire et port utilisé pour les connexions proxy. La combinaison de l'hôte et du port ne peut pas dépasser 100 caractères.
  - **Browser Exemption List** (Liste d'exemptions de proxy pour navigateur) : les connexions aux hôtes ou ports figurant dans cette liste ne passent pas par le serveur mandataire. Ajoutez toutes les valeurs d'hôte et port pour les destinations qui ne doivent pas utiliser le serveur mandataire. Par exemple, www.exemple.com port 80. Cliquez sur le lien **Add** (Ajouter) pour ajouter des éléments à la liste. Cliquez sur l'icône de la corbeille pour supprimer des éléments. La liste d'exceptions de serveurs mandataires complète, en combinant l'ensemble des adresses et des ports, ne peut pas dépasser 255 caractères.

Surveillance du VPN d'accès à distance

Pour surveiller et dépanner les connexions VPN d'accès à distance, ouvrez la console CLI ou connectez-vous à l'interface de ligne de commande du périphérique et utilisez les commandes suivantes.

- **show vpn-sessiondb** affiche les renseignements sur les sessions VPN. Vous pouvez réinitialiser ces statistiques à l'aide de la commande **clear vpn-sessiondb**.
- La commande **show webvpn** *keyword* affiche des renseignements sur la configuration du VPN d'accès à distance, y compris les statistiques et les images AnyConnect installées. Saisissez **show webvpn ?** pour afficher les mots-clés disponibles.
- **show aaa-server** affiche les statistiques sur le serveur de répertoire utilisé avec le VPN d'accès à distance.

Dépannage des VPN d'accès à distance

Les problèmes de connexion VPN d'accès à distance peuvent provenir du client ou de la configuration du périphérique FTD. Les rubriques suivantes couvrent les principaux problèmes de dépannage que vous pourriez rencontrer.

Dépannage des problèmes de connexion SSL

Si l'utilisateur ne peut pas établir la connexion SSL initiale, non-client AnyConnect, avec l'adresse IP externe afin de télécharger client AnyConnect, procédez comme suit :

1. Si vous avez configuré un port autre que celui par défaut pour le profil de connexion VPN d'accès à distance, vérifiez que l'utilisateur inclut le numéro de port dans l'URL. Par exemple : https://ravpn.example.com:4443
2. À partir du poste de travail client, vérifiez que vous pouvez effectuer un ping vers l'adresse IP Si vous ne le pouvez pas, déterminez pourquoi il n'y a pas de routage entre le poste de travail de l'utilisateur et l'adresse.
3. À partir du poste de travail client, vérifiez que vous pouvez effectuer un ping vers le nom de domaine complet (FQDN) de l'interface externe, celui défini dans le profil de connexion VPN d'accès à distance (RA). Si vous pouvez pinguer l'adresse IP, mais pas le nom de domaine complet (FQDN), vous devez mettre à jour les serveurs DNS utilisés par le client et le profil de connexion VPN d'accès à distance (RA) afin d'ajouter le mappage FQDN–adresse IP.
4. Vérifiez que l'utilisateur accepte le certificat présenté par l'interface externe. L'utilisateur doit l'accepter définitivement.
5. Examinez la configuration de la connexion VPN d'accès à distance et vérifiez que vous avez sélectionné la bonne interface externe. Une erreur courante est de sélectionner une interface interne, celle faisant face aux réseaux internes, plutôt que l'interface externe, qui fait face aux utilisateurs de VPN d'accès à distance.
6. Si le chiffrement SSL est correctement configuré, utilisez un analyseur de paquets externe pour vérifier si l'établissement de liaison TCP à trois voies a réussi.

Dépannage des problèmes de téléchargement et d'installation client AnyConnect

Si l'utilisateur peut établir une connexion SSL avec l'interface externe, mais ne peut pas télécharger et installer le progiciel client AnyConnect, tenez compte des éléments suivants :

- Assurez-vous d'avoir chargé un paquet client AnyConnect pour le système d'exploitation du client. Par exemple, si le poste de travail de l'utilisateur exécute Linux, mais que vous n'avez pas chargé d'image Linux client AnyConnect, aucun paquet ne pourra être installé.
- Pour les clients Windows, l'utilisateur doit disposer de droits d'administrateur pour installer le logiciel.
- Pour les clients Windows, le poste de travail doit activer ActiveX ou installer Java JRE 1.5 ou version ultérieure, avec JRE 7 recommandé.
- Pour les navigateurs Safari, Java doit être activé.
- Essayez différents navigateurs, l'un d'eux pourrait échouer alors qu'un autre réussit.

Dépannage des problèmes de connexion client AnyConnect

Si l'utilisateur a pu se connecter à l'interface externe, télécharger et installer client AnyConnect, mais n'a pas pu ensuite établir une connexion à l'aide de client AnyConnect, tenez compte des éléments suivants :

- Si l'authentification échoue, vérifiez que l'utilisateur saisit le bon nom d'utilisateur et le bon mot de passe, et que le nom d'utilisateur est défini correctement dans le serveur d'authentification. Le serveur d'authentification doit également être disponible dans l'une des interfaces de données.

Remarque Si le serveur d'authentification se trouve sur un réseau externe, vous devez configurer une connexion VPN de site à site avec le réseau externe et inclure l'adresse de l'interface VPN d'accès à distance dans le VPN. Pour de plus amples renseignements, consultez la section Comment utiliser un serveur de répertoire sur un réseau externe avec le VPN d'accès à distance, à la page 56.

- Si vous avez configuré un nom de domaine complet (FQDN) pour l'interface externe dans le profil de connexion VPN d'accès à distance (RA), vérifiez que vous pouvez pinguer le FQDN à partir du périphérique client. Si vous pouvez pinguer l'adresse IP, mais pas le nom de domaine complet (FQDN), vous devez mettre à jour les serveurs DNS utilisés par le client et le profil de connexion VPN d'accès à distance (RA) afin d'ajouter le mappage FQDN–adresse IP. Si vous utilisez le profil par défaut client AnyConnect qui est généré lorsque vous spécifiez un nom de domaine complet pour l'interface externe, l'utilisateur devra modifier l'adresse du serveur pour utiliser l'adresse IP jusqu'à ce que le DNS soit mis à jour.
- Vérifiez que l'utilisateur accepte le certificat présenté par l'interface externe. L'utilisateur doit l'accepter définitivement.
- Si le client AnyConnect de l'utilisateur comprend plusieurs profils de connexion, qu'il sélectionne le bon.
- Si tout semble correct du côté du client, établissez une connexion SSH avec le périphérique FTD et entrez la commande **debug webvpn** [ ]. Examinez les messages émis lors d'une tentative de connexion.

Dépannage des problèmes de flux de trafic du VPN d'accès à distance

Si l'utilisateur peut établir une connexion VPN d'accès à distance sécurisé (RA), mais ne peut pas envoyer et recevoir le trafic, procédez comme suit :

1. Demandez au client de se déconnecter, puis de se reconnecter. Parfois, cela élimine le problème.
2. Dans client AnyConnect, vérifiez les statistiques de trafic pour déterminer si les compteurs envoyés et reçus augmentent. Si le nombre de paquets reçus reste à zéro, le périphérique FTD ne renvoie aucun trafic. Il y a probablement un problème dans la configuration FTD. Les problèmes courants sont les suivants :
   - Les règles d'accès bloquent le trafic. Vérifiez la stratégie de contrôle d'accès pour connaître les règles qui empêchent le trafic entre les réseaux internes et l'ensemble des adresses du VPN d'accès à distance. Vous devrez peut-être créer une règle Allow (Autoriser) explicite si votre action par défaut est de bloquer le trafic.
   - Le filtre VPN bloque le trafic. Vérifiez le filtre de trafic d'ACL ou le filtre de VLAN configuré dans la politique de groupe pour le profil de connexion. Vous devrez peut-être effectuer des ajustements dans l'ACL ou modifier le VLAN, selon la façon (ou si) vous filtrez le trafic en fonction de la politique de groupe.
   - Les règles de NAT ne sont pas contournées pour le trafic VPN d'accès à distance. Assurez-vous que l'exemption de NAT est configurée pour la connexion VPN d'accès à distance pour chaque interface interne. Sinon, vérifiez que les règles de NAT n'affectent pas la communication entre les réseaux et les interfaces internes et l'ensemble d'adresses VPN d'accès à distance et l'interface externe.
   - Les routes sont mal configurées. Assurez-vous que toutes les routes définies sont valides et fonctionnent correctement. Par exemple : si une adresse IP statique est définie pour l'interface externe, assurez-vous que la table de routage comprend une route par défaut (pour 0.0.0.0/0 et ::/0).
   - Assurez-vous que le serveur DNS et le nom de domaine configurés pour le VPN d'accès à distance sont corrects et que le système client utilise les appropriés. Vérifiez que les serveurs DNS sont accessibles.
   - Si vous activez la tunnellisation fractionnée dans le VPN d'accès à distance, vérifiez si le trafic vers les réseaux internes spécifiés passe par le tunnel, tandis que tout autre trafic contourne le tunnel (de sorte que le périphérique FTD ne le voit pas).
3. Établissez une connexion SSH avec le périphérique FTD et vérifiez que le trafic est envoyé et reçu pour le VPN d'accès à distance. Utilisez les commandes suivantes :
   - **show webvpn anyconnect**
   - **show vpn-sessiondb**

Exemples d'utilisation du VPN d'accès à distance

Voici des exemples de configuration d'un VPN d'accès à distance.

Comment mettre en œuvre la modification d'autorisation RADIUS

Le changement d'autorisation (CoA) RADIUS, aussi appelé autorisation dynamique, assure la sécurité des points terminaux pour le VPN d'accès à distance Cisco Firepower Threat Defense. Un défi clé pour les VPN d'accès à distance est de sécuriser le réseau interne contre les points terminaux compromis et de sécuriser le point terminal lui-même lorsqu'il est affecté par des virus ou des programmes malveillants, en corrigeant l'attaque sur le point terminal. Il est nécessaire de sécuriser le point terminal et le réseau interne à toutes les étapes, c'est-à-dire avant, pendant et après la session VPN d'accès à distance. La fonctionnalité RADIUS CoA aide à atteindre cet objectif.

Si vous utilisez des serveurs RADIUS Cisco Identity Services Engine (ISE), vous pouvez configurer l'application de la politique de modification d'autorisation.

La fonctionnalité de changement d'autorisation ISE fournit un mécanisme pour modifier les attributs d'une session d'authentification, d'autorisation et de comptabilité (AAA) après son établissement. Lorsqu'une politique est modifiée pour un utilisateur ou un groupe d'utilisateurs dans AAA, ISE envoie des messages CoA au périphérique Cisco Firepower Threat Defense pour réinitialiser l'authentification et appliquer la nouvelle politique. Un point d'application de posture en ligne (IPEP) n'est pas nécessaire pour appliquer les listes de contrôle d'accès (ACL) à chaque session VPN établie avec le périphérique Cisco Firepower Threat Defense.

Les rubriques suivantes expliquent comment fonctionne le CoA et comment le configurer.

Flux système pour la modification d'autorisation

Cisco ISE dispose d'un agent de posture client qui évalue la conformité d'un point terminal pour des critères tels que les processus, les fichiers, les entrées de registre, la protection antivirus, la protection contre les logiciels espions et les logiciels de pare-feu installés sur l'hôte. Les administrateurs peuvent ensuite restreindre l'accès au réseau jusqu'à ce que le terminal soit conforme, ou rehausser les privilèges de l'utilisateur local afin qu'il puisse mettre en place des mesures correctives. ISE Posture effectue une évaluation côté client. Le client reçoit d'ISE la politique d'exigences de posture, effectue la collecte des données de posture, compare les résultats à la politique et renvoie les résultats de l'évaluation à ISE.

Voici le flux système entre le périphérique Cisco Firepower Threat Defense, ISE et le client VPN d'accès à distance (RA) pour le traitement de la modification d'autorisation (CoA).

1. L'utilisateur distant démarre une session VPN d'accès à distance à l'aide de client AnyConnect, avec le périphérique Cisco Firepower Threat Defense.
2. Le périphérique Cisco Firepower Threat Defense envoie un message de demande d'accès RADIUS pour cet utilisateur au serveur ISE.
3. Comme la posture du client est inconnue à ce stade, ISE fait correspondre l'utilisateur à la politique d'autorisation configurée pour une posture inconnue. Cette politique définit les options cisco-av-pair suivantes, qu'ISE envoie à Cisco Firepower Threat Defense dans une réponse RADIUS Access-Accept.
   - **url-redirect-acl=***acl_name*, où *acl_name* est le nom d'une liste de contrôle d'accès étendue configurée sur le périphérique Cisco Firepower Threat Defense. Cette liste de contrôle d'accès définit le trafic d'utilisateur qui doit être redirigé vers le serveur ISE, qui est le trafic HTTP. Par exemple :

     ```
     url-redirect-acl=redirect
     ```

   - **url-redirect=***url*, où l'URL est celle vers laquelle le trafic doit être redirigé. Par exemple :

```
url-redirect=https://ise2.example.com:8443/guestportal/gateway?sessionId=xx&action=cpp
```

Vous devez configurer le DNS pour les interfaces de données afin que le nom d'hôte puisse être résolu. Si vous configurez également le filtrage du trafic dans la politique de groupe pour le profil de connexion, vérifiez que l'ensemble de clients peut atteindre le serveur ISE par le port (TCP/8443 dans l'exemple).

4. Le périphérique Cisco Firepower Threat Defense envoie un paquet de début de demande de comptabilité RADIUS et reçoit une réponse d'ISE. La demande de comptabilité comprend tous les détails de la session, y compris l'ID de session, l'adresse IP externe du client VPN et l'adresse IP du périphérique Cisco Firepower Threat Defense. ISE utilise l'ID de session pour identifier cette session. Le périphérique Cisco Firepower Threat Defense envoie également des informations de comptabilité intérimaire périodiques, dont l'attribut le plus important est Framed-IP-Address, contenant l'adresse IP attribuée au client par le périphérique Cisco Firepower Threat Defense.
5. Lorsqu'il est dans un état de posture inconnu, le périphérique Cisco Firepower Threat Defense redirige le trafic du client qui correspond à l'ACL de redirection vers l'URL de redirection. ISE détermine si le client dispose du module de conformité de posture requis et invite l'utilisateur à l'installer au besoin.
6. Une fois l'agent installé sur le périphérique client, il effectue automatiquement les vérifications configurées dans la politique de posture ISE. Le client communique directement avec ISE. Il envoie un rapport de posture à ISE, lequel peut inclure plusieurs échanges utilisant le protocole SWISS et les ports TCP/UDP 8905.
7. Lorsqu'ISE reçoit le rapport de posture de l'agent, il traite à nouveau les règles d'autorisation. Cette fois, le résultat de la posture est connu et une règle différente correspond maintenant au client. ISE envoie un paquet RADIUS CoA, qui inclut une liste de contrôle d'accès téléchargeable (DACL) pour les points terminaux conformes ou non conformes. Par exemple, la DACL conforme peut autoriser tous les accès, tandis que la DACL non conforme refuse tous les accès. Le contenu de la DACL relève de l'administrateur ISE.
8. Le périphérique Cisco Firepower Threat Defense supprime la redirection. S'il n'a pas les listes de contrôle d'accès en cache, il doit envoyer une demande d'accès afin de les télécharger à partir d'ISE. La DACL spécifique est associée à la session VPN ; elle ne fait pas partie de la configuration du périphérique.
9. La prochaine fois que l'utilisateur du VPN d'accès à distance tente d'accéder à la page Web, il peut accéder aux ressources autorisées par la DACL installée sur le périphérique Cisco Firepower Threat Defense pour la session.

Remarque Si le point terminal ne satisfait pas à une exigence obligatoire et qu'une correction manuelle est requise, une fenêtre de correction s'ouvre dans le client AnyConnect, affichant les éléments nécessitant une intervention. La fenêtre de correction s'exécute en arrière-plan afin que les mises à jour de l'activité du réseau ne s'affichent pas et n'interfèrent pas ou ne provoquent pas de perturbations. Un utilisateur peut cliquer sur **Details** (Détails) dans la partie vignette de la posture ISE du client AnyConnect afin de voir ce qui a été détecté et les mises à jour requises avant de pouvoir rejoindre le réseau.

Configurer Change of Authorization (modification d'autorisation) sur le périphérique FTD

La majeure partie de la politique Change of Authorization (changement d'autorisation) est configurée dans le serveur ISE. Cependant, vous devez configurer le périphérique Cisco Firepower Threat Defense pour une

connexion correcte à ISE. La procédure suivante explique comment configurer le côté Cisco Firepower Threat Defense de la configuration.

Avant de commencer

Si vous utilisez des noms d'hôte dans un objet, veillez à configurer les serveurs DNS à utiliser avec les interfaces de données, comme expliqué dans la section Configuration DNS pour les données et le trafic de gestion. Vous devez généralement configurer le DNS de toute façon pour avoir un système entièrement fonctionnel.

Procédure

Étape 1 Configurez la liste de contrôle d'accès (ACL) étendue pour rediriger les connexions initiales vers ISE.

L'objectif de la liste de contrôle d'accès de redirection est d'envoyer le trafic initial à ISE afin qu'ISE puisse évaluer la posture du client. La liste de contrôle d'accès doit envoyer le trafic HTTPS à ISE, mais pas le trafic déjà destiné à ISE ou le trafic dirigé vers un serveur DNS pour la résolution de nom. Un exemple d'ACL de redirection peut ressembler à ce qui suit :

```
access-list redirect extended deny ip any host <ISE server IP>
access-list redirect extended deny ip any host <DNS server IP>
access-list redirect extended deny icmp any any
access-list redirect extended permit tcp any any eq www
```

Cependant, notez que les listes de contrôle d'accès ont un « deny any any » (refuser tout) implicite comme dernière entrée de contrôle d'accès (ACE). Dans cet exemple, la dernière ACE, qui correspond au port TCP www (c'est-à-dire au port 80), ne correspondra à aucun trafic correspondant aux 3 premières ACE, qui sont donc redondantes. Vous pouvez simplement créer une liste de contrôle d'accès avec la dernière ACE et obtenir les mêmes résultats.

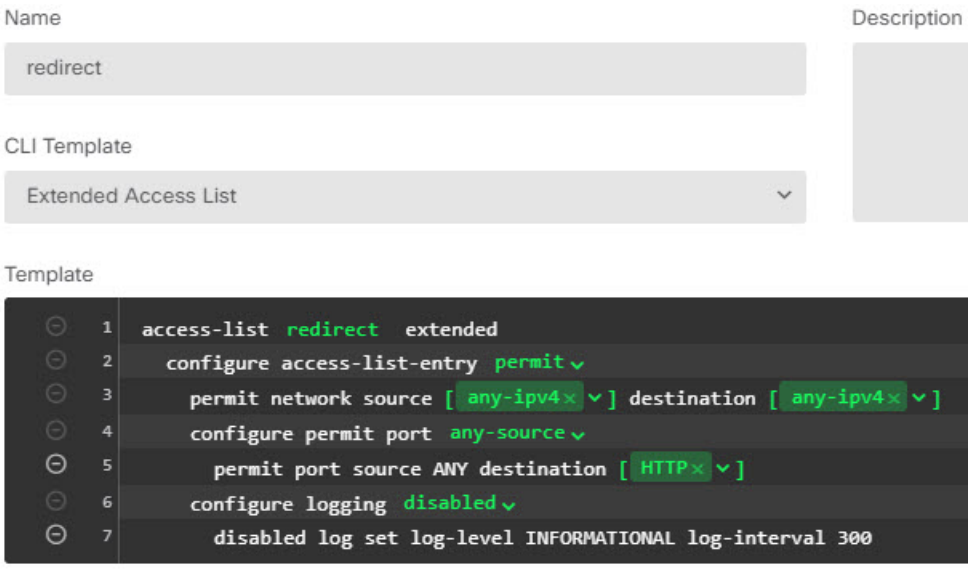
Notez que dans une liste de contrôle d'accès de redirection, les actions permit (autoriser) et deny (refuser) déterminent simplement quel trafic correspond à la liste de contrôle d'accès, avec permit correspondant et deny ne correspondant pas. Aucun trafic n'est réellement abandonné, le trafic refusé n'est tout simplement pas redirigé vers ISE.

Pour créer la liste de contrôle d'accès de redirection, vous devez configurer un objet Smart CLI.

a) Choisissez **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)** > **Smart CLI** > **Objects (Objets)**.
b) Cliquez sur **+** pour créer un nouvel objet.
c) Saisissez un nom pour la liste de contrôle d'accès. Par exemple, **rediriger**.
d) Pour **CLI Template** (Modèle CLI), sélectionnez **Extended Access List** (Liste d'accès étendue).
e) Configurez les éléments suivants dans le **corps du modèle** :

- configurer l'action de liste d'accès = autoriser
- réseau-source = any-ipv4
- réseau-destination = any-ipv4
- configurer autoriser port = any-source
- port-destination = HTTP
- configurer la journalisation = désactivée

L'ACE doit ressembler à ce qui suit :



f) Cliquez sur **OK**.

Cette liste de contrôle d'accès sera configurée lors du prochain déploiement de modifications. Vous n'avez pas besoin d'utiliser l'objet dans une autre politique pour forcer le déploiement.

Remarque
Cette liste de contrôle d'accès s'applique uniquement à IPv4. Si vous voulez également prendre en charge IPv6, ajoutez simplement une deuxième ACE avec tous les mêmes attributs, sauf que vous devez sélectionner any-ipv6 pour les réseaux source et de destination. Vous pouvez également ajouter les autres ACE pour vous assurer que le trafic vers le serveur ISE ou vers le serveur DNS n'est pas redirigé. Vous devrez d'abord créer des objets de réseau hôtes pour contenir les adresses IP de ces serveurs.

Étape 2 Configurer un groupe de serveurs RADIUS pour l'autorisation dynamique.

Il existe plusieurs options essentielles que vous devez sélectionner correctement dans le serveur RADIUS et les objets de groupe de serveurs pour activer la modification d'autorisation, également connue sous le nom d'autorisation dynamique. La procédure suivante se concentre sur ces attributs. Pour plus de détails sur ces objets, consultez Serveurs et groupes RADIUS.

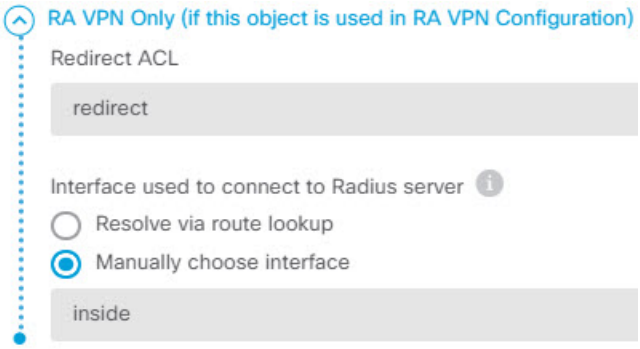
a) Choisissez **Objects (Objets)** > **Identity Sources (Sources d'identité)**.
b) Cliquez sur **+** > **RADIUS Server** (Serveur RADIUS).
c) Saisissez un nom pour le serveur, ainsi que le nom d'hôte/l'adresse IP du serveur ISE RADIUS, le port d'authentification et la clé secrète configurés sur le serveur. Ajustez le délai d'expiration si vous le souhaitez. Ces options ne sont pas directement liées à l'autorisation dynamique.
d) Cliquez sur le lien RA VPN Only (RA VPN uniquement) et configurez les options suivantes :

- **Redirect ACL**(ACL de redirection) —sélectionnez la liste de contrôle d'accès étendue que vous avez créée pour la redirection. Dans cet exemple, l'ACL nommée redirect.
- **Interface used to connect to Radius server** (Interface utilisée pour la connexion au serveur RADIUS) —sélectionnez **Manually Choose Interface** (Sélectionner l'interface manuellement, puis sélectionnez l'interface par laquelle le serveur peut être atteint. Vous devez sélectionner une interface spécifique pour que le système puisse activer correctement l'écouteur CoA sur celle-ci.

Si le serveur se trouve sur le même réseau que l'adresse de gestion, ce qui signifie que vous sélectionnerez l'interface de diagnostic, vous devez également configurer une adresse IP sur l'interface de diagnostic. Il n'est pas suffisant d'avoir une adresse IP de gestion. Accédez à **Device (Appareil)** > **Interfaces**, et configurez une adresse IP sur l'interface de diagnostic qui se trouve sur le même sous-réseau que l'adresse IP de gestion.

Si vous utilisez également ce serveur pour l'accès administratif FDM, cette interface est ignorée. Les tentatives d'accès administratif sont toujours authentifiées via l'adresse IP de gestion.

L'exemple suivant montre les options configurées pour l'interface interne.



e) Cliquez sur **OK** pour enregistrer l'objet serveur.

Si vous avez une configuration redondante avec plusieurs serveurs ISE RADIUS en double, créez des objets serveur pour chacun de ces serveurs.

f) Cliquez sur **+** > **RADIUS Server Group** (Groupe de serveurs RADIUS.

g) Saisissez un nom pour le groupe de serveurs et ajustez le temps mort et le nombre maximal de tentatives si vous le souhaitez.

h) Sélectionnez l'option **Dynamic Authorization** (Autorisation dynamique) et modifiez le numéro de port si votre serveur ISE est configuré pour utiliser un port différent. Le port 1700 est le port par défaut utilisé pour l'écoute des paquets CoA.

i) Si le serveur RADIUS est configuré pour utiliser un serveur AD pour authentifier les utilisateurs, sélectionnez le **domaine qui prend en charge le serveur RADIUS** qui spécifie le serveur AD utilisé en liaison avec ce serveur RADIUS. Si le domaine n'existe pas déjà, cliquez sur **Create New Identity Realm** (Créer un nouveau domaine d'identité au bas de la liste et configurez-le maintenant.

j) Sous **RADIUS Server** (Serveur RADIUS), cliquez sur **+** et sélectionnez l'objet serveur que vous avez créé pour le VPN d'accès à distance.

k) Cliquez sur **OK** pour enregistrer l'objet du groupe de serveurs.

Étape 3 Choisissez **Device (Périphérique)** > **RA VPN (VPN d'accès à distance)** > **Connection Profiles (Profils de connexion**, puis créez un profil de connexion qui utilise ce groupe de serveurs RADIUS.

Utilisez **l'authentification AAA** (uniquement ou avec des certificats) et sélectionnez le groupe de serveurs dans la **source d'identité principale pour les options d'authentification de l'utilisateur**, **d'autorisation** et **de comptabilité**.

Configurez toutes les autres options en fonction des besoins de votre organisation.

Remarque

Si les serveurs DNS sont accessibles via le réseau VPN, modifiez la politique de groupe utilisée dans le profil de connexion pour configurer l'option **Split DNS** (DNS fractionnée) sur la page Split Tunneling Attributes (Attributs de tunnellisation fractionnée).

Configurer la modification d'autorisation dans ISE

La majeure partie de la configuration de changement d'autorisation est effectuée dans le serveur ISE. ISE dispose d'un agent d'évaluation de posture qui fonctionne sur le périphérique terminal, et ISE communique directement avec le périphérique pour déterminer la position de posture. Le périphérique Cisco Firepower Threat Defense attend essentiellement les instructions d'ISE sur la façon de gérer un utilisateur final donné.

Une description complète de la configuration des politiques d'évaluation de la posture n'entre pas dans le cadre de ce document. Cependant, la procédure suivante explique certains des principes de base. Utilisez-le comme point de départ pour la configuration d'ISE. Notez que les chemins de commande exacts, les noms de page et les noms d'attribut peuvent changer d'une version à l'autre. La version d'ISE que vous utilisez peut utiliser une terminologie ou une organisation différente.

La version ISE minimale prise en charge est de 2.2 correctif 1.

Avant de commencer

Cette procédure suppose que vous ayez déjà configuré les utilisateurs dans le serveur ISE RADIUS.

Procédure

Étape 1 Choisissez **Administration** > **Network Resources (Ressources réseau)** > **Network Devices (Périphériques réseau)** > **Network Devices (Périphériques réseau)**, ajoutez le périphérique Cisco Firepower Threat Defense à l'inventaire des périphériques réseau ISE et configurez les paramètres RADIUS.

Sélectionnez les **RADIUS Authentication Settings** (Paramètres d'authentification RADIUS) et configurez le même **Shared Secret** (Secret partagé) que celui configuré dans l'objet serveur RADIUS Cisco Firepower Threat Defense. Si vous le souhaitez, modifiez le numéro **de port CoA** et veillez à configurer le même port dans l'objet de groupe de serveurs RADIUS Cisco Firepower Threat Defense.

Étape 2 Choisissez **Policy (Politique)** > **Policy Elements (Éléments de politique)** > **Results (Résultats)** > **Authorization (Autorisation)** > **Downloadable ACLs (ACL téléchargeables)**.

Créez 2 listes de contrôle d'accès téléchargeables (DACL), une pour une utilisation par des points terminaux conformes, et une pour les points terminaux non conformes.

Par exemple, vous pouvez autoriser tous les accès pour les points terminaux conformes (autoriser ip any any), tout en refusant tout accès aux points terminaux non conformes (refuser ip any any). Vous pouvez rendre ces listes de contrôle d'accès aussi complexes que vous le souhaitez, pour fournir l'accès exact que les utilisateurs doivent avoir en fonction de leur état de conformité. Vous utiliserez ces listes de contrôle d'accès dans les profils d'autorisation.

Étape 3 Choisissez **Policy (Politique)** > **Policy Elements (Éléments de politique)** > **Results (Résultats)** > **Authorization (Autorisation)** > **Authorization Profile (Profil d'autorisation)**, puis configurez les profils requis.

Vous avez besoin de profils pour les états suivants. Les attributs minimaux pour chacun sont répertoriés.

- **Unknown** (Inconnu) : le profil de posture inconnu est le profil de posture par défaut. Chaque terminal est mis en correspondance avec cette politique lors de l'établissement initial de la connexion VPN d'accès à distance. Le point de cette règle est d'appliquer la liste de contrôle d'accès et l'URL de redirection, et de télécharger l'agent de posture s'il n'est pas déjà sur le point terminal. Les points terminaux peuvent rester associés à ce profil si l'agent n'est pas installé ou si l'installation échoue. Sinon, après avoir évalué la posture, les points terminaux passent aux profils conforme ou non conforme.

  Les attributs minimaux incluent les suivants :

  - **Name** (Nom) : par exemple, PRE_POSTURE.
  - **Access Type** (Type d'accès) : sélectionnez **ACCESS_ACCEPT**.
  - **Common Tasks** (Tâches courantes) : sélectionnez **Web Redirection** (Redirection Web) (CWA, MDM, NSP, CPP), puis **Client Provisioning** (Provisionnement de client) (Posture), et saisissez le nom de l'ACL de redirection que vous avez configurée sur le périphérique Cisco Firepower Threat Defense. Dans **Value** (Valeur), sélectionnez **Client Provisioning Portal** (Portail de provisionnement client) s'il n'est pas déjà sélectionné.
  - Les **Attribute Details** (Détails de l'attribut) doivent afficher deux valeurs cisco-av-pair, pour url-redirect-acl et url-redirect. ISE enverra ces données au périphérique Cisco Firepower Threat Defense, qui appliquera les critères à la session utilisateur du VPN d'accès à distance.

- **Compliant (Conforme)**: après la fin de l'évaluation de la posture, si le point terminal respecte toutes les exigences configurées, le client est considéré comme conforme et reçoit ce profil. Vous donneriez généralement à ce client un accès complet.

  Les attributs minimaux incluent les suivants :

  - **Name** (Nom) : par exemple, FULL_ACCESS.
  - **Access Type** (Type d'accès) : sélectionnez **ACCESS_ACCEPT**.
  - **Common Tasks** (Tâches courantes) : sélectionnez **DACL Name**, puis la liste de contrôle d'accès téléchargeable pour les utilisateurs conformes, par exemple, PERMIT_ALL_TRAFFIC. ISE enverra la liste de contrôle d'accès au périphérique Cisco Firepower Threat Defense, qui l'appliquera à la session utilisateur. Cette DACL remplacera l'ACL de redirection initiale pour la session utilisateur.

- **Non-compliant** (Non conforme) : si l'évaluation de la posture détermine que le point terminal ne satisfait pas à toutes les exigences, un compte à rebours démarre pendant lequel le client peut mettre le terminal en conformité, par exemple en installant les mises à jour requises. Le client AnyConnect informe l'utilisateur des problèmes de conformité. Pendant le compte à rebours, le terminal reste dans l'état de conformité inconnu. Si le point terminal reste non conforme après l'expiration du compte à rebours, la session est marquée comme non conforme et elle obtient le profil non conforme. Vous devez généralement empêcher tout accès pour ce point terminal ou au moins restreindre l'accès d'une manière ou d'une autre.

  Les attributs minimaux incluent les suivants :

  - **Name** (Nom) : par exemple, Non_Compliant.
  - **Access Type** (Type d'accès) : sélectionnez **ACCESS_ACCEPT**.
  - **Common Tasks** (Tâches courantes) : sélectionnez **DACL Name**, puis la liste de contrôle d'accès téléchargeable pour les utilisateurs non conformes, par exemple, DENY_ALL_TRAFFIC. ISE enverra la liste de contrôle d'accès au périphérique Cisco Firepower Threat Defense, qui l'appliquera à la session utilisateur. Cette liste de contrôle d'accès remplacera l'ACL de redirection initiale pour la session utilisateur.

Étape 4 Choisissez **Policy (Politique)** > **Policy Elements (Éléments de politique)** > **Results (Résultats)** > **Client Provisioning (Provisionnement de client)** > **Resources (Ressources)**, puis configurez les ressources suivantes :

- **AnyConnect package** (Package AnyConnect) : le fichier de package head-end, que vous téléchargez depuis software.cisco.com. Vous avez besoin de packages distincts pour les plateformes client prises en charge ; vous devrez donc peut-être configurer plusieurs types, comme AnyConnectDesktopWindows.
- **ISE Posture Configuration File** (Fichier de configuration de posture ISE) : ce fichier de configuration définit les paramètres utilisés par le module de conformité pour évaluer le périphérique de l'utilisateur final. Ce fichier définit également le délai dont dispose l'utilisateur pour mettre en conformité un périphérique non conforme.
- **Compliance Module Package** (Package du module de conformité) (Type : ComplianceModule) : le fichier du module de conformité client AnyConnect est distribué vers le package AnyConnect installé afin de vérifier la conformité du point terminal. Téléchargez ce fichier à l'aide de la commande **Add Resource from Cisco Site** (Ajouter une ressource à partir du site Cisco). Assurez-vous de téléchargerle module approprié en fonction des packages client AnyConnect configurés, sans quoi les utilisateurs rencontreront des échecs de téléchargement. Vous pouvez également trouver ces fichiers sur software.cisco.com dans les listes client AnyConnect du dossier ISEComplianceModule.
- **AnyConnect Configuration File** (Fichier de configuration AnyConnect) (Type : AnyConnectConfig) : ces paramètres spécifiques à la version client AnyConnect définissent le **AnyConnect Package** (Package AnyConnect), le **Compliance Module (Module de conformité)** et la **ISE Posture (Posture ISE)** à appliquer. Comme les paquets sont propres au système d'exploitation, créez des fichiers de configuration distincts pour chaque SE client pris en charge (par exemple : Windows, Mac, Linux).

Étape 5 Choisissez **Policy (Politique)** > **Client Provisioning (Provisionnement de client)**, puis configurez la politique de provisionnement de client.

Créez de nouvelles règles, par exemple avec des noms comme CoA_ClientProvisionWin, pour chaque système d'exploitation devant mettre en œuvre CoA. Sélectionnez le système d'exploitation approprié pour la règle et, dans **Results** (Résultats), sélectionnez le fichier de configuration client AnyConnect créé pour ce système d'exploitation en tant qu'**Agent**.

Désactivez les règles par défaut propres au système d'exploitation que vous remplacez.

Étape 6 Configurez la politique de posture.

Au cours de cette étape, vous développez les exigences de posture qui ont du sens pour votre organisation.

- Choisissez **Policy (Politique)** > **Policy Elements (Éléments de politique)** > **Conditions** > **Posture**, puis définissez les conditions de posture simples à respecter. Par exemple, vous pouvez exiger que l'utilisateur ait certaines applications installées.
- Choisissez **Policy (Politique)** > **Policy Elements (Éléments de politique)** > **Results (Résultats)** > **Posture** > **Exigences**, puis définissez l'exigence du module de conformité pour le point terminal.
- Choisissez **Politiques** > **Posture** > **Politique de posture** et configurez les politiques pour les systèmes d'exploitation pris en charge.

Étape 7 Choisissez **Policy (Politique)** > **Policy Sets (Ensembles de politiques)** > **Default (Par défaut)** > **Authorization Policy (Politique d'autorisation)**, puis créez la politique.

Ajoutez des règles pour chacune des conditions de conformité. Ces exemples de valeurs sont basés sur les exemples des étapes précédentes.

- Inconnu, pour la pré-posture et le téléchargement de posture.
  - Name (Nom) : par exemple, PRE_POSTURE.
  - Conditions : « Session-PostureStatus EST ÉGAL À Inconnu » ET « Radius-NAS-Port-Type EST ÉGAL À Virtual »
  - Profiles (Profils) : par exemple, PRE_POSTURE
- Conforme, pour les clients qui répondent aux exigences de posture.
  - Name (Nom) : par exemple, FULL_ACCESS.
  - Conditions : « Session-PostureStatus EST ÉGAL À Conforme » ET « Radius-NAS-Port-Type EST ÉGAL À Virtual »
  - Profiles (Profils) : par exemple, FULL_ACCESS
- Non-conformité, pour les clients qui ne parviennent pas aux exigences de posture.
  - Name (Nom) : par exemple, NON-COMPLIANT
  - Conditions : « Session-PostureStatus EST ÉGAL À NonConforme » ET « Radius-NAS-Port-Type EST ÉGAL À Virtual »
  - Profiles (Profils) : par exemple, Non_Compliant

Étape 8 (Facultatif) Choisissez **Administration** > **Settings (Paramètres)** > **Posture** > **Reassessments (Réévaluations)**, puis activez la réévaluation de la posture.

Par défaut, la posture est évaluée au moment de la connexion uniquement. Vous pouvez activer la réévaluation de la posture pour vérifier périodiquement la posture des points terminaux connectés. Vous pouvez définir l'intervalle de réévaluation pour déterminer la fréquence à laquelle cela se produit.

Si le système échoue lors de la réévaluation, vous pouvez définir la réponse du système. Vous pouvez autoriser l'utilisateur à continuer (rester connecté), le déconnecter ou lui demander de corriger le système.

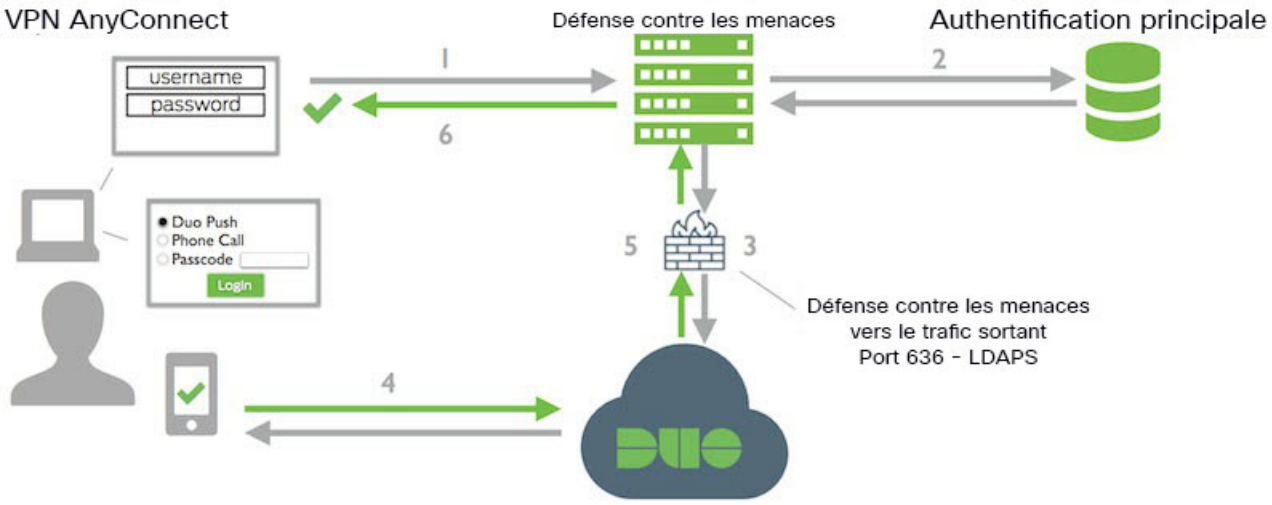
Comment configurer l'authentification à deux facteurs à l'aide de Duo LDAP

Vous pouvez utiliser le serveur LDAP Duo comme source d'authentification secondaire en conjonction avec un serveur Microsoft Active Directory (AD) ou RADIUS comme source principale. Avec Duo LDAP, l'authentification secondaire valide l'authentification principale avec un code d'accès Duo, une notification poussée ou un appel téléphonique.

Les rubriques suivantes expliquent la configuration plus en détail.

Flux système pour l'authentification secondaire Duo LDAP

Le graphique suivant montre comment le Cisco Firepower Threat Defense et Duo fonctionnent ensemble pour fournir une authentification à deux facteurs à l'aide de LDAP.



Voici une explication du flux système :

1. L'utilisateur établit une connexion VPN d'accès à distance avec le périphérique Cisco Firepower Threat Defense et fournit un nom d'utilisateur et un mot de passe.
2. FTD authentifie cette tentative d'authentification principale auprès du serveur d'authentification principal, qui peut être Active Directory ou RADIUS.
3. Si l'authentification principale réussit, le Cisco Firepower Threat Defense envoie une demande d'authentification secondaire au serveur Duo LDAP.
4. Duo authentifie ensuite l'utilisateur séparément, par notification poussée, message texte avec code d'accès ou appel téléphonique. L'utilisateur doit terminer cette authentification avec succès.
5. Duo répond au périphérique Cisco Firepower Threat Defense pour indiquer si l'utilisateur s'est authentifié avec succès.
6. Si l'authentification secondaire a réussi, le périphérique Cisco Firepower Threat Defense établit une connexion VPN d'accès à distance avec le client AnyConnect de l'utilisateur.

Configurer l'authentification secondaire Duo LDAP

La procédure suivante explique le processus de bout en bout de configuration de l'authentification à deux facteurs, en utilisant Duo LDAP comme source d'authentification secondaire, pour le VPN d'accès à distance. Notez que vous devez avoir un compte auprès de Duo et obtenir certaines informations auprès de Duo pour terminer cette configuration.

Procédure

Étape 1 Créez un compte Duo et obtenez la clé d'intégration, la clé secrète et le nom d'hôte API.

Voici un aperçu du processus. Pour en savoir plus, consultez le site Web de Duo, https://duo.com.

a) Inscrivez-vous pour un compte Duo.
b) Connectez-vous au Duo Admin Panel (panneau d'administration Duo) et accédez à **Applications**.

c) Cliquez sur **Protect an Application** (Protéger une application) et recherchez le VPN SSL de Cisco dans la liste des applications. Cliquez sur **Protect this Application** (Protéger cette application) pour obtenir votre clé d'intégration, votre clé secrète et votre nom d'hôte API. Pour obtenir de l'aide, consultez le *guide de démarrage* Duo, https://duo.com/docs/getting-started.

Étape 2 Créez une source d'identité LDAP Duo pour le serveur LDAP Duo.

Vous devez utiliser l'API Cisco Firepower Threat Defense pour créer l'objet LDAP Duo; vous ne pouvez pas le créer à l'aide de FDM. Vous pouvez soit utiliser API Explorer (Explorateur API), soit écrire votre propre application cliente pour créer l'objet. La procédure suivante explique comment créer l'objet à l'aide de API Explorer (Explorateur API).

a) Dans le FDM, cliquez sur le bouton des autres options (⋮) et choisissez **API Explorer** (Explorateur API.

Le système ouvre l'explorateur d'interface de protocole d'application dans un onglet ou une fenêtre distincte, en fonction des paramètres de votre navigateur.

b) (Facultatif) Obtenez les valeurs nécessaires pour identifier l'interface que le système doit utiliser pour se connecter au serveur LDAP Duo.

Si vous ne précisez pas d'interface, le système utilise la table de routage. Si nécessaire, vous pouvez créer une route statique pour le serveur Duo LDAP. Sinon, vous pouvez préciser l'interface à utiliser dans l'objet LDAP Duo. Si vous souhaitez préciser l'interface, utilisez les différentes méthodes GET dans le groupe Interfaces pour obtenir les valeurs nécessaires. Vous pouvez utiliser des interfaces physiques, de sous-interface, EtherChannel ou VLAN. Par exemple, pour obtenir les valeurs d'une interface physique, utilisez la méthode GET /devices/default/interfaces et recherchez l'objet correspondant à l'interface que vous devez utiliser. Vous avez besoin des valeurs suivantes de l'objet d'interface :

- ID
- type
- version
- name

c) Cliquez sur l'en-tête **DuoLDAPIdentitySource** pour ouvrir le groupe.
d) Cliquez sur la méthode **POST /object/duoldapidentitysources**.
e) Sous l'en-tête **Parameters** (Paramètres), pour l'élément **body** (corps, cliquez dans la zone d'affichage **Example Value** (Valeur d'exemple) dans la colonne **Data Type** (Type de données) à droite. Cette action charge l'exemple dans la zone d'édition de la valeur du corps.
f) Dans la zone d'édition de la **valeur du corps**, procédez comme suit :

- Supprimez les lignes d'attributs suivantes : **version**, **id**. (Ces attributs sont nécessaires pour les appels PUT, mais pas pour POST.)
- Pour **name**, saisissez un nom pour l'objet, tel que Duo-LDAP-server.
- Pour **description**, saisissez une description significative de l'objet à des fins de référence ou supprimez la ligne d'attribut.
- Pour **apiHostname**, saisissez le nom d'hôte API que vous avez obtenu de votre compte Duo. Le nom d'hôte doit ressembler à ce qui suit, en remplaçant toutefois les X par votre valeur unique : API-XXXXXXXX.DUOSECURITY.COM. Les majuscules ne sont pas obligatoires.

- Pour **port**, saisissez le port TCP à utiliser pour LDAPS. Il doit s'agir du port 636, à moins que Duo ne vous ait demandé d'utiliser un autre port. Notez que vous devez vous assurer que votre liste de contrôle d'accès autorise le trafic vers le serveur Duo LDAP par l'intermédiaire de ce port.
- Pour **timeout**, saisissez le délai d'expiration, en secondes, pour la connexion au serveur Duo. La valeur peut être comprise entre 1 et 300 secondes. La valeur par défaut est de 120 secondes. Pour utiliser la valeur par défaut, saisissez 120 ou supprimez la ligne d'attribut.
- Pour **integrationKey**, saisissez la clé d'intégration que vous avez obtenue de votre compte Duo.
- Pour **secretKey**, saisissez la clé secrète que vous avez obtenue de votre compte Duo. Cette clé sera ensuite masquée.
- Pour **interface**, saisissez les valeurs id, type, version et name de l'interface à utiliser pour la connexion au serveur Duo LDAP ou supprimez les 6 lignes utilisées pour définir l'attribut d'interface, y compris l'accolade de fermeture.
- Pour **type**, laissez la valeur duoldapidentitysource.

Par exemple, le corps de l'objet peut ressembler à ce qui suit, où apiHostname et integrationKey sont masqués, mais la clé secrète falsifiée intentionnellement est affichée :

```
{
  "name": "Duo-LDAP-server",
  "description": "Duo LDAP server for RA VPN",
  "apiHostname": "API-XXXXXXXX.DUOSECURITY.COM",
  "port": 636,
  "timeout": 120,
  "integrationKey": "XXXXXXXXXXXXXXXXXXXX",
  "secretKey": "123456789",
  "type": "duoldapidentitysource"
}
```

g) Cliquez sur le bouton **Try It Out!** (Essayez-le !).

Le système émettra la commande **curl** pour publier l'objet dans la configuration du périphérique. Vous verrez la commande curl, le corps de la réponse et le code de réponse. Si vous avez créé un corps valide, vous devriez voir **200** dans le champ **Response Code** (Code de réponse).

Si vous avez fait une erreur, consultez le corps de la réponse pour obtenir un message d'erreur. Vous pouvez corriger la valeur du corps et réessayer.

h) Revenez à FDM en cliquant sur **Device** (Périphérique) dans le menu supérieur.

i) Cliquez sur **Objects** (Objets), puis sur **Identity Sources** (Sources d'identité) dans la table des matières.

Votre objet Duo LDAP devrait apparaître dans la liste. Si ce n'est pas le cas, retournez à API Explorer (Explorateur API) et essayez de créer l'objet de nouveau. Vous pouvez utiliser la méthode GET pour vérifier s'il a bien été créé.

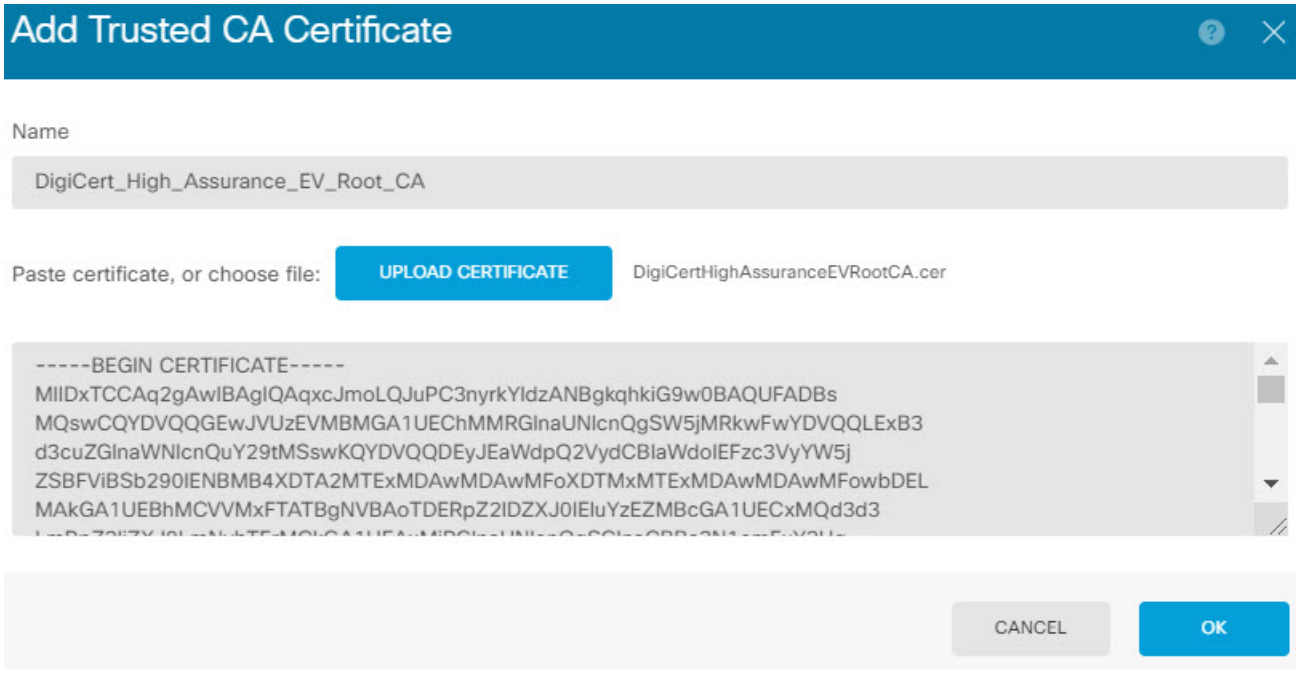
Notez que vous pouvez supprimer l'objet à l'aide de FDM, mais que vous ne pouvez pas le modifier ou voir son contenu. Vous devez utiliser l'API pour ces actions. Les méthodes pertinentes sont affichées dans le groupe **DuoLDAPIdentitySource**.

Étape 3 Chargez le certificat d'autorité de certification approuvé pour le site Web Duo dans FDM.

Le système FTD doit disposer du certificat nécessaire pour valider la connexion au serveur Duo LDAP. Vous pouvez obtenir et charger le certificat en suivant cette procédure, qui a été effectuée avec le navigateur Google Chrome. Les étapes exactes peuvent varier selon votre navigateur. Vous pouvez également accéder directement

à https://www.digicert.com/digicert-root-certificates.htm et télécharger le certificat, mais la procédure suivante est générique et vous pouvez l'utiliser pour obtenir des certificats d'autorité de certification racine approuvés pour n'importe quel site.

a) Ouvrez https://duo.com dans votre navigateur.
b) Cliquez sur le lien d'information du site dans le champ URL du navigateur, puis sur le lien **Certificate** (Certificat). Cette action ouvre la boîte de dialogue d'informations sur le certificat.
c) Cliquez sur l'onglet **Certificate Path** (Chemin du certificat) et sélectionnez le niveau racine (supérieur) du chemin. Dans ce cas, DigiCert.
d) Une fois DigiCert sélectionné, cliquez sur **Afficher le certificat**. Cette action ouvrira une nouvelle boîte de dialogue de certificat, et l'onglet Général devrait indiquer qu'il a été émis pour l'autorité de certification racine EV de DigiCert High Assurance. Il s'agit du certificat de l'autorité de certification racine que vous devez charger dans FDM.
e) Cliquez sur l'onglet **Details** (Détails), puis sur le bouton **Copy to File** (Copier dans un fichier) pour lancer l'assistant de téléchargement de certificat.
f) Utilisez l'assistant pour télécharger le certificat sur votre poste de travail. Téléchargez au format DER par défaut.
g) Dans la liste FDM, choisissez **Objects** > **(Objets)** > **Certificates** (Certificats) .
h) Cliquez sur **+** > **Add Trusted CA Certificate** (Ajouter un certificat d'autorité de certification de confiance).
i) Saisissez un nom pour le certificat, par exemple, DigiCert_High_Assurance_EV_Root_CA. (Les espaces ne sont pas autorisés.)
j) Cliquez sur **Upload Certificate** (Charger le certificat) et sélectionnez le fichier que vous avez téléchargé.



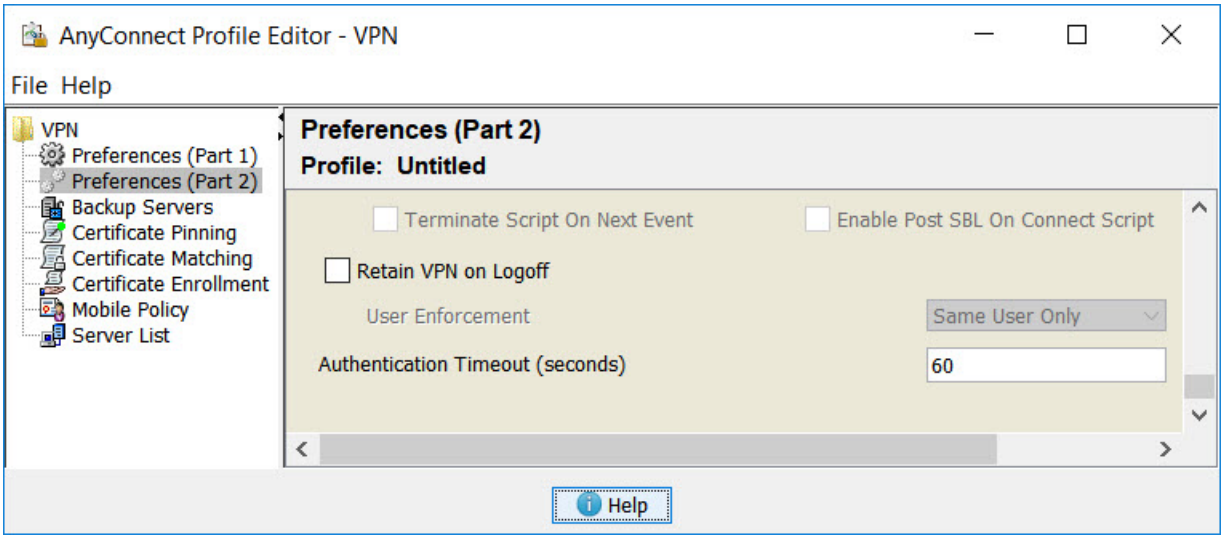
k) Cliquez sur **OK**.

Étape 4 Utilisez l'éditeur de profil client AnyConnect pour créer un profil qui spécifie 60 secondes ou plus pour le délai d'authentification.

Vous devez accorder aux utilisateurs un délai supplémentaire pour obtenir le code d'accès Duo et effectuer l'authentification secondaire. Nous recommandons au moins 60 secondes.

Pour en savoir plus sur la création de profils client AnyConnect et leur téléchargement, consultez Configurer et charger les profils client AnyConnect, à la page 11. La procédure suivante explique comment configurer le délai d'authentification uniquement, puis charger le profil dans FTD. Si vous souhaitez modifier d'autres paramètres, vous pouvez le faire maintenant.

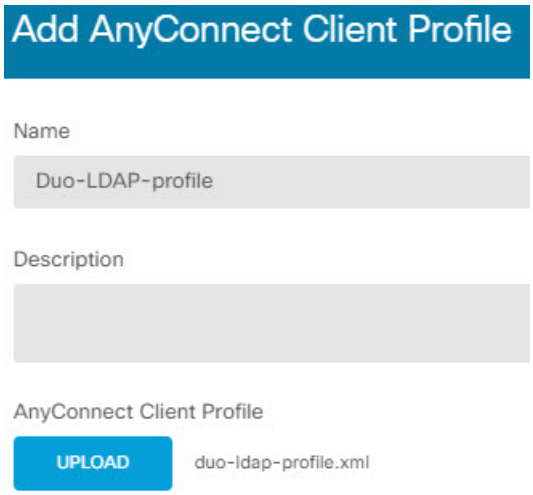
a) Si vous ne l'avez pas encore fait, téléchargez et installez le progiciel de l'éditeur de profil client AnyConnect. Vous pouvez le trouver dans le centre de logiciels Cisco (software.cisco.com), dans le dossier correspondant à votre version client AnyConnect.
b) Ouvrez le **VPN Profile Editor (Éditeur de profil VPN)** client AnyConnect.
c) Sélectionnez **Preferences (Part 2)** (Préférences (Partie 2)) dans la table des matières, faites défiler jusqu'à la fin de la page et modifiez **Authentication Timeout** (Délai d'authentification) à 60 (ou plus). L'image suivante provient de l'éditeur de profil VPN AnyConnect 4.7 ; les versions précédentes ou ultérieures peuvent être différentes.



d) Choisissez **File (Fichier)** > **Save (Enregistrer)**, puis enregistrez le fichier XML de profil sur votre poste de travail avec un nom approprié, par exemple « duo-ldap-profile.xml ».

   Vous pouvez maintenant fermer l'application de l'éditeur de profil VPN.

e) Dans FDM, choisissez **Objects (Objets)** > **AnyConnect Client Profiles (Profils client AnyConnect)**.
f) Cliquez sur **+** pour créer un nouvel objet de profil.
g) Saisissez un **Name** (Nom) pour l'objet. Par exemple, Duo-LDAP-profile.
h) Cliquez sur **Upload** (Charger), et sélectionnez le fichier XML que vous avez créé.



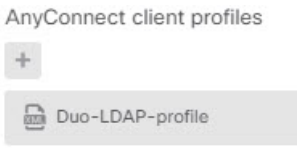
i) Cliquez sur **OK**.

Étape 5 Créez une politique de groupe et sélectionnez le profil client AnyConnect dans la politique.

La politique de groupe que vous affectez à un utilisateur contrôle de nombreux aspects de la connexion. La procédure suivante explique comment affecter le fichier XML de profil au groupe. Pour plus de détails sur ce que vous pouvez faire avec les politiques de groupe, consultez Configurer les politiques de groupe pour le VPN d'accès à distance, à la page 25.

a) Cliquez sur **View Configuration** (Afficher la configuration) dans **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance)**.
b) Choisissez **Group Policies** (Politiques de groupe) dans la table des matières.
c) Modifiez DfltGrpPolicy, ou cliquez sur **+** et créez une nouvelle politique de groupe. Par exemple, si vous avez besoin d'un profil de connexion VPN d'accès à distance unique pour tous les utilisateurs, la modification de la politique de groupe par défaut est appropriée.
d) Sur la page General (Général), configurez les propriétés suivantes :

- **Name** (Nom) : pour un nouveau profil, saisissez un nom. Par exemple, Duo-LDAP-group.
- **AnyConnect Client Profiles (Profils client AnyConnect)** : cliquez sur **+** et sélectionnez l'objet de profil client AnyConnect que vous avez créé.



e) Cliquez sur **OK** pour enregistrer le profil de groupe.

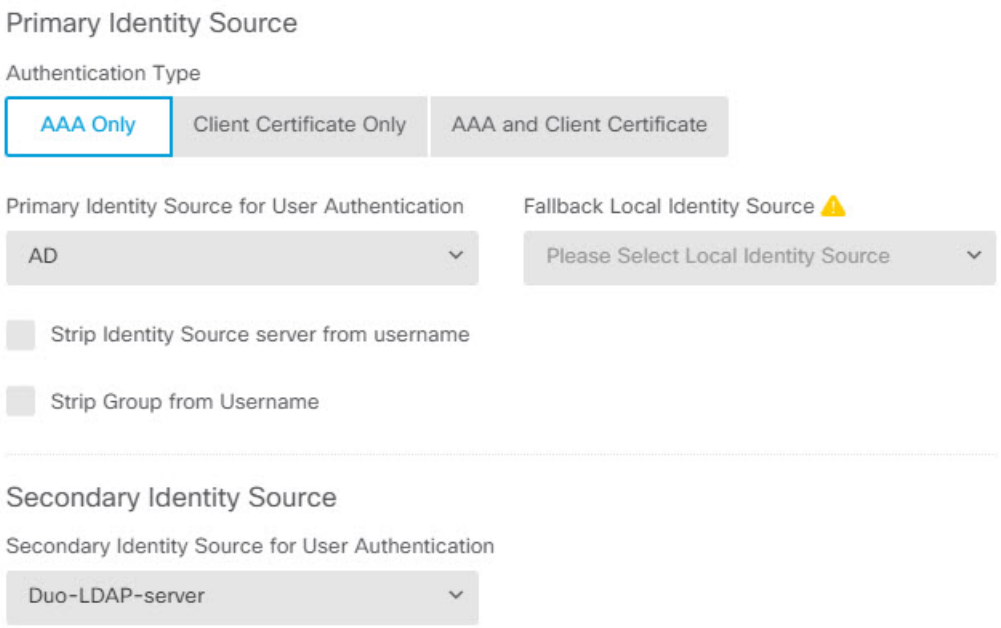
Étape 6 Créez ou modifiez le profil de connexion VPN d'accès à distance à utiliser pour l'authentification secondaire Duo-LDAP.

Il y a plusieurs étapes à suivre pour configurer un profil de connexion, qui sont expliquées dans Configurer un profil de connexion VPN d'accès à distance, à la page 16. La procédure suivante ne mentionne que les modifications clés à apporter pour activer Duo-LDAP comme source d'authentification secondaire et pour appliquer le profil client AnyConnect. Pour les nouveaux profils de connexion, vous devez configurer le reste

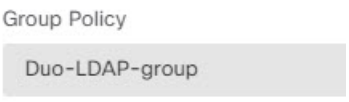
des champs obligatoires. Pour cette procédure, nous supposons que vous modifiez un profil de connexion existant, et vous devez simplement modifier ces deux paramètres.

a) Sur la page RA VPN (VPN d'accès à distance), choisissez **Connection Profiles (Profils de connexion)** dans la table des matières.
b) Modifiez un profil de connexion existant ou créez-en un nouveau.
c) Sous Primary Identity Source (Source d'identité principale), configurez les éléments suivants :

- **Authentication Type** (Type d'authentification) : choisissez **AAA Only** (AAA uniquement) ou **AAA and Client Certificate** (AAA et certificat client). Vous ne pouvez pas configurer l'authentification à deux facteurs, sauf si vous utilisez AAA.
- **Primary Identity Source for User Authentication** (Source d'identité principale pour l'authentification des utilisateurs) : sélectionnez votre serveur Active Directory ou RADIUS principal. Notez que vous pouvez sélectionner une source d'identité Duo-LDAP comme source principale. Cependant, Duo-LDAP fournit des services d'authentification uniquement, et non des services d'identité, donc si vous l'utilisez comme source d'authentification principale, vous ne verrez pas les noms d'utilisateur associés aux connexions VPN d'accès à distance dans les tableaux de bord, et vous ne pourrez pas écrire de règles de contrôle d'accès pour ces utilisateurs. (Vous pouvez configurer le retour à la source d'identité locale si vous le souhaitez.)
- **Secondary Identity Source** (Source d'identité secondaire) : sélectionnez la source d'identité Duo-LDAP.



d) Cliquez sur **Next** (suivant).
e) Sur la page Remote User Experience (Expérience de l'utilisateur à distance), sélectionnez la **Group Policy** (Politique de groupe) que vous avez créée ou modifiée.



f) Cliquez sur **Next (Suivant)** sur cette page et sur la page suivante, Global Settings (Paramètres globaux).
g) Cliquez sur **Finish** (Terminer) pour enregistrer vos modifications du profil de connexion.

Étape 7 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.

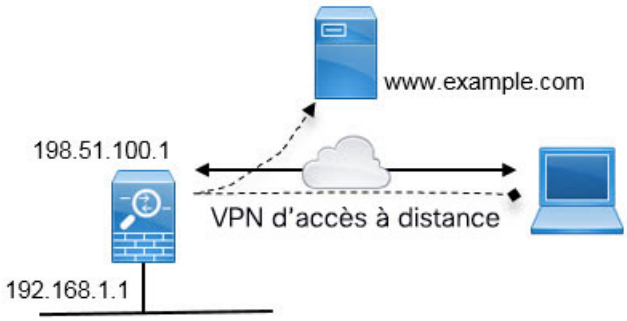
b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

Comment fournir un accès Internet sur l'interface externe pour les utilisateurs du VPN d'accès à distance (Hair Pinning)

En règle générale, dans le VPN d'accès à distance, vous pouvez souhaiter que les utilisateurs du VPN accèdent à Internet par l'intermédiaire de votre périphérique. Cependant, comme les utilisateurs distants accèdent à votre périphérique sur la même interface qui fait face à Internet (l'interface externe), vous devez faire revenir le trafic Internet directement sur l'interface externe. Cette technique est appelée hairpinning.

Le graphique suivant présente un exemple. Un VPN d'accès à distance est configuré sur l'interface externe, 198.51.100.1. Vous souhaitez fractionner le tunnel VPN de l'utilisateur distant, de sorte que le trafic Internet soit renvoyé par l'interface externe, tandis que le trafic vers vos réseaux internes continue par le périphérique. Ainsi, lorsqu'un utilisateur distant souhaite accéder à un serveur sur Internet, comme par exemple www.exemple.com, la connexion passe d'abord par le VPN, puis est acheminée vers l'Internet à partir de l'interface 198.51.100.1.



La procédure suivante explique comment configurer ce service.

Avant de commencer

Cet exemple suppose que vous avez déjà enregistré le périphérique, appliqué une licence VPN d'accès à distance et téléchargé l'image client AnyConnect. Il suppose également que vous ayez configuré le domaine d'identité, qui est également utilisé dans les politiques d'identité.

Procédure

Étape 1 Configurez la connexion VPN d'accès à distance.

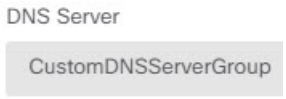
La configuration nécessite une politique de groupe personnalisée en plus du profil de connexion. Étant donné que le hairpinning est une configuration courante et que les paramètres requis dans la politique de groupe sont généralement applicables, dans cet exemple, nous modifierons la politique de groupe par défaut au lieu de créer une nouvelle politique de groupe. Vous pouvez adopter l'une ou l'autre des approches.

a) Cliquez sur **View Configuration** (Afficher la configuration) dans le groupe **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance**.

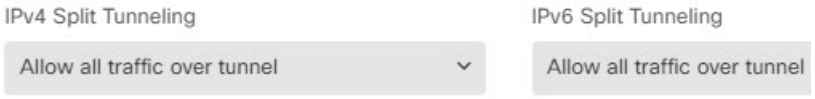
b) Cliquez sur **Group Policies** (Politiques de groupe) dans la table des matières, puis sur l'icône de modification () de l'objet DfltGrpPolicy.

c) Apportez les modifications suivantes à la politique de groupe par défaut :

- Sur la page **General** (Général), dans **DNS Server** (Serveur DNS), sélectionnez le groupe de serveurs DNS qui définit les serveurs que les points d'extrémité VPN doivent utiliser pour résoudre les noms de domaine.



- Sur la page **Split Tunneling** (Tunnellisation fractionnée), pour **IPv4 Split Tunneling** (Tunnellisation fractionnée IPv4) et **IPv6 Split Tunneling** (Tunnellisation fractionnée IPv6), sélectionnez l'option **Allow all traffic over tunnel** (Autoriser tout le trafic sur le tunnel). Il s'agit du paramètre par défaut, il est donc peut-être déjà configuré correctement.



Remarque
Il s'agit d'un paramètre critique pour activer le hair-pinning. Vous souhaitez que tout le trafic atteigne la passerelle VPN, alors que la tunnellisation fractionnée est un moyen de permettre aux clients distants d'accéder directement aux sites locaux ou Internet en dehors du VPN.

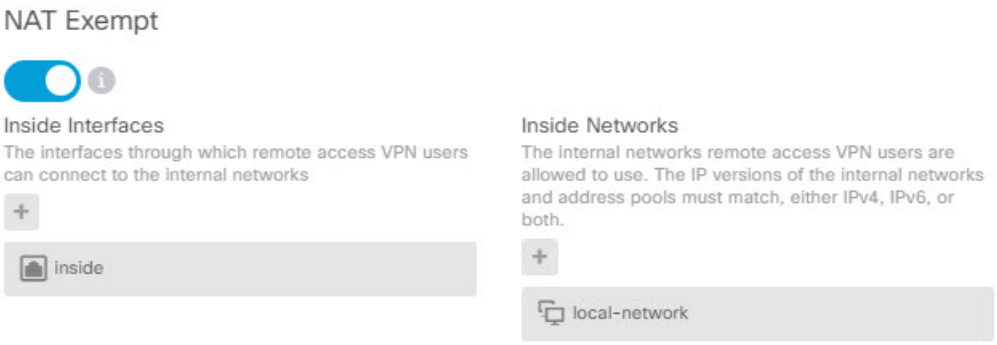
d) Cliquez sur **OK** pour enregistrer les modifications apportées à la politique de groupe par défaut.

e) Cliquez sur **Connection Profiles** (Profils de connexion) et modifiez un profil existant ou créez-en un nouveau.

f) Dans le profil de connexion, parcourez l'assistant et configurez toutes les options comme vous le feriez pour toute autre configuration de VPN d'accès à distance. Cependant, vous devez configurer correctement les options suivantes pour activer le hair-pinning :

- **Group Policy** (Politique de groupe), à l'étape 2. Sélectionnez la politique de groupe que vous avez personnalisée pour le hairpinning.

- **NAT Exempt (Exemption de NAT)**, à l'étape 3. Activez cette fonctionnalité. Sélectionnez l'interface interne, puis sélectionnez un objet réseau qui définit les réseaux internes. Dans cet exemple, l'objet doit préciser 192.168.1.0/24. Le trafic du VPN d'accès à distance (RA) vers le réseau interne ne fera pas l'objet d'une traduction d'adresses. Cependant, comme le trafic hair-pinned passe par l'interface externe, il sera toujours transmis à l'aide de la NAT, car l'exemption NAT s'applique uniquement à l'interface interne. Notez que si d'autres profils de connexion sont définis, vous devez ajouter aux paramètres existants, car la configuration s'applique à tous les profils de connexion.



Remarque
L'option **NAT Exempt** (Exemption de NAT) est l'autre paramètre critique pour la configuration de hairpinning.

g) (Facultatif) Dans l'étape **Global Settings** (Paramètres globaux), sélectionnez l'option **Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)** (Contourner la stratégie de contrôle d'accès pour le trafic déchiffré).

En sélectionnant cette option, vous n'avez plus besoin de configurer des règles de contrôle d'accès pour autoriser le trafic provenant des adresses du pool du VPN d'accès à distance (RA). Cette option améliore la sécurité (les utilisateurs externes ne peuvent pas usurper les adresses du pool), mais elle signifie que le trafic du VPN d'accès à distance (RA) est exempt d'inspection, y compris le filtrage d'URL et la protection contre les intrusions. Pesez le pour et le contre avant de choisir cette option.

h) Passez en revue la configuration du VPN d'accès à distance, puis cliquez sur **Finish** (Terminer).

Étape 2 Configurez la règle NAT pour traduire toutes les connexions sortant de l'interface externe en ports sur l'adresse IP externe (PAT de l'interface).

Lorsque vous avez terminé la configuration initiale du périphérique, le système crée une règle NAT nommée InsideOutsideNatRule. Cette règle applique la PAT d'interface au trafic IPv4 de toute interface qui quitte le périphérique par l'intermédiaire de l'interface externe. Comme l'interface externe est incluse dans l'interface source « Any », la règle dont vous avez besoin existe déjà, sauf si vous l'avez modifiée ou supprimée.

La procédure suivante explique comment créer la règle dont vous avez besoin.

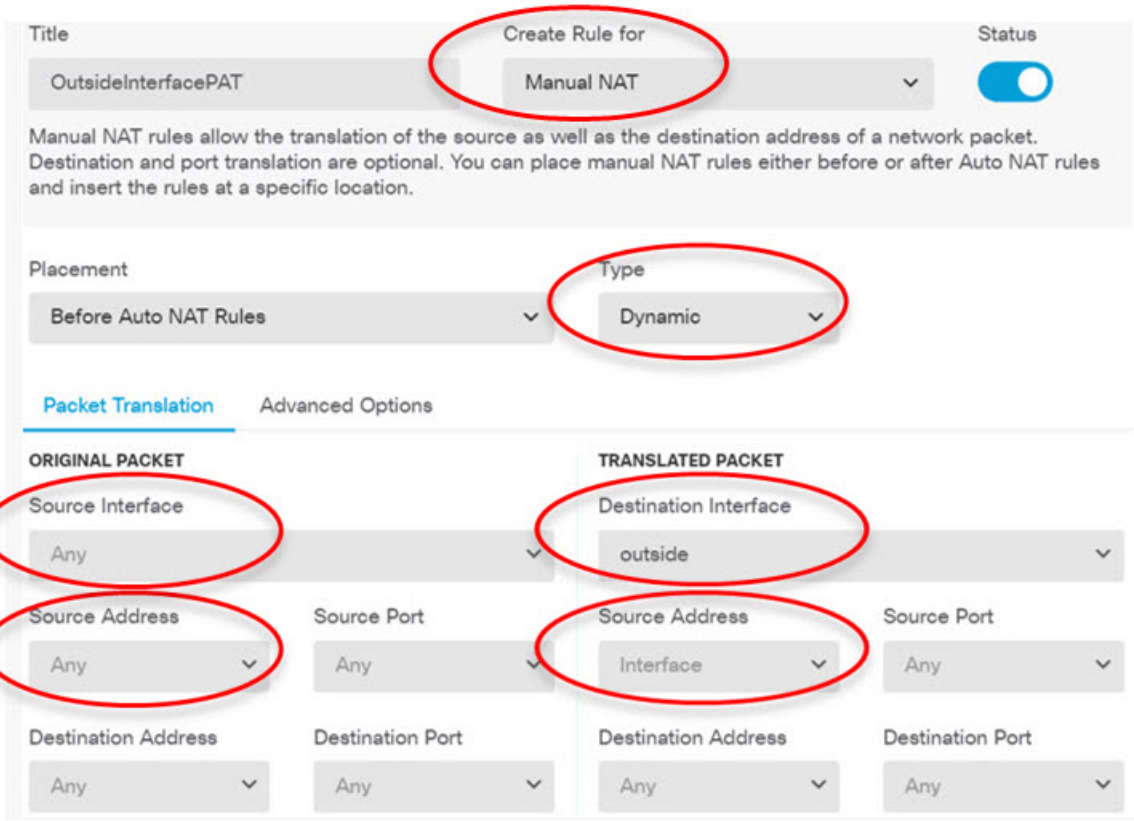
a) Cliquez sur **Policies (Politiques)** > **NAT**.
b) Effectuez l'une des opérations suivantes :

- Pour modifier la règle InsideOutsideNatRule, passez le curseur sur la colonne **Action** et cliquez sur l'icône de modification ( ).
- Pour créer une nouvelle règle, cliquez sur le bouton **+**.

c) Configurez une règle avec les propriétés suivantes :

- **Title** (Titre) : pour une nouvelle règle, saisissez un nom significatif, sans espaces. Par exemple, OutsideInterfacePAT.
- **Create Rule For** (Créer une règle pour) : **Manual NAT** (NAT manuelle).
- **Placement** : **Before Auto NAT Rules (Avant les règles de NAT automatique)** (valeur par défaut).
- **Type** :**Dynamic** (Dynamique).
- **Original Packet** (Paquet d'origine) : pour **Source Address** (Adresse source), sélectionnez Any (tout) ou any-ipv4. Pour **Source Interface** (Interface source), veillez à sélectionner Any (tout) (qui est la valeur par défaut). Pour toutes les autres options de Original Packet (Paquet d'origine), conservez la valeur par défaut, Any (tout).
- **Translated Packet** (Paquet traduit) : pour **Destination Interface** (Interface de destination), sélectionnez externe. Pour **Translated Address** (Adresse traduite), sélectionnez **Interface**. Pour toutes les autres options de Translated Packet (Paquet traduit), conservez la valeur par défaut, Any (tout).

Le graphique suivant montre le cas simple où vous sélectionnez Any (tout) pour l'adresse source.



d) Cliquez sur **OK**.

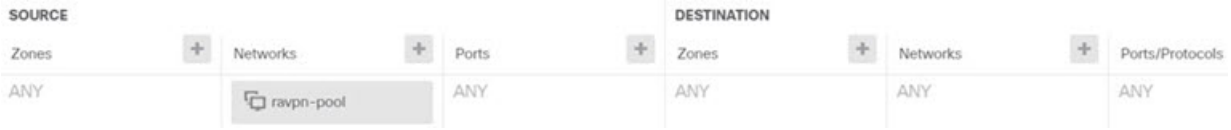
Étape 3 (Si vous ne configurez pas **Bypass Access Control policy for decrypted traffic** (sysopt permit-vpn) (stratégie de contrôle d'accès de contournement pour le trafic déchiffré) dans le profil de connexion.) Créez des règles de contrôle d'accès pour autoriser l'accès à partir de l'ensemble d'adresses VPN d'accès à distance.

Si vous sélectionnez **Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)** (stratégie de contrôle d'accès de contournement pour le trafic déchiffré) dans le profil de connexion, le trafic de l'ensemble d'adresses du VPN d'accès à distance contourne la stratégie de contrôle d'accès. Vous ne pouvez pas écrire de règles de contrôle d'accès qui s'appliqueront au trafic. Vous devez écrire les règles uniquement si vous désactivez l'option.

L'exemple suivant permet le trafic de l'ensemble d'adresses vers n'importe quelle destination. Vous pouvez l'ajuster selon vos besoins précis. Vous pouvez également faire précéder la règle de règles de blocage pour filtrer le trafic indésirable.

a) Cliquez sur **Policies (Politiques)** > **Access Control (Contrôle d'accès)**.
b) Cliquez sur **+** pour créer une nouvelle règle.
c) Configurez une règle avec les propriétés suivantes :

- **Order** (Ordre) : sélectionnez une position dans la politique avant toute autre règle qui pourrait correspondre à ces connexions et les bloquer. La valeur par défaut consiste à ajouter la règle à la fin de la politique. Si vous devez repositionner la règle ultérieurement, vous pouvez modifier cette option ou simplement faire glisser et déposer la règle dans le bon emplacement dans le tableau.
- **Titre** : saisissez un nom significatif sans espaces. Par exemple, RAVPN-address-pool.
- **Action** : **Autoriser**. Vous pouvez sélectionner Trust (Confiance) si vous ne souhaitez pas que ce trafic soit inspecté pour détecter des violations de protocole ou des intrusions.
- Onglet **Source/Destination** : pour **Source** > **Network (Réseau)**, sélectionnez le même objet que vous avez utilisé dans le profil de connexion VPN d'accès à distance pour l'ensemble d'adresses. Laissez la valeur par défaut, Any (Tout), pour toutes les autres options de source et de destination.



- Onglets **Application**, **URL** et **Users** (Utilisateurs) : laissez les paramètres par défaut sur ces onglets, c'est-à-dire qu'aucune option n'est sélectionnée.
- Onglets **Intrusion**, **File** (Fichiers) : vous pouvez, au besoin, sélectionner des politiques de prévention des intrusions ou des politiques de fichiers afin d'inspecter les menaces ou les logiciels malveillants.
- Onglet **Logging (journalisation)** : vous pouvez éventuellement activer la journalisation des connexions.

d) Cliquez sur **OK**.

Étape 4 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.

b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

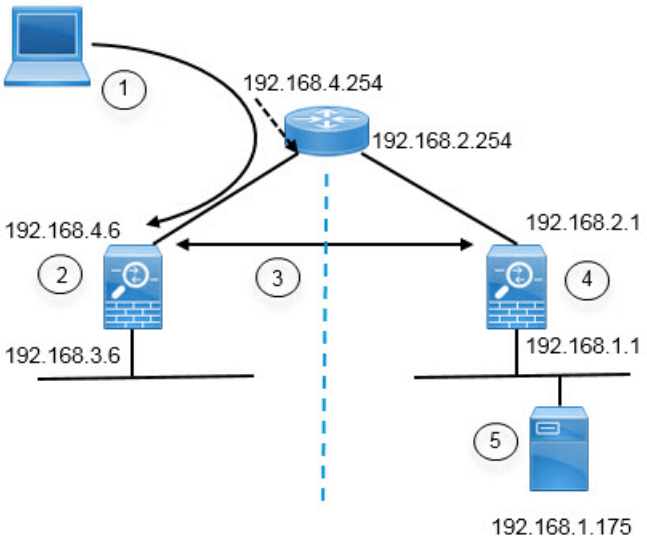
Comment utiliser un serveur de répertoire sur un réseau externe avec le VPN d'accès à distance

Vous pouvez configurer un VPN d'accès à distance pour permettre aux télétravailleurs et aux télétravailleurs de se connecter en toute sécurité à vos réseaux internes. La sécurité de la connexion dépend de votre serveur de répertoire, qui authentifie la connexion de l'utilisateur pour s'assurer que seuls les utilisateurs autorisés peuvent obtenir l'entrée.

Si votre serveur de répertoire se trouve sur un réseau externe plutôt que sur un réseau interne, vous devez configurer une connexion VPN de site à site à partir de l'interface externe vers le réseau qui comprend le serveur de répertoire. **Il existe une optimisation de la configuration VPN de site à site :** vous devez inclure l'adresse de l'interface externe du périphérique VPN d'accès à distance dans les réseaux « internes » de la connexion VPN de site à site, ainsi que dans les réseaux distants pour le périphérique derrière lequel se trouve le serveur de répertoire. Cela sera expliqué plus en détail dans la procédure suivante.

Remarque Si vous utilisez les interfaces de données comme passerelle pour l'interface de gestion virtuelle, cette configuration permet également l'utilisation du répertoire pour les politiques d'identité. Si vous n'utilisez pas d'interfaces de données comme passerelle de gestion, assurez-vous qu'il existe une voie de routage entre le réseau de gestion et le réseau interne qui participe à la connexion VPN de site à site.

Ce scénario d'utilisation met en œuvre le scénario réseau suivant.



Appel de la figure	Description
1	Hôte d'accès à distance qui établit une connexion VPN avec l'adresse 192.168.4.6. Les clients obtiendront une adresse dans l'ensemble d'adresses 172.18.1.0/24.

Appel de la figure	Description
2	Le site A, qui héberge le VPN d'accès à distance.
3	Le tunnel VPN de site à site entre les interfaces externes du site A et du site B, pour les périphériques Cisco Firepower Threat Defense.
4	Le site B, qui héberge le serveur de répertoire.
5	Le serveur de répertoire, sur le réseau interne du site B.

Avant de commencer

Ce scénario suppose que vous ayez suivi l'assistant de configuration du périphérique pour établir une configuration de référence normale. Plus précisément :

- Il existe une règle de contrôle d'accès Inside_Outside_Rule qui autorise (ou fait confiance) le trafic passant de la zone interne à la zone externe.
- Les zones de sécurité inside_zone et outside_zone contiennent respectivement les interfaces interne et externe.
- Il existe une règle InsideOutsideNATRule qui effectue une PAT d'interface pour tout le trafic provenant des interfaces internes vers l'interface externe. Sur les périphériques qui utilisent un groupe de ponts internes par défaut, il peut y avoir plusieurs règles pour la PAT de l'interface.
- Il existe une route IPv4 statique pour 0.0.0.0/0 qui pointe vers l'interface externe. Cet exemple suppose que vous utilisez des adresses IP statiques pour les interfaces externes, mais vous pouvez également utiliser DHCP et obtenir la route statique de manière dynamique. Pour cet exemple, nous supposons les routes statiques suivantes :
  - Site A : interface externe, la passerelle est 192.168.4.254.
  - Site B : interface externe, la passerelle est 192.168.2.254.

Procédure

Étape 1 Configurez la connexion VPN de site à site sur **le site B**, qui héberge le serveur de répertoire.

a) Cliquez sur **Device** (Périphérique), puis sur **View Configuration** (Afficher la configuration) dans le groupe VPN de site à site.

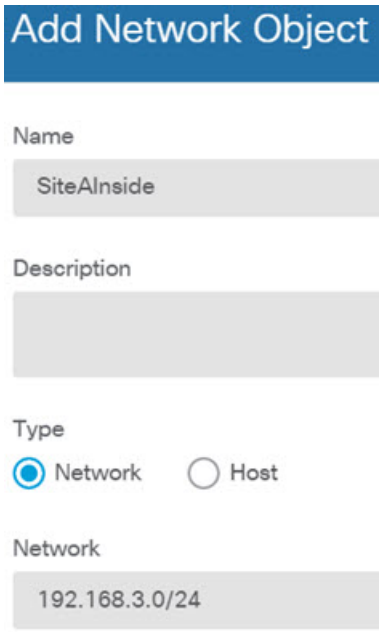
b) Cliquez sur le bouton **+**.

c) Configurez les options suivantes pour **Endpoint Setting**s (Paramètres de point terminal).

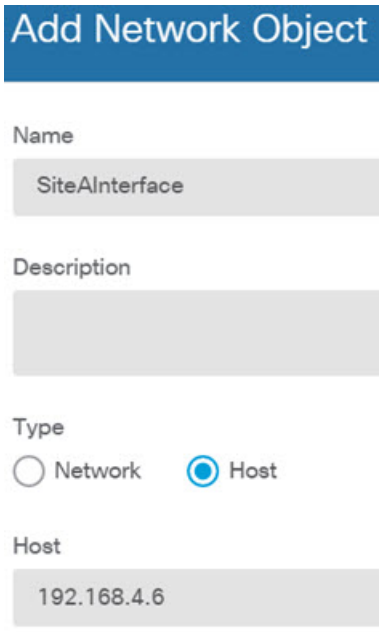
- **Connection Profile Name** (Nom du profil de connexion) : saisissez un nom, par exemple, Site A (pour indiquer que la connexion se fait au site A).
- **Local Site** (site local) : ces options définissent le point terminal local.
  - **Local VPN Access Interface** (Interface d'accès VPN local) : sélectionnez l'interface **externe** (celle dont l'adresse 192.168.2.1 dans le diagramme).
  - **Local Network** (Réseau local) : cliquez sur le signe plus **+** et sélectionnez l'objet réseau qui identifie le réseau local qui doit faire partie de la connexion VPN. Comme le serveur de

répertoire se trouve sur ce réseau, il peut participer au VPN de site à site. En supposant que l'objet n'existe pas déjà, cliquez sur **Create New Network** (Créer un nouveau réseau) et configurez un objet pour le réseau 192.168.1.0/24. Après avoir enregistré l'objet, sélectionnez-le dans la liste déroulante et cliquez sur **OK**.

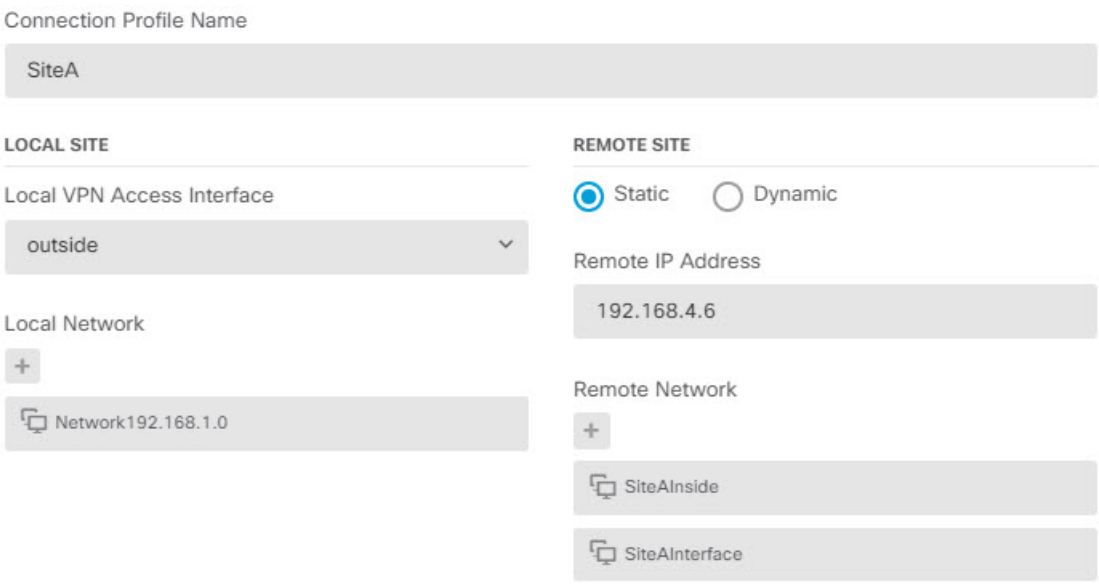
- **Remote Site** (Site distant) : ces options définissent le terminal distant.
  - **Remote IP Address** (Adresse IP distante) : saisissez 192.168.4.6, qui correspond à l'adresse IP de l'interface de l'homologue VPN distant qui hébergera la connexion VPN.
  - **Remote Networ**k (Réseau distant) : cliquez sur signe plus + et sélectionnez les objets réseau qui identifient les réseaux distants devant participer à la connexion VPN. Cliquez sur **Create New Network** (Créer un nouveau réseau), configurez les objets suivants, puis sélectionnez-les dans la liste.
    1. SiteAInside, réseau, 192.168.3.0/24.



2. SiteAInterface, hôte, 192.168.4.6. **Il s'agit de la clé : vous devez inclure l'adresse du point de connexion VPN d'accès à distance dans le cadre du réseau distant pour la connexion VPN de site à site afin que le VPN d'accès à distance hébergé sur cette interface puisse utiliser le serveur de répertoire.**



Lorsque vous avez terminé, les paramètres du terminal devraient ressembler à ce qui suit :



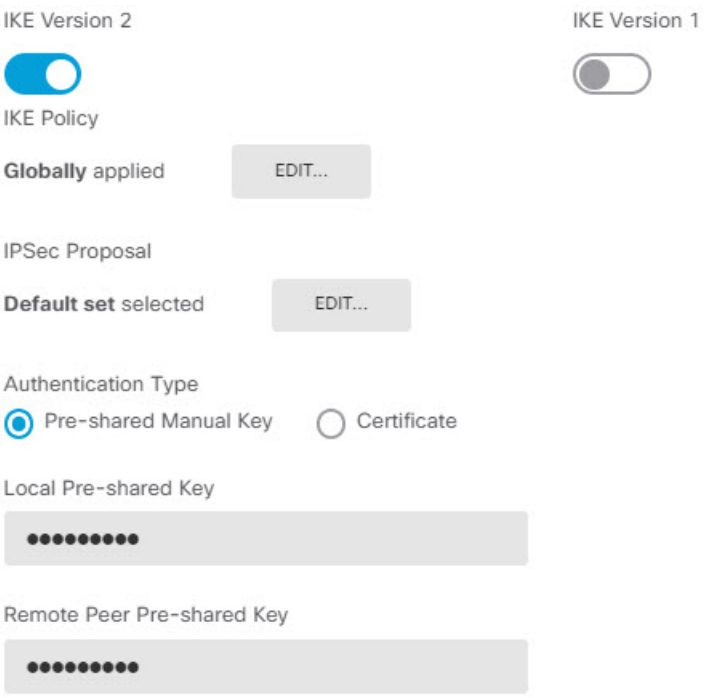
d) Cliquez sur **Next** (suivant).

e) Définissez la configuration de confidentialité pour le VPN.

Dans ce cas d'utilisation, nous supposons que vous êtes admissible aux fonctionnalités soumises à des restrictions d'exportation, ce qui permet l'utilisation d'un chiffrement renforcé. Ajustez ces exemples de paramètres en fonction de vos besoins et des exigences de votre licence.

- **IKE version 2**, **IKE version 1** : conservez les valeurs par défaut, **IKE version 2** activée, **IKE version 1** désactivée.
- **IKE Policy** (Politique IKE) : cliquez sur **Edit** (Modifier) et activez **AES-GCM-NULL-SHA** et **AES-SHA-SHA**, et désactivez **DES-SHA-SHA**.
- **IPsec Proposal** (Proposition IPsec) : cliquez sur **Edit** (Modifier). Dans la boîte de dialogue Select IPSec Proposals (Sélectionner les propositions IPSec), cliquez sur le signe **+**, puis cliquez sur **Set Default** (Définir par défaut) pour choisir les propositions AES-GCM par défaut.
- **Local Preshared Key** (Clé prépartagée locale), **Remote Peer Preshared Key** (Clé prépartagée de l'homologue distant) : saisissez les clés définies sur ce périphérique et sur le périphérique distant pour la connexion VPN. Ces clés peuvent être différentes dans IKEv2. La clé peut comporter entre 1 et 127 caractères alphanumériques. **N'oubliez pas ces clés, car vous devez configurer les mêmes chaînes lors de la création de la connexion VPN de site à site sur le périphérique du site A.**

La politique IKE doit ressembler à ce qui suit :



f) Configurez les **options supplémentaires**.

- **NAT Exempt** (Exemption NAT : sélectionnez l'interface qui héberge le réseau interne, dans cet exemple, l'interface **interne**. En règle générale, vous ne souhaitez pas que le trafic dans un tunnel VPN de site à site voie les adresses IP traduites. Cette option ne fonctionne que si le réseau local se trouve derrière une interface de routage unique (et non un membre d'un groupe de ponts). Si le réseau local se trouve derrière plusieurs interfaces de routage ou un ou plusieurs membres de groupes de ponts, vous devez créer manuellement les règles d'exemption de NAT. Pour plus d'informations sur la création manuelle des règles requises, consultez Exemption du trafic VPN de site à site de la NAT.
- **Diffie-Hellman Group for Perfect Forward Secrecy (Groupe Diffie-Hellman pour la confidentialité de transmission** parfaite) : sélectionnez **Group 19** (Groupe 19). Cette option détermine si l'on utilise la confidentialité de transmission parfaite (PFS) pour générer et utiliser une clé de session unique pour chaque échange chiffré. La clé de session unique protège l'échange du déchiffrement ultérieur, même si l'échange en entier a été enregistré et que l'agresseur a obtenu les clés prépartagées ou privées utilisées par les terminaux. Pour obtenir une explication des options, consultez Choix du groupe de module Diffie-Hellman à utiliser.

Les options doivent ressembler à ce qui suit.

g) Cliquez sur **Next** (suivant).
h) Passez en revue le résumé et cliquez sur **Finish** (Terminer).

Les informations récapitulatives sont copiées dans le presse-papiers. Vous pouvez coller ces renseignements dans un document et les utiliser pour vous aider à configurer l'homologue distant ou les envoyer à la personne responsable de la configuration de cet homologue.

i) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.

j) Cliquez sur le bouton **Deploy Now** (Déployer maintenant) et attendez la fin du déploiement.

Le périphérique du site B est maintenant prêt à héberger une extrémité de la connexion VPN de site à site.

Étape 2 Déconnectez-vous du périphérique **du site B** et connectez-vous au périphérique **du site A**.

Étape 3 Configurez la connexion VPN de site à site sur **le site A**, qui accueillera le VPN d'accès à distance.

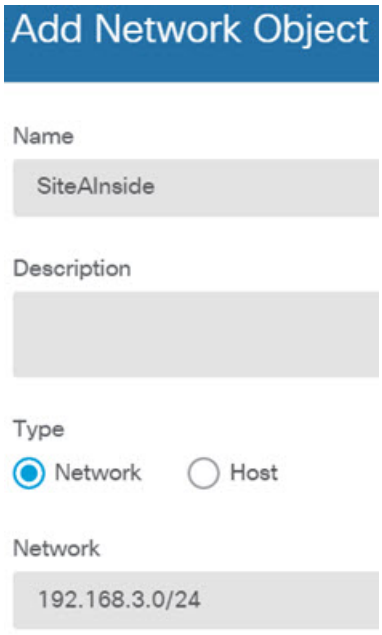
a) Cliquez sur **Device** (Périphérique), puis sur **View Configuration** (Afficher la configuration) dans le groupe Connexion VPN de site à site.

b) Cliquez sur le bouton **+**.

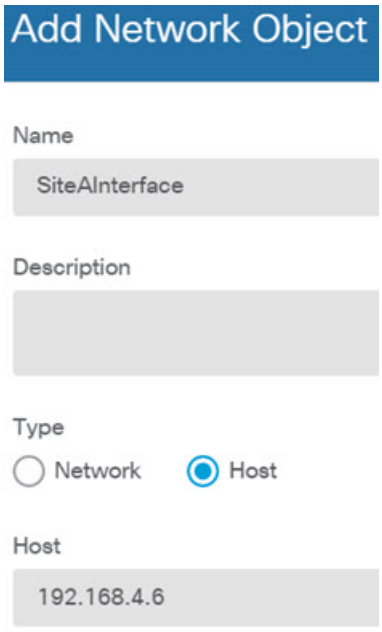
c) Configurez les options suivantes pour **Endpoint Setting**s (Paramètres de point terminal).

- **Connection Profile Name** (Nom du profil de connexion) : saisissez un nom, par exemple, Site B (pour indiquer que la connexion se fait au site B).
- **Local Site** (Site local) : ces options définissent le point terminal local.
  - **Local VPN Access Interface** (Interface d'accès VPN local) : sélectionnez l'interface **externe** (celle dont l'adresse 192.168.4.6 dans le diagramme).
  - **Local Network** (Réseau local) : cliquez sur le signe plus **+** et sélectionnez les objets réseau qui identifient les réseaux locaux qui doivent participer à la connexion VPN. Cliquez sur **Create New Network** (Créer un nouveau réseau), configurez les objets suivants, puis sélectionnez-les dans la liste. **Notez que vous avez créé les mêmes objets dans le périphérique du site B, mais que vous devez les créer à nouveau dans le périphérique du site A.**

    1. SiteAInside, réseau, 192.168.3.0/24.

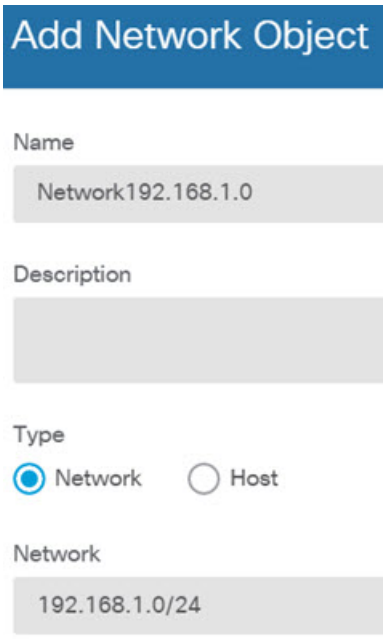


2. SiteAInterface, hôte, 192.168.4.6. **Il s'agit de la clé : vous devez inclure l'adresse du point de connexion VPN d'accès à distance en tant que partie du réseau interne pour la connexion VPN de site à site afin que le VPN d'accès à distance hébergé sur cette interface puisse utiliser le serveur de répertoire sur le réseau distant.**

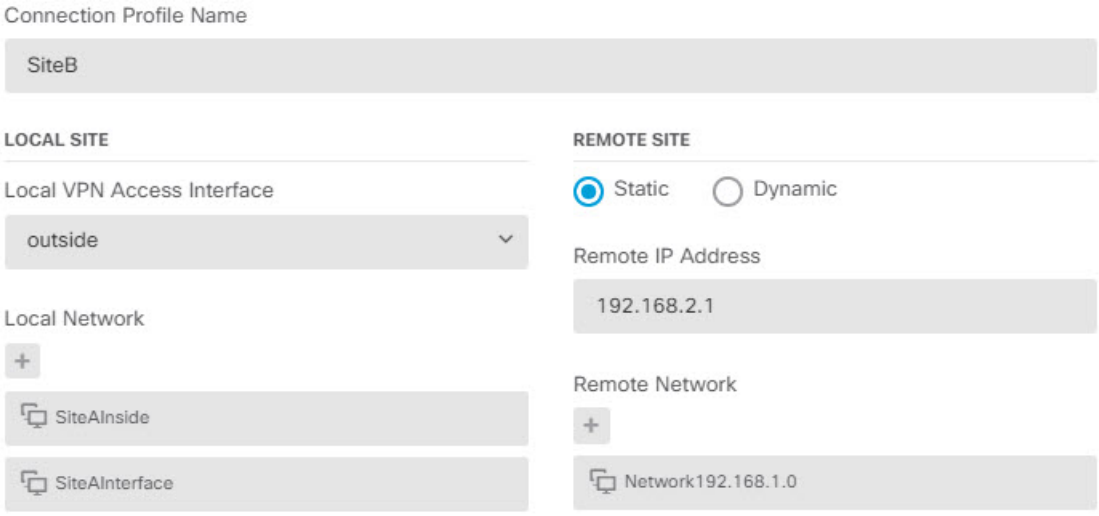


- **Remote Site** (Site distant) : ces options définissent le terminal distant.
  - **Remote IP Address** (Adresse IP distante) : saisissez 192.168.2.1, qui correspond à l'adresse IP de l'interface de l'homologue VPN distant qui hébergera la connexion VPN.

- **Remote Network** (Réseau distant) : cliquez sur le signe + et sélectionnez l'objet réseau qui identifie le réseau distant qui doit participer à la connexion VPN, celui qui comprend le serveur de répertoire. Cliquez sur **Create New Network** (Créer un nouveau réseau) et configurez un objet pour le réseau 192.168.1.0/24. Après avoir enregistré l'objet, sélectionnez-le dans la liste déroulante et cliquez sur **OK**. **Notez que vous avez créé le même objet dans le périphérique du site B, mais que vous devez le créer à nouveau dans le périphérique du site A.**



Lorsque vous avez terminé, les paramètres de terminal devraient ressembler à ce qui suit. Remarquez que les réseaux locaux/distants sont inversés par rapport aux paramètres du site B. C'est ainsi que les deux extrémités d'une connexion point à point doivent toujours ressembler.

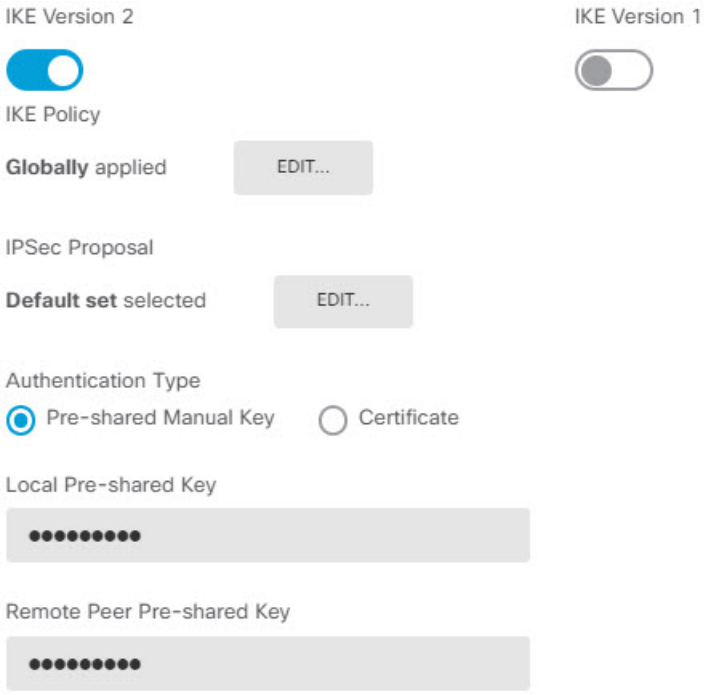


d) Cliquez sur **Next** (suivant).

e) Définissez la configuration de confidentialité pour le VPN.

Configurez la même version IKE, la même politique et la même proposition IPsec, et les mêmes clés prépartagées que vous l'avez fait pour la connexion au site B, **mais assurez-vous d'inverser les clés prépartagées Local et Remote**.

La politique IKE doit ressembler à ce qui suit :



f) Configurez les **options supplémentaires**.

- **NAT Exempt** (Exemption NAT : sélectionnez l'interface qui héberge le réseau interne, dans cet exemple, l'interface **interne**. En règle générale, vous ne souhaitez pas que le trafic dans un tunnel VPN de site à site voie les adresses IP traduites. Cette option ne fonctionne que si le réseau local se trouve derrière une interface de routage unique (et non un membre d'un groupe de ponts). Si le réseau local se trouve derrière plusieurs interfaces de routage ou un ou plusieurs membres de groupes de ponts, vous devez créer manuellement les règles d'exemption de NAT. Pour plus d'informations sur la création manuelle des règles requises, consultez Exemption du trafic VPN de site à site de la NAT.
- **Diffie-Hellman Group for Perfect Forward Secrecy (Groupe Diffie-Hellman pour la confidentialité de transmission** parfaite) : sélectionnez **Group 19** (Groupe 19).

Les options doivent ressembler à ce qui suit.

g) Cliquez sur **Next** (suivant).
h) Passez en revue le résumé et cliquez sur **Finish** (Terminer).
i) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.

j) Cliquez sur le bouton **Deploy Now** (Déployer maintenant) et attendez la fin du déploiement.

Le périphérique du site A est maintenant prêt à héberger l'autre extrémité de la connexion VPN de site à site. Comme le site B est déjà configuré avec des paramètres compatibles, les deux périphériques doivent négocier une connexion VPN.

Vous pouvez confirmer la connexion en vous connectant à l'interface de ligne de commande du périphérique et en envoyant un message ping au serveur de répertoire. Vous pouvez également utiliser la commande **show ipsec sa** pour afficher les informations de session.

Étape 4 Configurez le serveur de répertoire sur le **Site A**. Cliquez sur **Test** (Tester) pour vérifier qu'il y a une connexion.

a) Sélectionnez **Objects** (Objets), puis sélectionnez (Domaine d'identité) **Identity Sources** (Sources d'identité) dans la table des matières.
b) Cliquez sur **+** > **AD**.
c) Configurez les propriétés de base du domaine.

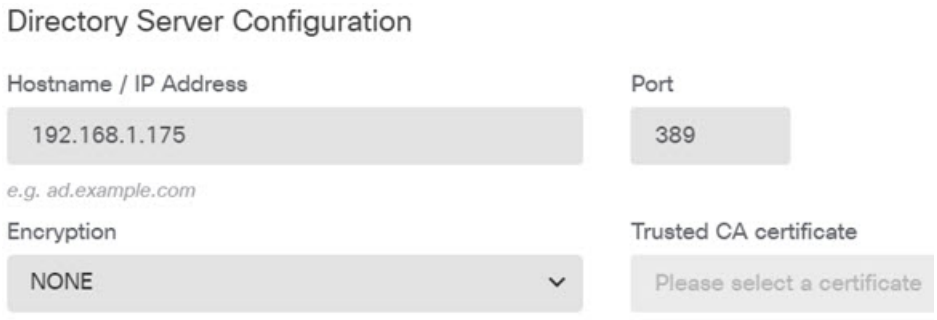
- **Name** (nom) : Nom du domaine de répertoire. Par exemple, AD.
- **Type** : Type de serveur d'annuaire. Active Directory est le seul type pris en charge et vous ne pouvez pas modifier ce champ.
- **Directory Username** (nom d'utilisateur), **Directory Password** (mot de passe d'annuaire) : nom d'utilisateur et mot de passe uniques pour un utilisateur disposant des droits appropriés sur les informations utilisateur que vous souhaitez récupérer. Pour Active Directory, l'utilisateur n'a pas besoin d'avoir des privilèges élevés. Vous pouvez préciser n'importe quel utilisateur dans le domaine. Le nom d'utilisateur doit être complet; par exemple, Administrateur@exemple.com (pas simplement Administrateur).

  Remarque
  Le système génère ldap-login-dn et ldap-login-password à partir de ces informations. Par exemple, Administrateur@exemple.com se traduit par cn=adminisntrator,cn=users,dc=example,dc=com. Notez que cn=users fait toujours partie de cette traduction; vous devez donc configurer l'utilisateur que vous précisez ici sous le nom usuel du dossier « users ».

- **Base DN** (base DN) : L'arborescence pour faire des recherches ou requêtes d'informations sur les utilisateurs et les groupes, c'est-à-dire le parent commun des utilisateurs et des groupes. Par exemple, cn=users,dc=example,dc=com. Pour en savoir plus sur la recherche du DN de base, consultez Détermination du DN de base du répertoire.
- **AD Primary Domain** (domaine principal AD) : le nom de domaine complet d'Active Directory que le périphérique doit joindre.' Par exemple, exemple.com.

d) Configurez les propriétés du serveur d'annuaire.

- **Hostname/IP Address** (nom d'hôte/adresse IP) : le nom d'hôte ou l'adresse IP du serveur d'annuaire. Si vous utilisez une connexion chiffrée avec le serveur, vous devez saisir le nom de domaine complet, et non l'adresse IP. Pour cet exemple, saisissez 192.168.1.175.
- **Port** : le numéro de port utilisé pour les communications avec le serveur. La valeur par défaut est 389. Utilisez le port 636 si vous sélectionnez LDAPS comme méthode de chiffrement. Pour cet exemple, conservez 389.
- **Encryption** (Chiffrement) : pour utiliser une connexion chiffrée afin de télécharger les informations sur les utilisateurs et les groupes. La valeur par défaut est **None** (aucun), ce qui signifie que les informations relatives aux utilisateurs et aux groupes sont téléchargées en texte en clair. Pour le VPN d'accès à distance, vous pouvez utiliser **LDAPS**, qui est LDAP sur SSL. Utilisez le port 636 si vous sélectionnez cette option. Le VPN d'accès à distance ne prend pas en charge STARTTLS. Pour cet exemple, sélectionnez **None** (Aucun).
- **Trusted CA Certificate** (certificat CA de confiance) : Si vous sélectionnez une méthode de chiffrement, téléchargez un certificat d'autorité de certification (CA) pour activer une connexion de confiance entre le système et le serveur d'annuaire. Si vous utilisez un certificat pour vous authentifier, le nom du serveur dans le certificat doit correspondre au nom d'hôte ou à l'adresse IP du serveur. Par exemple, si vous utilisez 192.168.1.175 comme adresse IP mais ad.exemple.com dans le certificat, la connexion échouera.



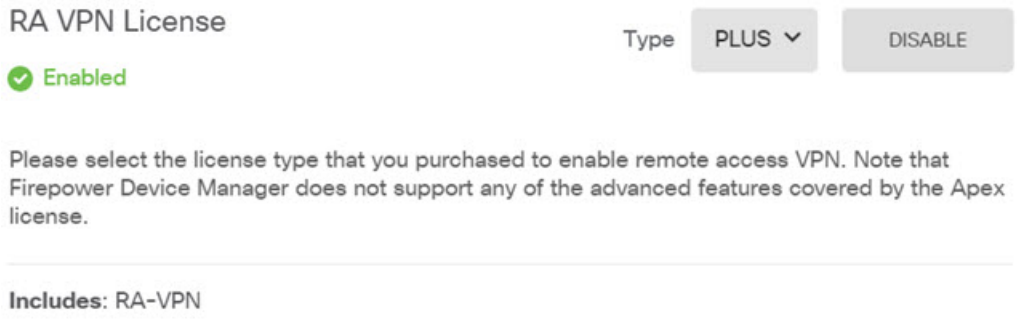
e) Cliquez sur le bouton **Test** (Tester) pour vérifier que le système peut communiquer avec le serveur.

Le système utilise des processus distincts pour accéder au serveur, de sorte que vous pourriez obtenir des erreurs indiquant que la connexion fonctionne pour un type d'utilisation mais pas pour un autre, par exemple, disponible pour les politiques d'identité mais pas pour le VPN d'accès à distance. Si le serveur n'est pas accessible, vérifiez que vous avez la bonne adresse IP et le bon nom d'hôte, que le serveur DNS dispose d'une entrée pour le nom d'hôte, etc. Vérifiez également que la connexion VPN de site à site fonctionne et que vous avez inclus l'adresse de l'interface externe du site A dans le VPN, et que la NAT ne traduit pas le trafic pour le serveur de répertoire. Vous devrez peut-être également configurer une route statique pour le serveur.

f) Cliquez sur **OK**.

Étape 5 Cliquez sur **Device (Périphérique)** > **Smart License (Licence Smart)** > **View Configuration (Afficher la configuration)**, et activez la licence de VPN d'accès à distance.

Lors de l'activation de la licence VPN d'accès à distance, sélectionnez le type de licence que vous avez acheté : Plus, Apex (ou les deux) ou VPN uniquement. Pour en savoir plus, consultez Exigences de licence pour le VPN d'accès à distance, à la page 8.

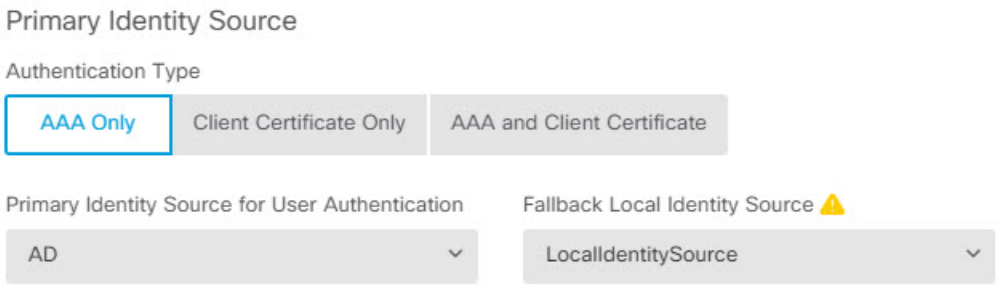


Étape 6 Configurez un VPN d'accès à distance sur le site A.

a) Cliquez sur **View Configuration** (Afficher la configuration) dans le groupe **Device (Périphérique)** > **Remote Access VPN (VPN d'accès à distance**. Assurez-vous que vous êtes sur la page **Connection Profiles** (Profils de connexion)..

b) Créer ou modifier un profil de connexion.

c) Dans la première étape de l'assistant, configurez le nom de profil, puis sélectionnez le domaine AD comme source d'authentification principale. Vous pouvez éventuellement sélectionner la base de données locale comme source d'identité de repli.



d) Configurez l'ensemble d'adresses.

Pour cet exemple, cliquez sur **+**, puis sélectionnez **Create New Network** (Créer un nouveau réseau) dans l'ensemble d'adresses IPv4 et créez un objet pour le réseau 172.18.1.0/24, puis sélectionnez l'objet. Les

clients reçoivent une adresse de cet ensemble. Laissez le champ IPv6 vide. L'ensemble d'adresses ne peut pas se trouver sur le même sous-réseau que l'adresse IP pour l'interface externe.

L'objet doit ressembler à ce qui suit :

La spécification de l'ensemble doit ressembler à ce qui suit :

e) Cliquez sur **Next** (Suivant), puis sélectionnez une politique de groupe appropriée.

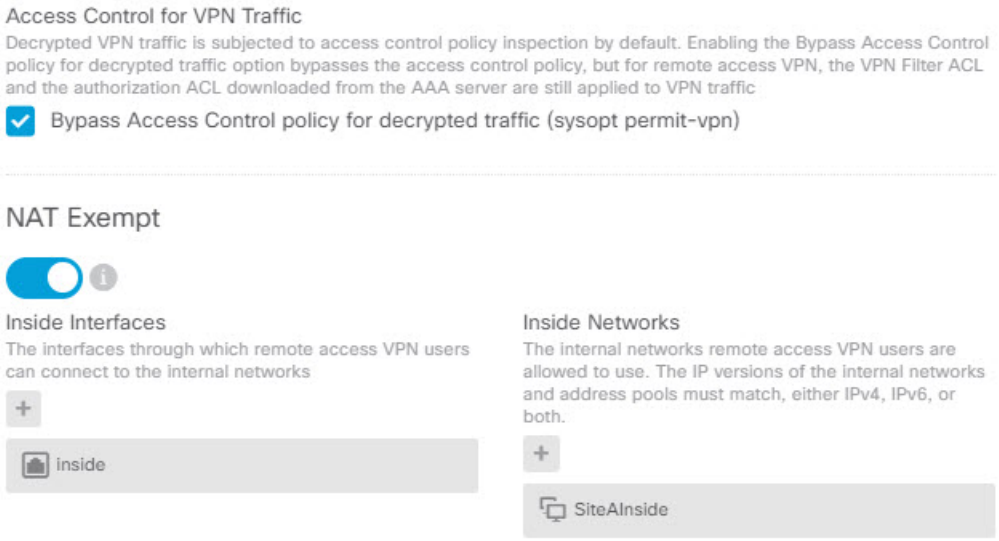
Vérifiez les renseignements récapitulatifs sur la politique que vous sélectionnez. Assurez-vous que les serveurs DNS sont configurés. Si ce n'est pas le cas, modifiez la politique maintenant et configurez le DNS.

f) Cliquez sur **Next** (Suivant), et dans les paramètres globaux, sélectionnez l'option **de contournement de la stratégie de contrôle d'accès pour le trafic déchiffré (sysopt permit-vpn)** et configurez les options **NAT Exempt** (Exemption NAT).

Pour **NAT Exempt** (Exemption NAT), vous devez configurer les options suivantes. Notez que si d'autres profils de connexion sont définis, vous devez ajouter aux paramètres existants, car la configuration s'applique à tous les profils de connexion.

- **Inside Interfaces** (Interfaces internes) : sélectionnez l'interface **inside**. Ce sont les interfaces des réseaux internes auxquels les utilisateurs distants accéderont. Les règles NAT sont créées pour ces interfaces.

- **Inside Networks** (Réseaux internes) : Sélectionnez l'objet réseau SiteAInside. Ce sont les objets réseau qui représentent les réseaux internes auxquels les utilisateurs distants accéderont.



g) Chargez les paquets client AnyConnect pour les plateformes que vous prenez en charge.

h) Cliquez sur **Next** (Suivant) et vérifiez les paramètres.

Tout d'abord, vérifiez que le résumé est correct.

Ensuite, cliquez sur **Instructions** pour voir ce que doivent faire les utilisateurs finaux pour installer initialement le logiciel client AnyConnect et vérifier qu'ils peuvent établir une connexion VPN. Cliquez sur **Copy** (Copier) pour copier ces instructions dans le presse-papiers et les coller dans un fichier texte ou un courriel.

i) Cliquez sur **Terminer**.

Étape 7 Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.

Étape 8 Cliquez sur le bouton **Deploy Now** (Déployer maintenant) et attendez la fin du déploiement.

L'appareil du site A est maintenant prêt à accepter les connexions VPN d'accès à distance. Demandez à un utilisateur externe d'installer le client AnyConnect et d'établir une connexion VPN.

Vous pouvez confirmer la connexion en vous connectant à l'interface de ligne de commande du périphérique et en utilisant la commande **show vpn-sessiondb anyconnect** pour afficher les informations de session.

Comment contrôler l'accès VPN RA par groupe

Vous pouvez configurer des profils de connexion VPN d'accès à distance pour fournir un accès différentiel aux ressources internes en fonction de la politique de groupe. Par exemple, si vous souhaitez fournir un accès sans restriction aux employé(e)s, mais que les sous-traitants ne peuvent accéder qu'à un seul réseau interne

et rien d'autre, vous pouvez utiliser les politiques de groupe pour définir différentes listes de contrôle d'accès afin de restreindre l'accès de manière appropriée.

L'exemple suivant montre comment configurer une connexion VPN d'accès à distance pour les sous-traitants qui doivent obtenir un accès au sous-réseau interne 192.168.2.0/24 uniquement. Pour les employés réguliers, vous pouvez utiliser la politique de groupe par défaut, qui n'a pas de filtre de trafic défini pour le VPN. Vous pouvez modifier la politique de groupe par défaut si vous souhaitez appliquer des restrictions à ces utilisateurs et appliquer une liste de contrôle d'accès bâtie comme décrit ci-dessous.

Avant de commencer

Cette procédure suppose que vous ayez déjà créé la source d'identité à utiliser pour les sous-traitants. Il peut s'agir d'une source différente de celle que vous utilisez pour les employés réguliers. Comme la source d'identité n'est pas strictement pertinente pour restreindre l'accès, nous l'avons omise dans cet exemple.

Cet exemple suppose également que l'interface « inside2 » est configurée pour héberger le sous-réseau 192.168.2.0/24, avec l'adresse IP 192.168.2.1 (toute autre adresse sur le sous-réseau est également acceptable).

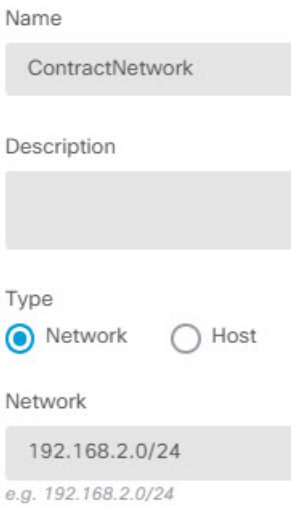
Procédure

Étape 1 Configurez la liste de contrôle d'accès (ACL) étendue pour restreindre le trafic VPN d'accès à distance.

Vous devez d'abord configurer l'objet réseau qui définit la cible 192.168.2.0/24, puis créer l'objet Smart CLI qui définit la liste d'accès. Comme la liste de contrôle d'accès comporte un refus implicite à la fin, vous n'avez qu'à autoriser l'accès au sous-réseau, et le trafic dirigé vers une adresse IP en dehors du sous-réseau sera refusé. Cet exemple s'applique uniquement à IPv4; vous pouvez également configurer des objets pour restreindre l'accès IPv6 à des sous-réseaux particuliers. Créez simplement l'objet réseau et ajoutez une commande ACE basée sur IPv6 à la même liste de contrôle d'accès.

a) Choisissez **Objects (Objets)** > **Networks (Réseaux)**, et créez l'objet requis.

Par exemple, nommez l'objet ContractNetwork. Le corps de l'objet doit ressembler à ce qui suit :



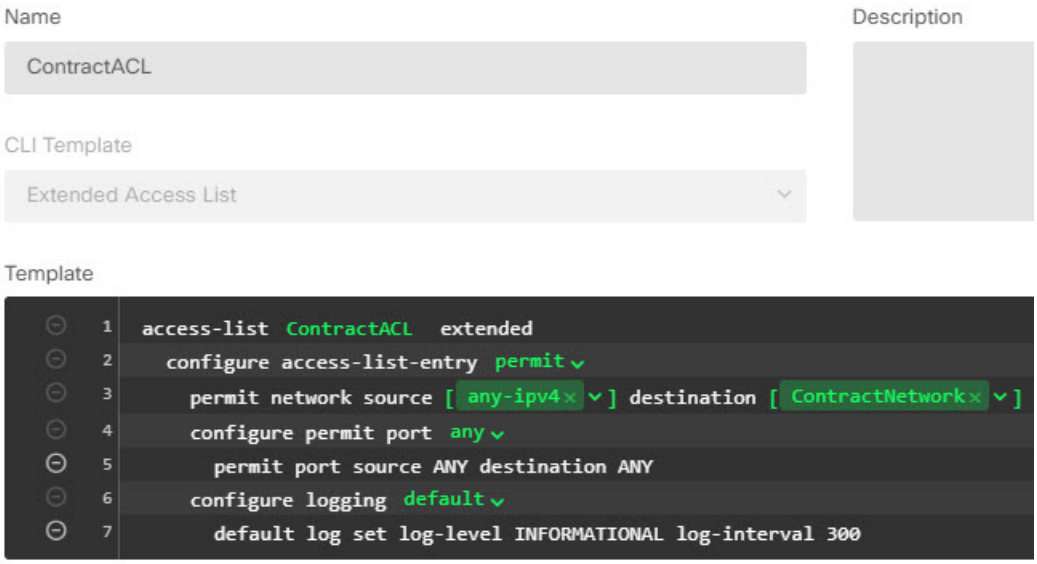
b) Choisissez **Device (Périphérique)** > **Advanced Configuration (Configuration avancée)** > **Smart CLI** > **Objects (Objets)**.

c) Cliquez + pour créer un nouvel objet.

d) Saisissez un nom pour la liste de contrôle d'accès. Par exemple, **ContractACL**.
e) Pour **CLI Template** (Modèle CLI), sélectionnez **Extended Access List** (Liste d'accès étendue).
f) Configurez les éléments suivants dans le **corps du modèle** :

- configurer l'action de liste d'accès = autoriser
- réseau-source = any-ipv4
- destination-network = objet ContractNetwork
- Configurer le port d'autorisation = tout
- Configurer la journalisation = par défaut

L'ACE doit ressembler à ce qui suit :



g) Cliquez sur **OK**.

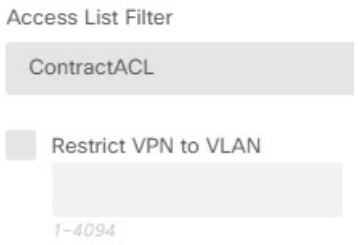
Cette liste de contrôle d'accès sera configurée lors du prochain déploiement de modifications. Vous n'avez pas besoin d'utiliser l'objet dans une autre politique pour forcer le déploiement.

Étape 2 Créez une politique de groupe qui utilise l'ACL.

Vous devez également configurer au minimum les serveurs DNS pour la politique de groupe. Configurez les options selon vos besoins. La procédure suivante se concentre sur le paramètre pertinent pour ce scénario.

a) Choisissez **Device (Périphérique)** > **RA VPN (VPN d'accès à distance)** > **Group Policies (Politiques de groupe)**.
b) Cliquez sur **+** pour créer une nouvelle politique de groupe.
c) Dans la page **General** (Général) , saisissez un nom pour la politique, par exemple **ContractGroup**.
d) Cliquez sur **Traffic Filters** (Filtres de trafic) dans la table des matières.
e) Pour **Access List Filter** (Filtre de liste d'accès), sélectionnez l'objet ContractACL.

Pour cet exemple, laissez l'option VLAN vide. Notez que vous pouvez également configurer un VLAN à des fins de filtrage et configurer une sous-interface pour le VLAN.



f) Cliquez sur **OK** pour enregistrer la politique de groupe.

Étape 3 Configurez le profil de connexion pour les sous-traitants.

a) Sur la page RA VPN (VPN d'accès à distance), cliquez sur **Connection Profiles** (Profils de connexion) dans la table des matières.

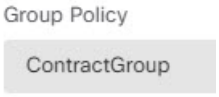
b) Cliquez sur **+** pour créer un nouveau profil de connexion.

c) Terminez l'étape 1 de l'assistant et cliquez sur **Next** (Suivant).

Saisissez un nom pour le profil, par exemple, Sous-traitants.

Configurez le reste des options comme d'habitude. Cela inclut la sélection de la source d'authentification appropriée pour les sous-traitants et la définition d'un ensemble d'adresses.

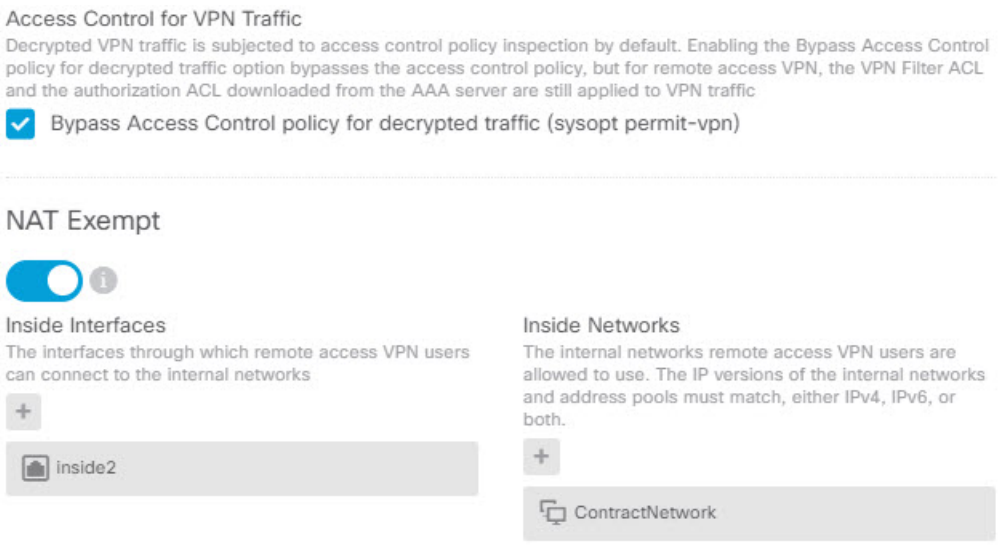
d) Sélectionnez la politique de groupe que vous avez configurée pour les sous-traitants, puis cliquez sur **Next** (Suivant).



e) Dans les paramètres globaux, sélectionnez l'option **Bypass Access Control policy for decrypted traffic** (Politique de contournement du contrôle d'accès pour le trafic déchiffré) (sysopt permit-vpn) et configurez les options **NAT Exempt** (Exemption NAT).

Pour **NAT Exempt** (Exemption NAT), vous devez configurer les options suivantes. Notez que si d'autres profils de connexion sont définis, vous devez ajouter aux paramètres existants, car la configuration s'applique à tous les profils de connexion.

- **Inside Interfaces** (Interfaces internes) : sélectionnez l'interface **inside2**. Ce sont les interfaces des réseaux internes auxquels les utilisateurs distants accéderont. Les règles NAT sont créées pour ces interfaces.
- **Inside Networks** (Réseaux internes) : sélectionnez l'objet réseau ContractNetwork. Ce sont les objets réseau qui représentent les réseaux internes auxquels les utilisateurs distants accéderont.



f) Chargez les paquets client AnyConnect pour les plateformes que vous prenez en charge.

g) Cliquez sur **Next** (Suivant) et vérifiez les paramètres.

Tout d'abord, vérifiez que le résumé est correct.

Ensuite, cliquez sur **Instructions** pour voir ce que doivent faire les utilisateurs finaux pour installer initialement le logiciel client AnyConnect et vérifier qu'ils peuvent établir une connexion VPN. Cliquez sur **Copy** (Copier) pour copier ces instructions dans le presse-papiers et les coller dans un fichier texte ou un courriel.

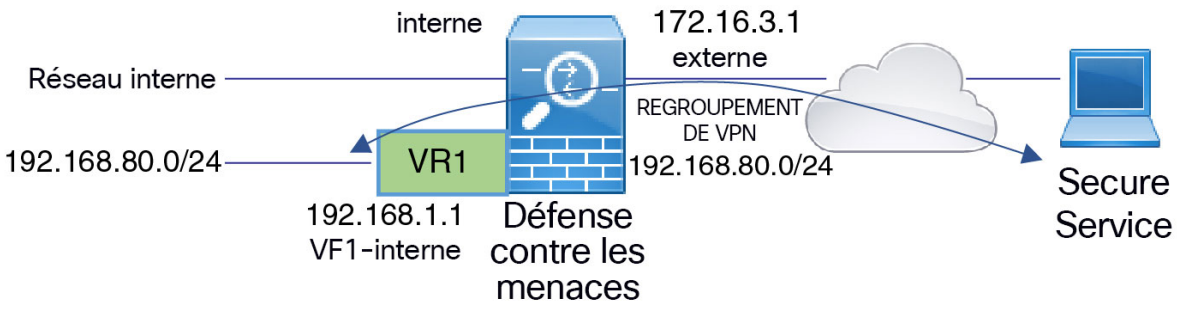
h) Cliquez sur **Terminer**.

Comment autoriser l'accès au VPN d'accès à distance aux réseaux internes dans différents routeurs virtuels.

Si vous configurez plusieurs routeurs virtuels sur un périphérique, vous devez configurer le VPN d'accès distant dans le routeur virtuel global. Vous ne pouvez pas configurer le VPN d'accès distant sur une interface affectée à un routeur virtuel personnalisé.

Comme les tables de routage pour les routeurs virtuels sont distinctes, vous devez créer des routes statiques si vos utilisateurs de VPN d'accès distant doivent avoir accès à des réseaux qui font partie d'un autre routeur virtuel.

Considérez l'exemple suivant. Dans ce cas, l'utilisateur de VPN d'accès distant se connecte à l'interface externe à l'adresse 172.16.3.1 et reçoit une adresse IP dans le pool de 192.168.80.0/24. Cet utilisateur peut maintenant accéder au réseau interne qui est attaché au routeur virtuel global. Cependant, l'utilisateur ne peut pas atteindre le réseau 192.168.1.0/24 qui fait partie du routeur virtuel VR1. Pour permettre le flux de trafic entre le réseau VR1 et l'utilisateur VPN d'accès distant, vous devez configurer des routes statiques dans les deux sens.



Avant de commencer

Cet exemple suppose que vous ayez déjà configuré de VPN d'accès à distance, défini les routeurs virtuels et configuré et affecté les interfaces aux routeurs virtuels appropriés.

Procédure

Étape 1 Configurez la fuite de route du routeur virtuel global vers VR1.

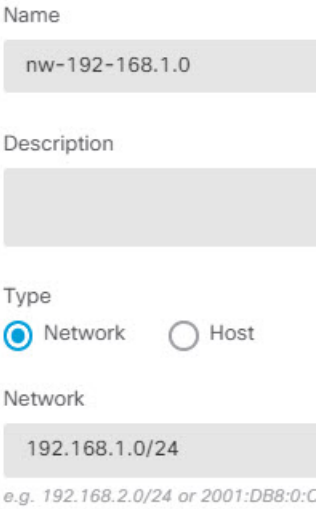
Cette route permet aux adresses IP client AnyConnect attribuées dans l'ensemble d'adresses du VPN d'accéder au réseau 192.168.1.0/24 du routeur virtuel VR1.

a) Choisissez **Device (Périphérique)** > **Routing (Routage)** > **View Configuration (Afficher la configuration)**.

b) Cliquez sur l'icône d'affichage ( ) du routeur virtuel global.

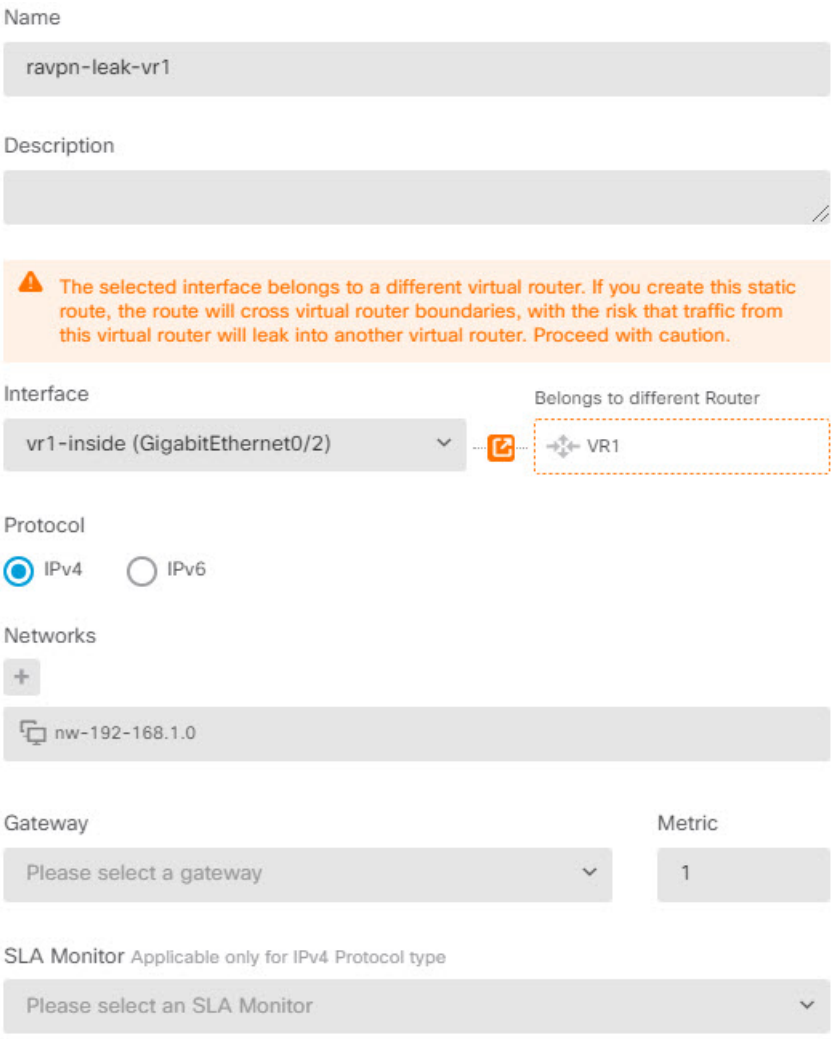
c) Dans l'onglet **Static Routing** (Routage statique) du routeur virtuel global, cliquez sur + et configurez la route :

- **Nom** : n'importe quel nom suffit, tel que **ravpn-leak-vr1**.
- **Interface** : sélectionnez **vr1-inside**.
- **Protocole** : sélectionnez **IPv4**.
- **Réseaux** : sélectionnez un objet qui définit le réseau 192.168.1.0/24. Cliquez sur **Create New Network** (Créer un nouveau réseau) pour créer l'objet maintenant, si nécessaire.



- **Gateway** (passerelle) : laissez ce champ vide. Lors de la fuite d'une route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.

La boîte de dialogue doit ressembler à ce qui suit :



d) Cliquez sur **OK**.

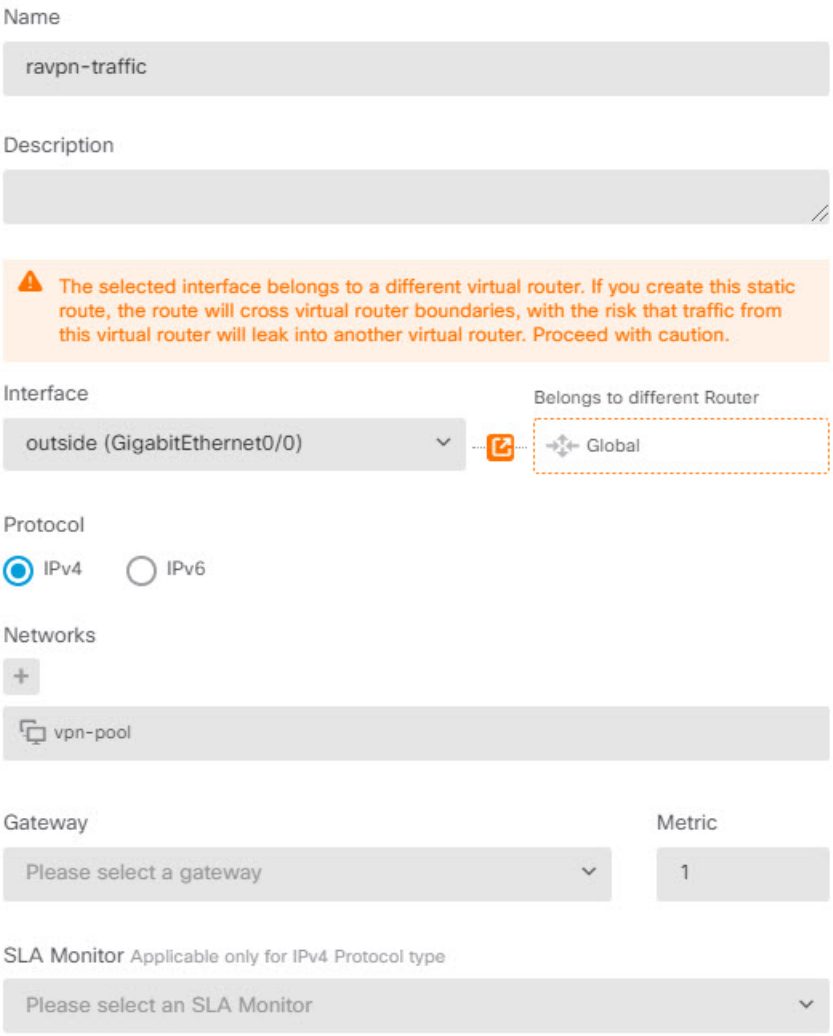
Étape 2 Configurez la fuite de route de VR1 vers le routeur virtuel global :

Cette route permet aux points terminaux sur le réseau 192.168.1.0/24 d'établir des connexions avec les client AnyConnect adresses IP attribuées dans l'ensemble d'adresses du VPN.

a) Choisissez **VR1** dans la liste déroulante des routeurs virtuels pour passer à la configuration VR1.
b) Dans l'onglet **Static Routing** (Routage statique) du routeur virtuel VR1, cliquez sur + et configurez la route :

- **Nom** : n'importe quel nom suffit, tel que **ravpn-trafic**.
- **Interface** : sélectionnez **outside**.
- **Protocole** : sélectionnez **IPv4**.
- **Réseaux** : sélectionnez l'objet que vous avez créé pour le regroupement VPN, par exemple, **vpn-pool**.
- **Gateway** (passerelle) : laissez ce champ vide. Lors de la fuite d'une route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.

La boîte de dialogue doit ressembler à ce qui suit :



c) Cliquez sur **OK**.

Prochaine étape

Si l'ensemble d'adresses du VPN d'accès à distance et les adresses IP du routeur virtuel défini par l'utilisateur se chevauchent, vous devez également utiliser des règles NAT statiques sur les adresses IP pour permettre un routage approprié. Cependant, il est beaucoup plus facile de modifier simplement votre ensemble d'adresses VPN d'accès à distance afin d'éviter les chevauchements.

Comment personnaliser l'icône et le logo client AnyConnect

Vous pouvez personnaliser l'icône et le logo de l'application client 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 obtenir 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 et de l'installateur dans le *Guide de l'administrateur du client Secure Client AnyConnect Secure Mobility Client*. 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

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 périphérique FTD agissant comme tête de réseau VPN d'accès à distance et devant utiliser les icônes et 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 normal. FTD

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) du périphérique. 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 omises 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 au périphérique de télécharger ces images lors de son installation sur les machines client AnyConnect

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
```

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. 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
```

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.