Politiques d'accès dynamique

Ce chapitre décrit comment configurer les politiques d'accès dynamique.

À propos des politiques d'accès dynamique

Les passerelles VPN fonctionnent dans des environnements dynamiques. Plusieurs variables peuvent affecter chaque connexion VPN, par exemple, les configurations intranet qui changent fréquemment, les différents rôles de chaque utilisateur au sein d'une organisation, et les connexions à partir de sites d'accès à distance avec des configurations et des niveaux de sécurité différents. La tâche d'autoriser les utilisateurs est beaucoup plus complexe dans un environnement VPN que dans un réseau avec une configuration statique.

Les politiques d'accès dynamiques (DAP) sur l'ASA vous permettent de configurer l'autorisation qui traite ces nombreuses variables. Vous créez une politique d'accès dynamique en définissant un ensemble d'attributs de contrôle d'accès que vous associez à un tunnel d'utilisateur ou à une session spécifique. Ces attributs traitent des problèmes d'appartenance à plusieurs groupes et de sécurité des points terminaux. L'ASA accorde l'accès à un utilisateur particulier pour une session particulière en fonction des politiques que vous définissez. L'ASA génère une DAP au moment où l'utilisateur se connecte en sélectionnant ou en agrégeant les attributs d'un ou de plusieurs enregistrements DAP. Il sélectionne ensuite ces enregistrements DAP en fonction des informations de sécurité au point terminal du périphérique distant et des informations d'autorisation AAA pour l'utilisateur authentifié. Ensuite, l'ASA applique l'enregistrement DAP au tunnel ou à la session d'utilisateur.

Le système DAP comprend les composants suivants qui nécessitent votre attention :

- Fichier de configuration de sélection DAP : fichier texte contenant les critères utilisés par l'ASA pour sélectionner et appliquer les enregistrements DAP lors de l'établissement de la session. Stocké sur l'ASA. Vous pouvez utiliser ASDM pour le modifier et le charger dans l'ASA au format de données XML. Les

fichiers de configuration de sélection DAP comprennent tous les attributs que vous configurez. Il peut s'agir d'attributs AAA, d'attributs de terminal et de politiques d'accès, comme configuré dans les listes de filtre d'ACL de type réseau et Web, de transfert de port et d'URL.

- DfltAccess Policy (politique d'accès) : toujours la dernière entrée dans la table récapitulative DAP, toujours avec une priorité de 0. Vous pouvez configurer les attributs de politique d'accès pour la politique d'accès par défaut, mais celle-ci ne contient pas (et vous ne pouvez pas configurer) les attributs d'AAA ou de point terminal. Vous ne pouvez pas supprimer DfltAccessPolicy, et il doit s'agir de la dernière entrée du tableau récapitulatif.

Reportez-vous au *guide de déploiement de Dynamic Access* (https://supportforums.cisco.com/docs/DOC-1369) pour obtenir des renseignements supplémentaires.

Prise en charge par DAP des protocoles d'accès à distance et des outils d'évaluation de la posture

L'ASA obtient les attributs de sécurité de point terminal en utilisant des outils d'évaluation de la posture que vous configurez. Ces outils d'évaluation de la posture comprennent le module de posture AnyConnect , le paquet indépendant HostScan/Secure Firewall Posture et NAC.

Le tableau suivant identifie chacun des protocoles d'accès à distance pris en charge par DAP, les outils d'évaluation de la posture disponibles pour cette méthode et les informations que cet outil fournit.

Protocole d'accès à distance pris en charge	**Module de posture de pare-feu sécurisé** **Progiciel HostScan** **Cisco Secure Firewall Posture**	**Module de posture de pare-feu sécurisé** **Progiciel HostScan** **Cisco Secure Firewall Posture**	**NAC**	**Cisco NAC Appliance**
	Renvoie les renseignements sur les fichiers, les valeurs de clé de registre, les processus en cours d'exécution et le système d'exploitation	Renvoie les informations sur les logiciels de protection contre les programmes malveillants et de pare-feu personnel.	Renvoie l'état de la NAC	Renvoie le type de VLAN et les ID de VLAN
VPN IPsec	Non	Non	Oui	Oui
VPN AnyConnect de Cisco	Oui	Oui	Oui	Oui
VPN SSL sans client (basé sur un navigateur)	Oui	Oui	Non	Non

Protocole d'accès à distance pris en charge	Module de posture de pare-feu sécurisé Progiciel HostScan Cisco Secure Firewall Posture	Module de posture de pare-feu sécurisé Progiciel HostScan Cisco Secure Firewall Posture	NAC	Cisco NAC Appliance
proxy PIX (évaluation de la posture non disponible)	Non	Non	Non	Non

Séquence de connexion d'accès à distance avec les DAP

La séquence suivante décrit un établissement typique d'accès à distance.

1. Un client distant tente d'établir une connexion VPN.
2. L'ASA effectue une évaluation de la posture à l'aide des valeurs de posture du NAC et de HostScan/Secure Firewall configurées.
3. L'ASA authentifie l'utilisateur par le biais du protocole AAA. Le serveur AAA renvoie également les attributs d'autorisation pour l'utilisateur.
4. L'ASA applique les attributs d'autorisation AAA à la session et établit le tunnel VPN.
5. L'ASA sélectionne les enregistrements DAP en fonction des informations d'autorisation AAA pour l'utilisateur et des informations d'évaluation de la posture pour la session.
6. L'ASA regroupe les attributs DAP des enregistrements DAP sélectionnés et ils deviennent la politique DAP.
7. L'ASA applique la politique DAP à la session.

Licences des politiques d'accès dynamique

Remarque Cette fonctionnalité n'est pas disponible sur les modèles sans chiffrement de charge utile.

Les politiques d'accès dynamiques (DAP) nécessitent l'une des licences suivantes :

- Secure Client Premier : pour utiliser toutes les fonctionnalités DAP.
- Secure Client Advantage : pour la vérification de version du système d'exploitation et du système d'exploitation/Secure Client uniquement.

Sujets connexes

Ajouter les attributs de point terminal Secure Client à une DAP, à la page 14

Configurer des politiques d'accès dynamique

Avant de commencer

- Sauf indication contraire, vous devez installer HostScan/Secure Firewall Posture avant de configurer les attributs des points terminaux DAP.
- Si vous effectuez une mise à niveau d'HostScan 4.3.x vers HostScan 4.6.x ou une version ultérieure, vous devez migrer tous les attributs de point terminal AV/AS/FW existants vers les attributs de point terminal AM/FW de remplacement correspondants avant d'effectuer la mise à niveau. Consultez le guide de migration AnyConnect HostScan de la version 4.3.x à la version 4.6.x pour obtenir une procédure de mise à niveau et de migration complète.
- En raison de problèmes de sécurité dans Java Web Start, vous risquez de ne pas pouvoir remplir l'attribut de terminal avancé avec des valeurs configurées si vous utilisez une configuration basée sur Webvpn sur le périphérique. Pour résoudre ce problème, utilisez l'application de bureau ASDM ou ajoutez la ou les URL liées à l'AEA en tant qu'exceptions dans la sécurité Java.
- Avant de configurer les attributs de fichier, de processus et de registre, configurez les attributs de base de fichier, de processus et de registre HostScan/Secure Firewall Posture. Pour obtenir des instructions, accédez dans ASDM à l'écran de l'interface utilisateur approprié et cliquez sur **Help** (Aide).
- DAP ne prend en charge que les caractères ASCII.

Procédure

Étape 1 Démarrez ASDM et choisissez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Network (Client) Access (Accès au réseau (client))**> **Dynamic Access Policies (Politiques d'accès dynamiques)**.

Remarque
Si un bouton d'action **Incompatible** s'affiche sous les actions Add (Ajouter), Edit (Modifier) et Delete (Supprimer), il y a eu une tentative de mise à niveau de HostScan vers une version (4.6.x ou ultérieure) qui a eu des mises à jour de bibliothèque internes qui le rendent incompatible avec vos politiques DAP existantes (créées lors de l'utilisation de HostScan 4.3.x ou d'une version antérieure). Vous devez effectuer une procédure de migration unique pour adapter votre configuration.

L'apparition de l'action **Incompatible** indique que la mise à niveau de HostScan a été lancée et que vous devez maintenant migrer votre configuration. Reportez-vous au Guide de migration AnyConnect Hostscan de la version 4.3.x à la version 4.6.x pour obtenir des instructions détaillées.

Étape 2 Pour inclure certains attributs de point terminal de pare-feu personnel ou de protection contre les programmes malveillants, cliquez sur le lien de **configuration** près du haut du volet. Ce lien ne s'affiche pas si vous avez déjà activé ces deux fonctionnalités.

Étape 3 Affichez la liste des DAP précédemment configurées.

Les champs suivants sont affichés dans le tableau :

- ACL Prior (priorité d'ACL) : affiche la priorité de l'enregistrement DAP.

  L'ASA utilise cette valeur pour séquencer logiquement les listes de contrôle d'accès lors de l'agrégation des listes de contrôle d'accès réseau et de type Web à partir de plusieurs enregistrements DAP. L'ASA

classe les enregistrements du numéro de priorité le plus élevé au plus bas, le plus bas au bas du tableau. Les numéros plus élevés ont une priorité plus élevée, c'est-à-dire qu'un enregistrement DAP avec une valeur de 4 a une priorité plus élevée qu'un enregistrement avec une valeur de 2. Vous ne pouvez pas les trier manuellement.

- Name (nom) : affiche le nom de l'enregistrement DAP.
- Network ACL List (Liste d'ACL de réseau) : affiche le nom de l'ACL de pare-feu qui s'applique à la session.
- Web-Type ACL List (Liste d'ACL de type Web) : affiche le nom de l'ACL VPN SSL qui s'applique à la session.
- Description : décrit l'objectif de l'enregistrement DAP.

Étape 4 Cliquez sur **Add** (Ajouter) ou **Edit** (Modifier) pour Ajouter ou modifier une politique d'accès dynamique, à la page 5.

Étape 5 Cliquez sur **Apply** (Appliquer) pour enregistrer votre configuration DAP.

Étape 6 Recherchez une politique d'accès dynamique (DAP) en utilisant le champ **Find** (Rechercher).

Commencez à taper dans le champ et l'outil recherchera les caractères de début de chaque champ du tableau DAP pour une correspondance. Vous pouvez utiliser des caractères génériques pour élargir votre recherche.

Par exemple, taper **`sal`** dans le champ **Find** (Rechercher) correspond à une DAP nommée `Sales`, mais pas à une DAP nommée `Wholesalers`. Si vous tapez **`*sal`** dans le champ **Find** (Rechercher), la recherche trouve la première instance de **`Sales`** ou **`Wholesalers`** dans le tableau.

Étape 7 Tester les politiques d'accès dynamique, à la page 7 pour vérifier votre configuration.

Ajouter ou modifier une politique d'accès dynamique

Procédure

Étape 1 Démarrez ASDM et choisissez **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Network (Client) Access (Accès réseau [client])** ou **Clientless SSL VPN Access (Accès VPN SSL sans client)** > **Dynamic Access Policies (Politiques d'accès dynamique)** > **Add** or **Edit (Ajouter ou Modifier).**

Étape 2 Indiquez un nom (obligatoire) et une description (facultatif) de cette politique d'accès dynamique.

- Le **Policy Name** (Nom de la politique) est une chaîne de 4 à 32 caractères ; aucun espace n'est autorisé.
- Vous pouvez utiliser un maximum de 80 caractères dans le champ DAP **Description**.

Étape 3 Dans le champ **ACL Priority** (Priorité ACL), définissez une priorité pour la politique d'accès dynamique.

L'appareil de sécurité applique les politiques d'accès dans l'ordre que vous définissez ici, le numéro le plus élevé ayant la priorité la plus élevée. Les valeurs de 0 à 2 147 483 647 sont valides. La valeur par défaut est 0.

Étape 4 Précisez vos critères de sélection pour cette DAP :

a) Dans le volet Selection Criteria (Critères de sélection), utilisez la liste déroulante ANY/ALL/NONE (sans étiquette) pour choisir si un utilisateur doit avoir une, toutes ou aucune des valeurs d'attribut AAA que vous configurez pour utiliser cette politique d'accès dynamique, ainsi que satisfaire à chaque attribut de point terminal.

   Les entrées en double ne sont pas autorisées. Si vous configurez un enregistrement DAP sans attribut AAA ou de point terminal, l'ASA le sélectionne toujours, puisque tous les critères de sélection sont satisfaits.

b) Cliquez sur **Add** or **Edit** (Ajouter ou Modifier) dans le champ AAA Attributes (Attributs AAA) pour Configurer les critères de sélection des attributs AAA dans une DAP, à la page 8.

c) Cliquez sur **Add** or **Edit** (Ajouter ou Modifier) dans la zone Endpoint Attributes (Attributs de point terminal) pour Configurer les critères de sélection des attributs de point terminal dans une DAP, à la page 11.

d) Cliquez sur le champ **Advanced** (Avancé) pour #unique_179. Cette fonctionnalité nécessite une connaissance du langage de programmation Lua.

   - AND/OR (ET/OU) : cliquez pour définir la relation entre les règles de sélection de base et les expressions logiques que vous saisissez ici, c'est-à-dire si les nouveaux attributs ajoutent ou remplacent les attributs AAA et de point terminal déjà définis. La valeur par défaut est ET.
   - Logical Expressions (Expressions logiques) : vous pouvez créer plusieurs instances de chaque type d'attribut de point terminal. Saisissez du texte LUA de forme libre qui définit les nouveaux attributs de sélection AAA et/ou de point terminal. ASDM ne valide pas le texte que vous saisissez ici; il copie simplement ce texte dans le fichier XML DAP et l'ASA le traite, en rejetant les expressions qu'il ne peut pas analyser.

     Pour en savoir plus sur l'importation ou l'exportation d'un fichier *dap.xml*, consultez Importer et exporter le fichier XML DAP entre deux ASA, à la page 6.

Étape 5 Précisez les **Access/Authorization Policy Attributes** (Attributs de politique d'accès/d'autorisation pour cette DAP).

Les valeurs d'attribut que vous configurez ici remplacent les valeurs d'autorisation du système AAA, y compris celles des utilisateurs existants, des groupes, des groupes de tunnels et des enregistrements de groupe par défaut. Consultez Configurer les attributs de la politique d'accès DAP et d'autorisation, à la page 31.

Étape 6 Cliquez sur **OK**.

Importer et exporter le fichier XML DAP entre deux ASA

La configuration des politiques d'accès dynamique (DAP) de l'ASA est stockée dans un fichier appelé *dap.xml* dans la mémoire flash de l'ASA. Le fichier contient les attributs de sélection des politiques DAP.

Remarque Bien que vous puissiez exporter le fichier *dap.xml*, le modifier (si vous connaissez la syntaxe xml) et le réimporter, soyez très prudent, car vous pouvez forcer ASDM à cesser de traiter les enregistrements DAP si vous avez mal configuré quelque chose. Il n'y a pas d'interface de ligne de commande pour manipuler cette partie de la configuration.

Utilisez ces étapes pour importer et exporter le fichier *dap.xml* entre deux ASA.

La procédure utilise l'exemple d'exportation d'un fichier *dap.xml* à partir d'ASA#1 et d'importation sur ASA#2.

Pour en savoir plus sur le traitement des fichiers sur ASA à l'aide d'ASDM, consultez la section sur la *gestion des fichiers* du *Guide de configuration d'ASDM pour les opérations générales Cisco ASA*.

Procédure

Étape 1 Effacez le fichier *dap.xml* sur l'ASA#2.

a) Enregistrez la configuration ASA#2 et *dap.xml* en externe sur un serveur tftp ou ftp.
b) Quittez ASDM pour ASA#2.

Remarque
Vous pouvez également utiliser l'option ASDM (**ASDM)** > **Tools (Outils)** > **Back Up Configurations (Sauvegarder les configurations)** > **DAP Configurations (Configurations DAP)**pour enregistrer le fichier *dap.xml*.

Vous pouvez également renommer ou supprimer le fichier *dap.xml* dans la mémoire flash ASA #2.

Étape 2 Sur l'invite de commande ASA#2, saisissez la commande **clear configure dynamic-access-policy-record** pour supprimer les configurations d'enregistrement DAP.

Étape 3 Exportez le fichier *dap.xml* à partir de la mémoire flash ASA#1 et importez-le sur la mémoire flash ASA#2.

Étape 4 Utilisez la commande **dynamic-access-policy-record** pour configurer les entrées d'enregistrement DAP d'ASA#1 sur ASA#2.

Étape 5 Sur l'ASA#2, activez le DAP à l'aide de la commande **dynamic-access-policy-config activate**.

Remarque
Vous pouvez également relancer ASDM pour ASA#2 afin d'activer la configuration DAP.

Étape 6 Relancez l'ASDM sur l'ASA#2.
Les nouvelles politiques DAP sont configurées dans l'ASA n° 2.

Tester les politiques d'accès dynamique

Ce volet vous permet de tester la récupération de l'ensemble des enregistrements DAP configurés sur le périphérique en spécifiant des paires de valeurs d'attribut d'autorisation.

Procédure

Étape 1 Utilisez les boutons Add/Edit (Ajouter/Modifier) associés aux tableaux d'attributs AAA et d'attributs de point terminal pour spécifier des paires de valeurs d'attribut.

Les boîtes de dialogue qui s'affichent lorsque vous cliquez sur ces boutons Add/Edit (Ajouter/Modifier) sont similaires à celles des boîtes de dialogue Add/Edit AAA Attributes (Ajouter/Modifier des attributs AAA) et Add/Edit Endpoint Attributes (Ajouter/Modifier des attributs de point terminal).

Étape 2 Cliquez sur le bouton **Test** (Tester).

Le sous-système DAP sur le périphérique fait référence à ces valeurs lors de l'évaluation des attributs de sélection AAA et de point terminal pour chaque enregistrement. Les résultats s'affichent dans la zone **Test Results** (Résultats du test).

Configurer les critères de sélection des attributs AAA dans une DAP

DAP complète les services AAA en fournissant un ensemble limité d'attributs d'autorisation qui peuvent remplacer les attributs fournis par AAA. Vous pouvez spécifier les attributs AAA à partir de la hiérarchie des attributs Cisco AAA ou à partir de l'ensemble complet d'attributs de réponse que l'ASA reçoit d'un serveur RADIUS ou LDAP. L'ASA sélectionne les enregistrements DAP en fonction des informations d'autorisation AAA pour l'utilisateur et des informations d'évaluation de la posture pour la session. L'ASA peut choisir plusieurs enregistrements DAP en fonction de ces informations, qu'il regroupe ensuite pour créer des attributs d'autorisation DAP.

Procédure

Pour configurer les attributs AAA comme critères de sélection des enregistrements DAP, dans la boîte de dialogue Add/Edit AAA Attributes (Ajouter/Modifier les attributs AAA), définissez les attributs Cisco, LDAP ou RADIUS que vous souhaitez utiliser. Vous pouvez définir ces attributs à la valeur = ou != de la valeur que vous saisissez. Il n'y a aucune limite au nombre d'attributs AAA pour chaque enregistrement DAP. Pour de plus amples renseignements, voir Définitions des attributs AAA, à la page 11.

AAA Attributes Type (Type d'attributs AAA) : utilisez la liste déroulante pour choisir les attributs Cisco, LDAP ou RADIUS.

- Cisco : fait référence aux attributs d'autorisation des utilisateurs stockés dans le modèle hiérarchique AAA. Vous pouvez spécifier un petit sous-ensemble de ces attributs pour les attributs de sélection AAA dans l'enregistrement DAP. Il s'agit notamment de :
  - Group Policy (Stratégie de groupe) : nom de la stratégie de groupe associée à la session utilisateur VPN. Peut être défini localement sur l'appareil de sécurité ou envoyé par un serveur RADIUS/LDAP en tant qu'attribut IETF-Class (25). Maximum de 64 caractères.
  - Assigned IP Address (Adresse IP affectée) : saisissez l'adresse IPv4 que vous souhaitez affecter à la politique.
  - Assigned IPv6 Address (Adresse IPv6 affectée) : saisissez l'adresse IPv6 que vous souhaitez affecter à la politique.
  - Connection Profile (Profil de connexion) : nom du groupe de tunnels. Maximum de 64 caractères.
  - Username (Nom d'utilisateur) : nom d'utilisateur de l'utilisateur authentifié. Maximum de 64 caractères. S'applique si vous utilisez l'authentification/autorisation locale, RADIUS, LDAP ou tout autre type d'authentification (par exemple, RSA/SDI), domaine NT, etc.).
  - =/!= : égal à/non égal à.

- LDAP : le client LDAP (appareil de sécurité) stocke toutes les paires de valeurs d'attributs de réponse LDAP natives dans une base de données associée à la session AAA pour l'utilisateur. Le client LDAP écrit les attributs de réponse dans la base de données dans l'ordre dans lequel il les reçoit. Il supprime tous les attributs suivants avec ce nom. Ce scénario peut se produire lorsqu'un enregistrement d'utilisateur et un enregistrement de groupe sont tous deux lus à partir du serveur LDAP. Les attributs d'enregistrement d'utilisateur sont lus en premier et ont toujours la priorité sur les attributs d'enregistrement de groupe.

  Pour prendre en charge l'appartenance au groupe Active Directory, le client LDAP AAA fournit un traitement spécial de l'attribut de réponse LDAP memberOf. L'attribut AD memberOf spécifie la chaîne DN d'un enregistrement de groupe dans AD. Le nom du groupe est la première valeur CN dans la chaîne DN. Le client LDAP extrait le nom de groupe à partir de la chaîne de nom distinctif et le stocke en tant qu'attribut AAA memberOf et dans la base de données d'attributs de réponse en tant qu'attribut LDAP memberOf. S'il y a des attributs de memberOf supplémentaires dans le message de réponse LDAP, le nom de groupe est extrait de ces attributs et est combiné avec l'attribut AAA memberOf précédent pour former une chaîne de noms de groupe séparés par des virgules, également mise à jour dans la base de données des attributs de réponse.

  Dans le cas où la session d'accès à distance VPN à un serveur d'authentification/autorisation LDAP renvoie les trois groupes Active Directory suivants (énumérations de memberOf) :

  cn=Engineering,ou=People,dc=company,dc=com

  cn=Employees,ou=People,dc=company,dc=com

  cn=EastCoast,ou=People,dc=company,dc=com

  L'ASA traite trois groupes Active Directory : Engineering, Employees et EastCoast qui peuvent être utilisés dans n'importe quelle combinaison comme critères de sélection aaa.ldap.

  Les attributs LDAP comprennent un nom d'attribut et une paire de valeur d'attribut dans l'enregistrement DAP. Le nom de l'attribut LDAP est sensible à la syntaxe et à la casse. Si, par exemple, vous spécifiez l'attribut LDAP Department au lieu de ce que le serveur AD renvoie comme department, l'enregistrement DAP ne correspondra pas en fonction de ce paramètre d'attribut.

  Remarque
  Pour saisir plusieurs valeurs dans le champ Value (Valeur), utilisez le point-virgule (;) comme délimiteur. Par exemple :

  eng;sale; cn=Audgen VPN,ou=USERS,o=OAG

- RADIUS : le client RADIUS stocke toutes les paires de valeurs d'attribut de réponse RADIUS natives dans une base de données associée à la session AAA pour l'utilisateur. Le client RADIUS écrit les attributs de réponse dans la base de données dans l'ordre dans lequel il les reçoit. Il supprime tous les attributs suivants avec ce nom. Ce scénario peut se produire lorsqu'un enregistrement d'utilisateur et un enregistrement de groupe sont tous deux lus à partir du serveur RADIUS. Les attributs d'enregistrement d'utilisateur sont lus en premier et ont toujours la priorité sur les attributs d'enregistrement de groupe.

  Les attributs RADIUS comprennent un numéro d'attribut et une paire de valeurs d'attribut dans l'enregistrement DAP.

  Remarque
  Pour les attributs RADIUS, DAP définit l'ID d'attribut = 4096 + ID RADIUS.

  Par exemple :

  L'attribut RADIUS « Access Hours » a un ID Radius = 1, donc la valeur de l'attribut DAP = 4096 + 1 = 4097.

L'attribut RADIUS « Member Of » a un ID Radius = 146, donc la valeur de l'attribut DAP = 4096 + 146 = 4242.

- Les attributs LDAP et RADIUS comprennent :
  - Attribute ID (ID d'attribut) : nomme et numérote l'attribut. Maximum de 64 caractères.
  - Value (Valeur) : nom (LDAP) ou numéro (RADIUS) de l'attribut.

    Pour saisir plusieurs valeurs dans le champ Value (Valeur), utilisez le point-virgule (;) comme délimiteur. Par exemple : `eng;sale; cn=Audgen VPN,ou=USERS,o=OAG`
  - =/!= : égal à/non égal à.
- LDAP comprend le bouton Get AD Groups (Obtenir les groupes AD). Consultez Récupérer des groupes Active Directory, à la page 10.

Récupérer des groupes Active Directory

Vous pouvez interroger un serveur Active Directory pour connaître les groupes AD disponibles dans ce volet. Cette fonctionnalité s'applique uniquement aux serveurs Active Directory utilisant LDAP. Ce bouton interroge le serveur LDAP Active Directory pour obtenir la liste des groupes auxquels l'utilisateur appartient (énumérations de MemberOf). Utilisez les informations de groupe pour préciser les critères de sélection AAA de la politique d'accès dynamique.

Les groupes AD sont récupérés à partir du serveur LDAP à l'aide de la commande CLI **how-ad-groups** en arrière-plan. Le délai par défaut pendant lequel l'ASA attend une réponse du serveur est de 10 secondes. Vous pouvez ajuster cette heure à l'aide de la commande **group-search-timeout** en mode de configuration d'hôte aaa-server.

Vous pouvez modifier le niveau dans la hiérarchie Active Directory où la recherche commence en modifiant Group Base DN (DN de base de groupe) dans le volet Edit AAA Server (Modifier le serveur AAA). Vous pouvez également modifier le délai pendant lequel l'ASA attend une réponse du serveur dans la fenêtre. Pour configurer ces fonctionnalités, choisissez **Configuration > Remote Access VPN (VPN d'accès à distance) > AAA/Local Users (Utilisateurs AAA/locaux) > AAA Server Groups (Groupes de serveurs AAA) > Edit AAA Server (Modifier le serveur AAA)**.

Remarque Si le serveur Active Directory comporte un grand nombre de groupes, la liste des groupes AD récupérés (ou la sortie de la commande **show ad-groups**) peut être tronquée en fonction des limites de la quantité de données que le serveur peut contenir dans un paquet de réponse. Pour éviter ce problème, utilisez la fonction de filtre pour réduire le nombre de groupes signalés par le serveur.

AD Server Group (groupe de serveurs AD) : nom du groupe de serveurs AAA pour récupérer les groupes AD.

Filter By (Filtrer par) : spécifiez un groupe ou le nom partiel d'un groupe pour réduire les groupes affichés.

Group Name (Nom du groupe) : liste des groupes AD récupérés du serveur.

Définitions des attributs AAA

Le tableau suivant définit les noms d'attributs de sélection AAA qui sont disponibles pour une utilisation DAP. Le champ Attribute Name (nom d'attribut) vous montre comment saisir chaque nom d'attribut dans une expression logique LUA, ce que vous pouvez faire dans la section Advanced (Avancé) du volet Ajouter/Modifier une Politique d'accès dynamique.

Type d'attribut	Nom de l'attribut	Source	Valeur	Longueur maximale de la chaîne	Description
Cisco	aaa.cisco.grouppolicy	AAA	chaîne	64	Nom de la stratégie de groupe sur l'ASA ou envoyé par un serveur Radius/LDAP en tant qu'attribut IETF-Class (25)
	aaa.cisco.ipaddress	AAA	number	-	Adresse IP affectée pour les clients VPN de tunnel complet (IPsec, L2TP/IPsec, module SSL VPN Anyconnect)
	aaa.cisco.tunnelgroup	AAA	chaîne	64	Nom du profil de connexion ou nom du groupe de tunnels
	aaa.cisco.username	AAA	chaîne	64	Nom de l'utilisateur authentifié (s'applique si vous utilisez l'authentification/l'autorisation locale)
LDAP	aaa.ldap.<*label*>	LDAP	chaîne	128	Valeur d'attribut LDAP
RADIUS	aaa.radius.<number>	RADIUS	chaîne	128	Paire de valeurs d'attribut RADIUS

Configurer les critères de sélection des attributs de point terminal dans une DAP

Les attributs de point terminal contiennent des informations sur l'environnement système du point terminal, les résultats de l'évaluation de la posture et les applications. L'ASA génère dynamiquement un ensemble d'attributs de point terminal lors de l'établissement de la session et stocke ces attributs dans une base de données associée à la session. Chaque enregistrement DAP spécifie les attributs de sélection de point terminal qui doivent être satisfaits pour que l'ASA le choisisse pour une session. L'ASA sélectionne uniquement les enregistrements DAP qui satisfont toutes les conditions configurées.

Avant de commencer

- La configuration des attributs de point terminal en tant que critères de sélection pour les enregistrements DAP fait partie d'un processus plus vaste vers Configurer des politiques d'accès dynamique, à la page 4. Passez en revue cette procédure avant de configurer les attributs de point terminal comme critères de sélection pour les DAP.

- Pour des informations détaillées sur les attributs de point terminal, consultez Définitions des attributs de point terminal, à la page 21.
-
- Pour des informations détaillées sur la façon dont HostScan/Secure Firewall Posture vérifie les programmes de protection contre les programmes malveillants et de pare-feu personnel qui résident en mémoire, consultez DAP et programmes de protection contre les programmes malveillants et pare-feu personnel, à la page 20.

Procédure

Étape 1 Cliquez sur **Add** or **Edit** (Ajouter ou modifier) et ajoutez l'un des attributs de point terminal suivants comme critères de sélection.

Vous pouvez créer plusieurs instances de chaque type d'attribut de point terminal. Il n'y a aucune limite au nombre d'attributs de point terminal pour chaque enregistrement DAP.

- Ajouter un attribut de point terminal Anti-Malware/ à une DAP, à la page 13
- Ajouter un attribut d'application à une DAP, à la page 13
- Ajouter les attributs de point terminal Secure Client à une DAP, à la page 14
- Ajouter un attribut de point terminal de fichier à une DAP, à la page 15
- Ajouter un attribut de point terminal de périphérique à une DAP, à la page 16
- Ajouter un attribut de point terminal NAC à une DAP, à la page 17
- Ajouter un attribut de point terminal de système d'exploitation à une DAP, à la page 17
- Ajouter un attribut de point terminal Personal Firewall à une DAP, à la page 17
- Ajouter un attribut de point terminal à une DAP, à la page 18
- Ajouter un attribut de point terminal de processus à une DAP, à la page 18
- Ajouter un attribut de point terminal de registre à une DAP, à la page 19
- Ajouter plusieurs attributs d'authentification de certificat à DAP, à la page 20

Étape 2 Précisez les critères de correspondance de la politique DAP.

Pour chacun de ces types d'attribut de point terminal, décidez si la politique DAP doit exiger que l'utilisateur dispose de toutes les instances d'un type (Match All = AND, par défaut) ou d'une seule d'entre elles (Match Any = OR).

a) Cliquez sur **Logical Op** (Opération logique).
b) Choisissez **Match Any** (Correspondance avec n'importe lequel) (par défaut) ou **Match All** (Correspondance avec tous) pour chaque type d'attribut de point terminal.
c) Cliquez sur **OK**.

Étape 3 Retour à Ajouter ou modifier une politique d'accès dynamique, à la page 5.

Ajouter un attribut de point terminal Anti-Malware/ à une DAP

Avant de commencer

Si vous effectuez une mise à niveau d'HostScan 4.3.x vers HostScan 4.6.x ou une version ultérieure, vous devez migrer tous les attributs de point terminal AV/AS/FW existants vers les attributs de point terminal AM/FW de remplacement correspondants avant d'effectuer la mise à niveau. Consultez le guide de migration AnyConnect HostScan de la version 4.3.x à la version 4.6.x pour obtenir une procédure de mise à niveau et de migration complète.

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (Type d'attribut de point terminal), choisissez **Anti-Malware**.

Étape 2 Cliquez sur le bouton approprié **Installed (Installé) ou Not Installed (Non installé)** pour indiquer si l'attribut de point terminal sélectionné et les qualificateurs qui l'accompagnent (champs sous la colonne Name/Operation/Value [Nom/Opération/Valeur]) sont installés ou non installés.

Étape 3 Déterminez si vous souhaitez activer ou désactiver l'analyse en temps réel.

Étape 4 Dans la zone de liste **Vendor** (Fournisseur), choisissez le nom du fournisseur d'anti-programmes malveillants pour lequel vous effectuez le test.

Étape 5 Cochez la case **Product Description** (Description du produit) et choisissez dans la zone de liste le nom du produit du fournisseur pour lequel vous effectuez le test.

Étape 6 Cochez la case **Version** et définissez le champ d'opération sur Equal to (=) (Égal à [=]), not equal (!=) (différent de [!=]), less than (<) (inférieur à [<]), greater than (>) (supérieur à [>]), less than or equal to (<=) (inférieur ou égal à [<=]) ou greater than or equal to (>=) (supérieur ou égal à [>=]) le numéro de version du produit que vous choisissez dans la zone de liste **Version**.

Si le choix dans la zone de liste de versions comporte un x, comme par exemple 3.x, remplacez le x par un numéro de version spécifique, par exemple, 3.5.

Étape 7 Cochez la case **Last Update** (Dernière mise à jour). Indiquez le nombre de jours depuis la dernière mise à jour. Vous pouvez indiquer qu'une mise à jour doit se produire dans un délai inférieur à (<) ou supérieur (>) au nombre de jours que vous spécifiez.

Étape 8 Cliquez sur **OK**.

Ajouter un attribut d'application à une DAP

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (type d'attribut de terminal), choisissez **Application**.

Étape 2 Dans le champ d'opération du type de client, choisissez égal (=) ou non égal (!=).

Étape 3 Dans la zone de liste Client type (type de client), indiquez le type de connexion d'accès à distance pour lequel vous testez.

Étape 4 Cliquez sur **OK**.

Ajouter les attributs de point terminal Secure Client à une DAP

Les attributs de point terminal Secure Client, également connus sous le nom de posture mobile ou d'extensions d'identité AnyConnect (ACIDex), sont utilisés par le module VPN du client Cisco Secure Client pour communiquer les informations de posture à l'ASA. Les politiques d'accès dynamiques utilisent ces attributs de point terminal pour autoriser les utilisateurs.

Ces attributs de posture mobile peuvent être inclus dans une politique d'accès dynamique et appliqués sans installer HostScan/Secure Firewall Posture sur le point terminal.

Certains attributs de posture mobile ne sont pertinents que pour Secure Client exécuté sur les périphériques portables. Certains attributs de posture mobile sont pertinents à la fois pour les Secure Client exécuté sur les périphériques portables et les clients de poste de travail Secure Client.

Avant de commencer

La posture mobile nécessite une licence mobiSecure Client et une licence Premium Secure Client installées sur l'ASA. Les entreprises qui installent ces licences pourront appliquer les politiques DAP aux périphériques mobiles pris en charge en fonction des attributs DAP et d'autres attributs de point terminal existants. Cela inclut l'autorisation ou le refus de l'accès à distance à partir d'un appareil portable.

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (type d'attribut de terminal), choisissez Secure Client.

Étape 2 Cochez la case **Client Version** (Version du client) et définissez le champ d'opération pour qu'il soit égal à (=), non égal à (!=), inférieur à (<), supérieur à (>), inférieur ou égal à (<=) ou supérieur ou égal à (>=) au numéro de version Secure Client que vous spécifiez ensuite dans le champ **Client Version** (Version du client).

Vous pouvez utiliser ce champ pour évaluer la version du client sur les périphériques portables, tels que les téléphones portables et les tablettes, ou les appareils de bureau et d'ordinateur portable.

Étape 3 Cochez la case **Platform** (Plateforme) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) au système d'exploitation que vous choisissez ensuite dans la zone de liste **Platform** (Plateforme).

Vous pouvez utiliser ce champ pour évaluer le système d'exploitation sur les périphériques portables, tels que les téléphones portables et les tablettes, ainsi que le système d'exploitation sur les appareils de bureau et d'ordinateur portable. La sélection d'une plateforme active les champs d'attribut supplémentaires Device Type (Type de périphérique) et Device Unique ID (ID unique du périphérique).

Étape 4 Cochez la case **Platform Version** (Version de la plateforme) et définissez le champ d'opération pour qu'il soit égal à (=), non égal à (!=), inférieur à (<), supérieur à (>), inférieur ou égal à (<=) ou supérieur ou égal à (>=) au numéro de version du système d'exploitation que vous spécifiez ensuite dans le champ **Platform Version** (Version de la plateforme).

Si vous souhaitez créer un enregistrement DAP qui contient cet attribut, veillez à également spécifier une plateforme à l'étape précédente.

Étape 5 Si vous avez coché la case Platform (Plateforme), vous pouvez cocher la case **Device Type** (Type de périphérique). Définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) au périphérique que vous choisissez ensuite ou saisissez dans le champ **Device Type** (Type de périphérique).

Si vous avez un périphérique pris en charge qui ne figure pas dans le champ Device Type (Type de périphérique), vous pouvez le saisir dans le champ Device Type (Type de périphérique). Le moyen le plus fiable pour obtenir les informations sur le type de périphérique est d'installer Secure Client sur le point terminal, de vous connecter à l'ASA et d'effectuer un suivi DAP. Dans les résultats du suivi DAP, recherchez la valeur de **endpoint.anyconnect.devicetype**. Il s'agit de la valeur que vous devez saisir dans le champ Device Type (Type de périphérique).

Étape 6 Si vous avez coché la case Platform (Plateforme), vous pouvez cocher la case **Device Unique ID** (ID unique du périphérique). Définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) à l'ID unique du périphérique que vous spécifiez ensuite dans le champ **Device Unique ID** (ID unique du périphérique).

L'ID unique du périphérique distingue les périphériques individuels, ce qui vous permet de définir des politiques pour un périphérique portable particulier. Pour obtenir l'ID unique d'un périphérique, le périphérique doit se connecter à l'ASA et effectuer un suivi DAP. Recherchez la valeur **endpoint.anyconnect.deviceuniqueid**. Il s'agit de la valeur que vous devez saisir dans le champ Device Unique ID (ID unique du périphérique).

Étape 7 Si vous avez sélectionné une plateforme, vous pouvez ajouter des adresses MAC dans le champ **MAC Addresses Pool** (Ensemble d'adresses MAC). Définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) aux adresses MAC précisées. Chaque adresse MAC doit être au format xx-xx-xx-xx-xx-xx, où chaque 'x' est un caractère hexadécimal valide (0-9, A-F ou a-f). Les adresses MAC doivent être séparées par au moins un espace.

L'adresse MAC distingue les systèmes individuels, ce qui vous permet de définir des politiques pour un périphérique particulier. Pour obtenir l'adresse MAC d'un système, le périphérique doit se connecter à l'ASA et effectuer un suivi DAP. Recherchez la valeur **endpoint.anyconnect.macaddress**. Il s'agit de la valeur que vous devez saisir dans le champ MAC Addresses Pool (Ensemble d'adresses MAC).

Étape 8 Cliquez sur **OK**.

Ajouter un attribut de point terminal de fichier à une DAP

Avant de commencer

Avant de configurer un attribut de point terminal de fichier, définissez le fichier pour lequel vous souhaitez effectuer une analyse dans la fenêtre HostScan/Secure Firewall Posture.

Pour HostScan version 4.x, choisissez **Configuration > Remote Access VPN (VPN d'accès à distance) > Secure Desktop Manager (Gestionnaire Secure Desktop) > HostScan** dans ASDM. Pour Secure Firewall Posture version 5.x, choisissez **Configuration > Remote Access VPN (VPN d'accès à distance) > Posture (for Secure Firewall) (Posture (pour Secure Firewall)) > Posture Settings (Paramètres de posture)** dans ASDM.

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (Type d'attribut de point terminal), choisissez **File** (Fichier).

Étape 2 Sélectionnez le bouton radio approprié **Exists** (Existe) ou **Does not exist** N'existe pas) pour indiquer si l'attribut de point terminal sélectionné et les qualificateurs qui l'associent (champs sous les boutons Exists/Does not exist) doivent être présents ou non.

Étape 3 Dans la zone de liste **Endpoint ID** (ID de point terminal), choisissez dans la liste déroulante l'ID de terminal qui correspond à l'entrée de fichier pour laquelle vous souhaitez effectuer une analyse.

Les renseignements sur le fichier sont affichés sous la zone de liste des ID de terminal.

Étape 4 Cochez la case **Last Update** (Dernière mise à jour) et définissez le champ d'opération à inférieur à (<) ou supérieur à (>) un certain nombre de jours. Saisissez le nombre de jours anciens dans le champ **days** (jours) .

Étape 5 Cochez la case de **Checksum** (Somme de contrôle) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) la valeur de la somme de contrôle du fichier pour lequel vous testez.

Étape 6 Cliquez sur **Compute CRC32 Checksum** (Calculer la somme de contrôle CRC32) pour déterminer la valeur de la somme de contrôle du fichier pour lequel vous testez.

Étape 7 Cliquez sur **OK**.

Ajouter un attribut de point terminal de périphérique à une DAP

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (Type d'attribut de point terminal), choisissez **Device** (Périphérique).

Étape 2 Cochez la case **Host Name** (Nom d'hôte) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) au nom d'hôte du périphérique pour lequel vous effectuez le test. Utilisez uniquement le nom d'hôte de l'ordinateur, pas le nom de domaine complet (FQDN).

Étape 3 Cochez la case **MAC Address** (Adresse MAC) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) à l'adresse MAC de la carte d'interface réseau pour laquelle vous effectuez le test. Une seule adresse MAC par entrée. L'adresse MAC doit être au format XX-XX-XX-XX-XX-XX, où chaque X est un caractère hexadécimal.

Étape 4 Cochez la case **BIOS Serial Number** (Numéro de série du BIOS) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) à la valeur du numéro de série BIOS du périphérique pour lequel vous effectuez le test. Le format des numéros dépend du fabricant. Il n'y a aucune exigence de format.

Étape 5 Cochez la case **TCP/UDP Port Number** (Numéro de port TCP/UDP) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) au port TCP ou UDP dans l'état d'écoute pour lequel vous effectuez le test.

Dans la zone de liste déroulante TCP/UDP, choisissez le type de port pour lequel vous effectuez le test : TCP (IPv4), UDP (IPv4), TCP (IPv6) ou UDP (IPv6). Si vous testez pour plus d'un port, créez plusieurs règles d'attributs de point terminal individuelles dans le DAP et spécifiez un port dans chacune.

Étape 6 Cochez la case **Version of Secure Desktop** (CSD) (Version de Secure Desktop [CSD]) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) à la version de l'image HostScan/Secure Firewall Posture exécutée sur le terminal.

Étape 7 Cochez la case **Version of Endpoint Assessment** (Version de l'évaluation des points terminaux) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) à la version de l'évaluation des points terminaux (OPSWAT) pour laquelle vous effectuez le test.

Étape 8 Cliquez sur **OK**.

Ajouter un attribut de point terminal NAC à une DAP

Procédure

Étape 1 Dans la zone de liste **Attribute Type (type d'attribut)**, choisissez **NAC**.

Étape 2 Cochez la case **Posture Status** (état de la posture) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) la chaîne de jeton de posture reçue par l'ACS. Saisissez la chaîne du jeton de posture dans la zone Posture Status (État de la posture).

Étape 3 Cliquez sur **OK**.

Ajouter un attribut de point terminal de système d'exploitation à une DAP

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (Type d'attribut de terminal), choisissez **Operating System** (Système d'exploitation).

Étape 2 Cochez la case **OS Version** (Version du SE) et définissez le champ d'opération pour qu'il soit égal à (=) ou différent de (!=) du système d'exploitation Windows, Mac ou Linux que vous définissez dans la zone de liste **OS Version** (Version du SE).

Étape 3 Cochez la case **OS Update** (Mise à jour du SE) et définissez le champ d'opération pour qu'il soit égal à (=) ou différent de (!=) de la version de service Windows, Mac ou Linux pour le système d'exploitation que vous saisissez dans la zone de texte **OS Update** (Mise à jour du SE).

Étape 4 Cliquez sur **OK**.

Ajouter un attribut de point terminal Personal Firewall à une DAP

Avant de commencer

Si vous effectuez une mise à niveau d'HostScan 4.3.x vers HostScan 4.6.x ou une version ultérieure, vous devez migrer tous les attributs de point terminal AV/AS/FW existants vers les attributs de point terminal AM/FW de remplacement correspondants avant d'effectuer la mise à niveau. Consultez le guide de migration AnyConnect HostScan de la version 4.3.x à la version 4.6.x pour obtenir une procédure de mise à niveau et de migration complète.

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (Type d'attribut de terminal), choisissez **Operating System** (Système d'exploitation).

Étape 2 Cliquez sur le bouton **Installed (Installé) ou Not Installed (Non installé)** approprié pour indiquer si l'attribut de terminal sélectionné et les qualificateurs qui l'accompagnent (champs sous la colonne Name (Nom)/Operation (Opération)/Value (Valeur)) sont installés ou non installés.

Étape 3 Dans la zone de liste **Vendor** (Fournisseur), cliquez sur le nom du fournisseur de pare-feu personnel pour lequel vous effectuez le test.

Étape 4 Cochez la case **Product Description** (Description du produit) et choisissez dans la zone de liste le nom du produit du fournisseur pour lequel vous effectuez le test.

Étape 5 Cochez la case **Version** et définissez le champ d'opération sur Equal to (=) (Égal à), Not equal (!=) (Non égal à), Less than (<) (Inférieur à), Greater than (>) (Supérieur à), Less than or equal to (<=) (Inférieur ou égal à) ou Greater than or equal to (>=) (Supérieur ou égal à) le numéro de version du produit que vous choisissez dans la zone de liste **Version**.

Si le choix dans la zone de liste **Version** comporte un x, comme par exemple 3.x, remplacez le x par un numéro de version spécifique, par exemple, 3.5.

Étape 6 Cochez la case **Last Update** (Dernière mise à jour). Indiquez le nombre de jours depuis la dernière mise à jour. Vous pouvez indiquer qu'une mise à jour doit se produire dans un délai inférieur à (<) ou supérieur (>) au nombre de jours que vous spécifiez.

Étape 7 Cliquez sur **OK.**

Ajouter un attribut de point terminal à une DAP

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (Type d'attribut de point terminal), choisissez **Policy** (Politique).

Étape 2 Cochez la case **Location** (Emplacement) et définissez le champ d'opération pour qu'il soit égal à (=) ou non égal à (!=) au profil d'emplacement Microsoft Windows Cisco Secure Desktop. Saisissez la chaîne de profil d'emplacement Microsoft Windows Cisco Secure Desktop dans la zone de texte **Location** (Emplacement).

Étape 3 Cliquez sur **OK**.

Ajouter un attribut de point terminal de processus à une DAP

Avant de commencer

Avant de configurer un attribut de point terminal de processus, définissez le processus que vous souhaitez analyser dans la fenêtre HostScan/Secure Firewall Posture pour Cisco Secure Desktop.

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (Type d'attribut de terminal), choisissez **Process** (Processus).

Étape 2 Cliquez sur le bouton **Exists (Existe) ou Does not exist (N'existe pas)** approprié pour indiquer si l'attribut de terminal sélectionné et les qualificateurs qui l'accompagnent (champs sous les boutons Exists (Existe) et Does not exist (N'existe pas)) doivent être présents ou non.

Étape 3 Dans la zone de liste **Endpoint ID** (ID de terminal), choisissez dans la liste déroulante l'ID du terminal pour lequel vous souhaitez effectuer l'analyse.

Les informations sur le processus d'ID de terminal sont affichées sous la zone de liste.

Étape 4 Cliquez sur **OK**.

Ajouter un attribut de point terminal de registre à une DAP

L'analyse des attributs de point terminal du registre s'applique aux systèmes d'exploitation Windows uniquement.

Avant de commencer

Avant de configurer un attribut de terminal de registre, définissez la clé de registre que vous souhaitez analyser dans la fenêtre HostScan/Secure Firewall Posture.

Procédure

Étape 1 Dans la zone de liste **Endpoint Attribute Type** (Type d'attribut de terminal), choisissez **Registry** (Registre).

Étape 2 Cliquez sur le bouton approprié **Exists (Existe) ou Does not exist (N'existe pas)** pour indiquer si l'attribut de terminal de **Registry** (Registre) et les qualificateurs qui l'accompagnent (champs sous les boutons Exists [Existe] et Does not exist [N'existe pas]) doivent être présents ou non.

Étape 3 Dans la zone de liste **Endpoint ID** (ID de terminal), choisissez dans la liste déroulante l'ID de terminal qui correspond à l'entrée de registre pour laquelle vous souhaitez effectuer une analyse.

Les informations du registre sont affichées sous la zone de liste Endpoint ID (ID de terminal).

Étape 4 Cochez la case **Value** (Valeur) et définissez le champ d'opération sur égal à (=) ou non égal à (!=).

Étape 5 Dans la première zone de liste **Value** (Valeur), identifiez la clé de registre comme un dword ou une chaîne.

Étape 6 Dans la deuxième zone de liste Value operation (Opération de valeur), saisissez la valeur de la clé de registre que vous analysez.

Étape 7 Si vous souhaitez ne pas tenir compte de la casse de l'entrée de registre lors de l'analyse, cochez la case. Si vous souhaitez que la recherche soit sensible à la casse, ne cochez pas la case.

Étape 8 Cliquez sur **OK**.

Ajouter plusieurs attributs d'authentification de certificat à DAP

Vous pouvez indexer chaque certificat pour permettre le référencement à l'un des certificats reçus, selon les règles configurées. En fonction de ces champs de certificat, vous pouvez configurer des règles DAP pour autoriser ou interdire les tentatives de connexion.

Procédure

Étape 1 Accédez à **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau (client)) > Dynamic Access Policies (Politiques d'accès dynamiques) > Add Endpoint Attribute (Ajouter un attribut de terminal)**.

Étape 2 Choisissez **Multiple Certificate Authentication** (Authentification de certificat multiple) comme type d'attribut de terminal dans le menu déroulant.

Étape 3 Configurez l'un des éléments suivants ou tous, selon vos préférences :

- Nom du sujet
- Nom de l'émetteur
- Autre nom de l'objet
- Numéro de série

Étape 4 Laissez le magasin de certificats à la valeur par défaut de Aucun pour autoriser les certificats de l'un ou l'autre du magasin ou choisissez lequel autoriser, uniquement l'utilisateur ou uniquement la machine. Si vous choisissez Utilisateur ou Machine, vous devez saisir le magasin d'origine du certificat. Ces informations sont envoyées par le client dans le protocole.

DAP et programmes de protection contre les programmes malveillants et pare-feu personnel

L'appareil de sécurité utilise une politique DAP lorsque les attributs de l'utilisateur correspondent aux attributs de AAA et de point terminal configurés. L'évaluation de préconnexion et HostScan/la posture de pare-feu sécurisé renvoient des informations au périphérique de sécurité sur les attributs de point terminal configurés, et le sous-système DAP utilise ces informations pour choisir un enregistrement DAP qui correspond aux valeurs de ces attributs.

La plupart des programmes de protection contre les programmes malveillants et de pare-feu personnel, mais pas tous, prennent en charge l'analyse active, ce qui signifie que les programmes sont résident en mémoire et donc toujours en cours d'exécution. HostScan/Secure Firewall Posture vérifie si un terminal est installé et s'il réside en mémoire, comme suit :

- Si le programme installé ne prend pas en charge l'analyse active, HostScan/Secure Firewall Posture signale la présence du logiciel. Le système DAP sélectionne les enregistrements DAP qui précisent le programme.
- Si le programme installé prend en charge l'analyse active et que l'analyse active est activée pour le programme, HostScan/Secure Firewall Posture signale la présence du logiciel. L'appareil de sécurité sélectionne à nouveau les enregistrements DAP qui précisent le programme.

- Si le programme installé prend en charge l'analyse active et que l'analyse active est désactivée pour le programme, HostScan/Secure Firewall Posture ignore la présence du logiciel. L'appareil de sécurité ne choisit pas les enregistrements DAP qui précisent le programme. De plus, la sortie de la commande **debug trace**, qui comprend de nombreuses informations sur DAP, n'indique pas la présence du programme, même s'il est installé.

Remarque Si vous effectuez une mise à niveau d'HostScan 4.3.x vers HostScan 4.6.x ou une version ultérieure, vous devez migrer tous les attributs de point terminal AV/AS/FW existants vers les attributs de point terminal AM/FW de remplacement correspondants avant d'effectuer la mise à niveau. Consultez le guide de migration AnyConnect HostScan de la version 4.3.x à la version 4.6.x pour obtenir une procédure de mise à niveau et de migration complète.

Définitions des attributs de point terminal

Les attributs de sélection de point terminal suivants sont disponibles pour une utilisation DAP. Le champ Attribute Name (Nom d'attribut) vous montre comment saisir chaque nom d'attribut dans une expression logique LUA utilisée dans la zone Advanced (Avancé) du volet Dynamic Access Policy Selection Criteria (Critères de sélection de la politique d'accès dynamique). La variable *label* identifie l'application, le nom de fichier, le processus ou l'entrée de registre.

Type d'attribut	Nom de l'attribut	Source	Valeur	Longueur maximale de la chaîne	Description
Antimalware	endpoint.am["*label*"].exists	Host ScanSecure Firewall Posture	vrai	—	Un programme de protection contre les programmes malveillants existe
	endpoint.am["*label*"].version		chaîne	32	Version
	endpoint.am["*label*"].description		chaîne	128	Description de l'antiprogramme malveillant
	endpoint.am["*label*"].lastupdate		nombre entier	—	Secondes depuis la mise à jour des définitions de programmes malveillants

Type d'attribut	Nom de l'attribut	Source	Valeur	Longueur maximale de la chaîne	Description
Pare-feu personnel	endpoint.pfw["*label*"].exists	Host Scan Secure Firewall Posture	vrai	—	Le pare-feu personnel existe
	endpoint.pfw["*label*"].version		chaîne	chaîne	Version
	endpoint.pfw["*label*"].description		chaîne	128	Description du pare-feu personnel
AnyConnect (Ne nécessite pas Host Scan Secure Firewall Posture)	Point terminaux.anyconnect. version du client	Point d'accès	version	—	version Secure Client
	Point terminaux.anyconnect. plateforme		chaîne	—	Système d'exploitation sur lequel Secure Client est installé
	Point terminaux.anyconnect. version de plateforme		version	64	Version du système d'exploitation sur lequel Secure Client est installé
	Point terminaux.anyconnect. type d'appareil		chaîne	64	Type de périphérique portable sur lequel Secure Client est installé
	endpoint.anyconnect. deviceuniqueid			64	ID unique du périphérique portable sur lequel Secure Client est installé
	endpoint.anyconnect. macaddress		chaîne	—	Adresse MAC du périphérique sur lequel Secure Client est installé L'adresse MAC doit être au format xx-xx-xx-xx-xx-xx, où chaque 'x' est un caractère hexadécimal
Application	endpoint.application. clienttype	Application	chaîne	—	Type de client : CLIENTLESS ANYCONNECT IPSEC L2TP

Type d'attribut	Nom de l'attribut	Source	Valeur	Longueur maximale de la chaîne	Description
Périphérique	endpoint.device. hostname	Point d'accès	chaîne	64	Nom d'hôte uniquement. Non FQDN
	endpoint.device.MAC		chaîne	—	Adresse MAC d'une carte d'interface réseau. Une seule adresse MAC par entrée L'adresse MAC doit être au format xxxx.xxxx.xxxx, où chaque x est un caractère hexadécimal.
	endpoint.device.id		chaîne	64	Numéro de série du BIOS Le format des numéros dépend du fabricant. Il n'y a aucune exigence de format
	endpoint.device.port		chaîne	—	État d'écoute du port TCP Vous pouvez définir un seul port par ligne Saisissez un entier entre 1 et 65 535.
	endpoint.device.protection_version		chaîne	64	Version de l'image HostScan/Secure Firewall Posture qu'ils utilisent
	endpoint.device. protection_extension		chaîne	64	Version de l'évaluation des points terminaux (OPSWAT)
Fichier	endpoint.file["*label*"].exists		vrai	—	Le fichier existe
	endpoint.file["label"]. endpointid				
	endpoint.file["*label*"]. lastmodified		nombre entier	—	Secondes écoulées depuis la dernière modification du fichier
	endpoint.file["*label*"]. crc.32		nombre entier	—	Hachage CRC32 du fichier

Type d'attribut	Nom de l'attribut	Source	Valeur	Longueur maximale de la chaîne	Description
NAC	endpoint.nac.status	NAC	chaîne	—	Chaîne d'état définie par l'utilisateur
Système d'exploitation	endpoint.os.version		chaîne	32	Système d'exploitation
	endpoint.os.servicepack		nombre entier	—	Service Pack pour Windows
Politique	endpoint.policy.location		chaîne	64	
Processus	endpoint. process["*label*"].exists		vrai	—	Le processus existe
	endpoint. process["*label*"].path		chaîne	255	Chemin complet du processus
Registre	endpoint. registry["*label*"].type		*dword string*	—	dword
	endpoint. registry["*label*"].value		chaîne	255	Valeur de l'entrée du registre
VLAN	endoint.vlan.type	CNA	chaîne	—	Type de VLAN : ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

Créer des critères de sélection DAP supplémentaires dans DAP à l'aide de LUA

Cette section fournit des informations sur la création d'expressions logiques pour les attributs AAA ou de point terminal. Sachez que cela nécessite une connaissance approfondie de LUA. Vous pouvez trouver des renseignements détaillés sur la programmation LUA à l'adresse suivante : http://www.lua.org/manual/5.1/manual.html.

Dans le champ Advanced (Avancé), vous saisissez du texte LUA de forme libre qui représente les opérations logiques AAA et/ou de sélection de point terminal. ASDM ne valide pas le texte que vous saisissez ici; il copie simplement ce texte dans le fichier de politique DAP, et l'ASA le traite en rejetant toute expression qu'il ne peut pas analyser.

Cette option est utile pour ajouter des critères de sélection autres que ceux possibles dans les zones des attributs AAA et de point terminal ci-dessus. Par exemple, bien que vous puissiez configurer l'ASA pour utiliser des attributs AAA qui satisfont un, tous ou aucun des critères spécifiés, les attributs de point terminal sont cumulatifs

et doivent tous être satisfaits. Pour permettre au périphérique de sécurité d'utiliser un attribut de point terminal ou un autre, vous devez créer les expressions logiques appropriées dans LUA et les saisir ici.

Les sections suivantes fournissent des instructions détaillées sur la création d'expressions LUA EVAL, ainsi que des exemples.

- Syntaxe pour la création d'expressions EVAL LUA, à la page 25
- Exemples d'expressions DAP EVAL, à la page 29
- Fonctions LUA supplémentaires, à la page 26

Syntaxe pour la création d'expressions EVAL LUA

Remarque Si vous devez utiliser le mode avancé, nous vous recommandons d'utiliser des expressions EVAL chaque fois que cela est possible pour des raisons de clarté, ce qui facilite la vérification du programme.

EVAL(<*attribute*> , <comparison>, {<*value*> | <*attribute*>}, [<type>])

<attribute>	Attribut AAA ou un attribut renvoyé par Cisco Secure Desktop, consultez Définitions des attributs de point terminal, à la page 21 pour les définitions d'attribut	
<comparison>	L'une des chaînes suivantes (guillemets requis)	
	« EQ »	égal à
	« NE »	n'est pas égal à
	« LT »	inférieur à
	« GT »	supérieur à
	« LE »	inférieur ou égal à
	« GE »	supérieur ou égal à
<value>	Une chaîne entre guillemets qui contient la valeur à laquelle comparer l'attribut	
<type>	L'une des chaînes suivantes (guillemets requis)	
	« string »	comparaison de chaînes sensibles à la casse
	""	comparaison de chaînes insensibles à la casse
	« integer »	comparaison de nombres, convertit les valeurs de chaîne en nombres
	« hex »	comparaison de nombres à l'aide de valeurs hexadécimales, convertit la chaîne hexadécimale en nombres hexadécimaux
	« version »	compare les versions du formulaire XHz où X, Y et Z sont des nombres

Procédures LUA pour HostScan 4.6 (et version ultérieure) et Secure Firewall Posture version 5

Script LUA pour « ANY » antiprogramme malveillant (endpoint.am) avec la dernière mise à jour

Utilisez le script LUA suivant pour vérifier s'il y a un produit ou un fournisseur de programmes malveillants « ANY » (endpoint.am). Des modifications peuvent s'appliquer pour s'adapter à un intervalle de dernière mise à jour différent. L'exemple suivant montre comment une dernière mise à jour doit avoir été effectuée en moins de 30 jours (2 592 000 secondes).

```
assert(function()
  for k,v in pairs(endpoint.am) do
    if(EVAL(v.activescan, "EQ", "ok", "string")and EVAL (v.lastupdate, "LT", "2592000",
"integer"))
     then
              return true
         end
  end
  return false
end)()
```

Script LUA pour pare-feu personnel « ANY » (tout)

Utilisez le script LUA suivant pour vérifier le produit ou le fournisseur de pare-feu « ANY » (endpoint.pfw) :

```
assert(function()
    for k,v in pairs(endpoint.pfw) do
         if (EVAL(v.enabled, "EQ", "ok", "string")) then
              return true
         end
    end
    return false
end)()
```

Fonctions LUA supplémentaires

Lorsque vous utilisez des politiques d'accès dynamiques, vous aurez peut-être besoin d'une plus grande flexibilité pour les critères de correspondance. Par exemple, vous pourriez vouloir appliquer une DAP différente en fonction des éléments suivants :

- CheckAndMsg est une fonction LUA que vous pouvez configurer DAP pour appeler. Il génère un message utilisateur en fonction d'une condition.
- Unité organisationnelle (OU) ou autre niveau de la hiérarchie pour l'objet utilisateur.
- Les noms de groupe qui suivent une convention de dénomination avec de nombreuses correspondances possibles peuvent nécessiter la possibilité d'utiliser un caractère générique.

Vous pouvez obtenir cette flexibilité en créant une expression logique LUA dans la section Avancé du volet DAP dans ASDM.

La fonction DAP CheckAndMsg

L'ASA affiche le message à l'utilisateur uniquement lorsque l'enregistrement DAP contenant la fonction LUA CheckAndMsg est sélectionné et entraîne la fin de la connexion.

La syntaxe de la fonction CheckAndMsg est la suivante :

```
CheckAndMsg(value, "<message string if value is true>", "<message string if value if false>")
```

Gardez à l'esprit les éléments suivants lors de la création des fonctions CheckAndMsg :

- CheckAndMsg renvoie la valeur transmise comme premier argument.
- Utilisez la fonction EVAL comme premier argument si vous ne souhaitez pas utiliser la comparaison de chaîne. Par exemple :

  ```
  (CheckAndMsg((EVAL(...)) , "true msg", "false msg"))
  ```

  CheckandMsg renvoie le résultat de la fonction EVAL, et l'appareil de sécurité l'utilise pour déterminer s'il faut choisir l'enregistrement DAP. Si l'enregistrement est sélectionné et entraîne la terminaison de la connexion, le périphérique de sécurité affiche le message approprié.

Exemple de correspondance basée sur OU

DAP peut utiliser de nombreux attributs renvoyés par un serveur LDAP dans une expression logique. Consultez la section sur le suivi DAP pour obtenir un exemple de sortie de celui-ci, ou exécutez un suivi DAP de débogage.

Le serveur LDAP renvoie le nom distinctif (DN) de l'utilisateur. Cela identifie implicitement l'endroit du répertoire où se trouve l'objet utilisateur. Par exemple, si le DN de l'utilisateur est CN=Example User, OU=Admins, dc=cisco, dc=com, cet utilisateur se trouve dans OU=Admins, dc=cisco, dc=com. Si tous les administrateurs se trouvent dans cette unité ou dans tout conteneur inférieur à ce niveau, vous pouvez utiliser une expression logique pour correspondre à ce critère comme suit :

```
assert(function()
   if ( (type(aaa.ldap.distinguishedName) == "string") and
        (string.find(aaa.ldap.distinguishedName, "OU=Admins,dc=cisco,dc=com$") ~= nil) )
then
       return true
   end
   return false
end)()
```

Dans cet exemple, la fonction string.find permet une expression régulière. Utilisez le caractère $ à la fin de la chaîne pour ancrer cette chaîne à la fin du champ distinguishedName.

Exemple d'appartenance à un groupe

Vous pouvez créer une expression logique de base pour la mise en correspondance de modèle de l'appartenance au groupe AD. Comme les utilisateurs peuvent être membres de plusieurs groupes, DAP analyse la réponse du serveur LDAP en entrées distinctes dans un tableau. Vous avez besoin d'une fonction avancée pour effectuer les opérations suivantes :

- Comparez le champ memberOf avec une chaîne (dans le cas où l'utilisateur n'appartient qu'à un seul groupe).
- Répétez l'itération sur chaque champ memberOf renvoyé si les données renvoyées sont de type « table ».

La fonction que nous avons écrite et testée à cette fin est indiquée ci-dessous. Dans cet exemple, si un utilisateur est membre d'un groupe se terminant par « -stu », il correspond à cette DAP.

```
assert(function()
   local pattern = "-stu$"
   local attribute = aaa.ldap.memberOf
   if ((type(attribute) == "string") and
       (string.find(attribute, pattern) ~= nil)) then
       return true
   elseif (type(attribute) == "table") then
       local k, v
       for k, v in pairs(attribute) do
           if (string.find(v, pattern) ~= nil) then
               return true
           end
       end
   end
   return false
end)()
```

Exemple de refus d'accès

Vous pouvez utiliser la fonction suivante pour refuser l'accès en l'absence d'un programme antimalware. Utilisez-le avec une DAP dont l'action est définie pour terminer.

```
assert(
    function()
for k,v in pairs(endpoint.am) do

        if (EVAL(v.exists, "EQ", "true", "string")) then

            return false

        end
    end
    return CheckAndMsg(true, "Please install antimalware software before connecting.", nil)
end)()
```

Si un utilisateur sans programme antimalware tente de se connecter, DAP affiche le message suivant :

```
Please install antimalware software before connecting.
```

Exemple d'authentification à certificats multiples

Vous pouvez définir un caractère générique pour le CN de l'émetteur avec l'authentification à certificats multiples dans les règles DAP.

Si vous avez configuré deux certificats émis à deux machines différentes par deux autorités de certification différentes (par exemple abc.cisco.com et xyz.cisco.com), la règle DAP doit avoir une condition d'authentification de plusieurs certificats dans laquelle le CN de l'émetteur est *.cisco.com ou cisco.com.

Vous pouvez utiliser la fonction suivante pour définir une règle DAP pour un certificat avec le caractère générique issuer_cn cisco.com pour les certificats utilisateur et machine :

```
assert(
 function()
  if ((string.find(endpoint.cert[1].issuer.cn[0], "cisco.com") ~= nil) and
   (string.find(endpoint.cert[2].issuer.cn[0], "cisco.com") ~= nil)) then
     return true;
 end
 return false;
end)()
```

Exemples d'expressions DAP EVAL

Étudiez ces exemples pour obtenir de l'aide dans la création d'expressions logiques dans LUA :

Description	Exemple
Vérifications LUA des points terminaux pour Windows 10	`(EVAL(endpoint.os.version,"EQ","Windows 10","string"))`
LUA de point terminal vérifie une correspondance sur les types de clients CLIENTLESS ou CVC.	`(EVAL(endpoint.application.clienttype,"EQ","CLIENTLESS") or EVAL(endpoint.application.clienttype, "EQ","CVC"))`
LUA de point terminal vérifie si un seul programme de protection contre les programmes malveillants Symantec Enterprise Protection est installé sur le PC de l'utilisateur et affiche un message si ce n'est pas le cas.	`(CheckAndMsg(EVAL(endpoint.am["538"].description,"NE","Symantec Endpoint Protection","string"),"Symantec Endpoint Protection was not found on your computer", nil))`
LUA de point terminal vérifie les versions de McAfee Endpoint Protection de 10 à 10.5.3 et les versions ultérieures à 10.6.	`(EVAL(endpoint.am["1637"].version,"GE","10","version") and EVAL(endpoint.am["1637"].version,"LT","10.5.4","version") or EVAL(endpoint.am["1637"].version,"GE","10.6","version"))`
LUA de point terminal vérifie si les définitions de l'antiprogramme malveillant McAfee ont été mises à jour au cours des 10 derniers jours (864000 s) et affiche un message si une mise à jour est nécessaire.	`(CheckAndMsg(EVAL(endpoint.am["1637"].lastupdate,"GT","864000","integer"),"Update needed! Please wait for McAfee to load the latest dat file.", nil))`

Description	Exemple
Vérifiez un correctif rapide spécifique après que le suivi de débogage DAP retourne : endpoint.os.windows.hotfix["KB923414"] = "true";	(CheckAndMsg(EVAL(endpoint.os.windows.hotfix["KB923414"],"NE","true"), "The required hotfix is not installed on your PC.",nil))

Vérifier les programmes de protection contre les programmes malveillants et fournir des messages

Vous pouvez configurer des messages afin que les utilisateurs finaux soient au courant des problèmes de leur logiciel anti-programme malveillant et soient en mesure de les résoudre. Si l'accès est autorisé, l'ASA affiche tous les messages générés dans le processus d'évaluation DAP sur la page du portail. Si l'accès est refusé, l'ASA collecte tous les messages pour le DAP qui ont causé l'état « terminer » et les affiche dans le navigateur sur la page de connexion.

L'exemple suivant montre comment utiliser cette fonctionnalité pour vérifier l'état de Symantec Endpoint Protection.

1. Copiez et collez l'expression LUA suivante dans le champ Advanced (Avancé) du volet Add/Edit Dynamic Access Policy (Ajouter/Modifier une politique d'accès dynamique) (cliquez sur la double flèche à l'extrémité droite pour développer le champ).

   ```
   (CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint
   Protection","string") and EVAL(endpoint.am["538"].activescan,"NE","ok","string") "Symantec
    Endpoint Protection is disabled. You must enable before being granted access", nil))
   ```

2. Dans le même champ Advanced (Avancé), cliquez sur le bouton **OR** (OU).
3. Dans la section Attributs d'accès ci-dessous, dans l'onglet **Action** le plus à gauche, cliquez sur **Terminate** (Terminer).
4. Connectez-vous à partir d'un PC sur lequel Symantec Endpoint Protection est installé, mais dont Symantec Endpoint Protection est désactivé. Le résultat attendu est que la connexion n'est pas autorisée et que l'utilisateur verra le message « Symantec Endpoint Protection est désactivé. Vous devez l'activer avant de vous accorder l'accès ».

Vérifier les programmes de protection contre les programmes malveillants et les définitions antérieures à 2 jours

Cet exemple vérifie la présence des programmes anti-programme malveillant Symantec et McAfee et si les définitions de virus sont antérieures à 2 jours (172 800 secondes). Si les définitions sont antérieures à 2 jours, l'ASA met fin à la session avec un message et des liens pour la correction. Pour effectuer cette tâche, procédez comme suit.

1. Copiez et collez l'expression LUA suivante dans le champ Advanced (Avancé) du volet Add/Edit Dynamic Access Policy (Ajouter/Modifier une politique d'accès dynamique) :

   ```
   (CheckAndMsg(EVAL(endpoint.am["538"].description,"EQ","Symantec Endpoint
   Protection","string") and EVAL(endpoint.am["538"].lastupdate,"GT","172800","integer"),
   "Symantec Endpoint Protection Virus Definitions are Out of Date. You must run LiveUpdate
    before being granted access", nil)) or
   (CheckAndMsg(EVAL(endpoint.am["1637"].description,"EQ","McAfee Endpoint
   Security","string") and EVAL(endpoint.am["1637"].lastupdate,"GT","172800","integer"),
   "McAfee Endpoint Security Virus Definitions are Out of Date. You must update your McAfee
    Virus Definitions before being granted access", nil))
   ```

2. Dans le même champ Advanced (Avancé), cliquez sur **AND** (ET).
3. Dans la section Attributs d'accès ci-dessous, dans l'onglet Action (Action) le plus à gauche, cliquez sur **Terminate** (Terminer).
4. Connectez-vous à partir d'un PC doté de programmes anti-programme malveillant Symantec et McAfee avec des versions antérieures à 2 jours.

   Le résultat attendu est que la connexion n'est pas autorisée et qu'un message est présenté à l'utilisateur indiquant que les définitions de virus sont obsolètes.

Configurer les attributs de la politique d'accès DAP et d'autorisation

Cliquez sur chacun des onglets et configurez les champs contenus.

Procédure

Étape 1 Sélectionnez l'onglet **Action** pour spécifier le traitement spécial à appliquer à une connexion ou une session spécifique.

- Continue (Continuer) : cliquez pour appliquer les attributs de politique d'accès à la session.
- Quarantine (Quarantaine) : au moyen de la mise en quarantaine, vous pouvez restreindre un client particulier qui a déjà un tunnel établi par l'intermédiaire d'un VPN. L'ASA applique des listes de contrôle d'accès restreintes à une session pour former un groupe restreint, en fonction de l'enregistrement DAP sélectionné. Lorsqu'un point terminal n'est pas conforme à une politique définie par l'administrateur, l'utilisateur peut toujours accéder aux services de correction, mais des restrictions sont imposées à l'utilisateur. Après la correction, l'utilisateur peut se reconnecter, ce qui invoque une nouvelle évaluation de la posture. Si cette évaluation réussit, l'utilisateur se connecte. Ce paramètre nécessite une version Secure Client qui prend en charge les fonctionnalités de Cisco Secure Client/.
- Terminate (Mettre fin) : cliquez pour mettre fin à la session.
- User Message (Message utilisateur) : saisissez un message texte à afficher sur la page du portail lorsque cet enregistrement DAP est sélectionné. Maximum 490 caractères. Un message utilisateur s'affiche sous forme d'orbe jaune. Lorsqu'un utilisateur se connecte, il clignote trois fois pour attirer l'attention, puis il reste fixe. Si plusieurs enregistrements DAP sont sélectionnés et que chacun d'entre eux comporte un message d'utilisateur, tous les messages d'utilisateur s'affichent.

  Vous pouvez inclure des URL ou d'autres types de texte intégrés, ce qui nécessite l'utilisation des balises HTML appropriées. Par exemple : tous les sous-traitants lisent Instructions pour connaître la procédure de mise à niveau de votre logiciel anti-programme malveillant.

Étape 2 Sélectionnez l'onglet **Network ACL Filters** (Filtres d'ACL réseau) pour configurer les listes de contrôle d'accès réseau à appliquer à cet enregistrement DAP.

Une liste de contrôle d'accès pour DAP peut contenir des règles d'autorisation ou de refus, mais pas les deux. Si une liste de contrôle d'accès contient des règles d'autorisation et de refus, l'ASA la rejette.

- Liste déroulante Network ACL (ACL réseau) : sélectionnez des listes de contrôle d'accès réseau déjà configurées à ajouter à cet enregistrement DAP. Les listes de contrôle d'accès peuvent être n'importe quelle combinaison de règles d'autorisation et de refus. Ce champ prend en charge les listes de contrôle d'accès unifiées qui peuvent définir des règles d'accès pour le trafic réseau IPv4 et IPv6.
- **Manage** (Gérer) : cliquez pour ajouter, modifier et supprimer des listes de contrôle d'accès réseau.
- **Network ACL list** (Liste d'ACL réseau) : affiche les listes d'ACL réseau pour cet enregistrement DAP.
- **Add** (Ajouter) : cliquez pour ajouter l'ACL réseau sélectionnée dans la liste déroulante à la liste Network ACLs (ACL réseau) sur la droite.
- **Delete** (Supprimer) : cliquez pour supprimer une liste de contrôle d'accès réseau en surbrillance dans la liste Network ACLs (ACL réseau). Vous ne pouvez pas supprimer une liste de contrôle d'accès de l'ASA, sauf si vous l'avez d'abord supprimée des enregistrements DAP.

Étape 3 Sélectionnez l'onglet **Web-Type ACL Filters (clientless) (**Filtres d'ACL de type Web [sans client]) pour configurer les listes de contrôle d'accès de type Web à appliquer à cet enregistrement DAP. Une liste de contrôle d'accès pour DAP ne peut contenir que des règles d'autorisation ou de refus. Si une liste de contrôle d'accès contient des règles d'autorisation et de refus, l'ASA la rejette.

- Liste déroulante **Web-Type ACL** (ACL de type Web) : sélectionnez des listes de contrôle d'accès de type Web déjà configurées à ajouter à cet enregistrement DAP. Les listes de contrôle d'accès peuvent être n'importe quelle combinaison de règles d'autorisation et de refus.
- **Manage** (Gérer) : cliquez pour ajouter, modifier et supprimer des listes de contrôle d'accès de type Web.
- **Web-Type ACL list** (Liste d'ACL de type Web) : affiche les listes de contrôle d'accès de type Web pour cet enregistrement DAP.
- **Add** (Ajouter) : cliquez pour ajouter l'ACL de type Web sélectionnée dans la liste déroulante à la liste Web-Type ACLs (ACL de type Web) sur la droite.
- **Delete** (Supprimer) : cliquez pour supprimer une liste de contrôle d'accès de type Web dans la liste Web-Type ACLs (ACL de type Web). Vous ne pouvez pas supprimer une liste de contrôle d'accès de l'ASA, sauf si vous l'avez d'abord supprimée des enregistrements DAP.

Étape 4 Sélectionnez l'onglet **Functions** (Fonctions) pour configurer l'entrée et la navigation dans le serveur de fichiers, le proxy HTTP et l'entrée d'URL pour l'enregistrement DAP.

- **File Server Browsing** (Navigation dans le serveur de fichiers) : active ou désactive la navigation CIFS pour les serveurs de fichiers ou les fonctionnalités partagées.

  La navigation nécessite NBNS (Master Browser ou WINS). S'il échoue ou n'est pas configuré, nous utilisons le DNS. La fonctionnalité de navigation CIFS ne prend pas en charge l'internationalisation.
- **File Server Entry** (Entrée du serveur de fichiers) : permet ou interdit à un utilisateur de saisir les chemins et les noms du serveur de fichiers sur la page du portail. Lorsque cette option est activée, place le tiroir d'entrée du serveur de fichiers sur la page du portail. Les utilisateurs peuvent saisir directement les noms de chemin d'accès aux fichiers Windows. Ils peuvent télécharger, modifier, supprimer, renommer et déplacer des fichiers. Ils peuvent également ajouter des fichiers et des dossiers. Les partages doivent également être configurés pour l'accès des utilisateurs sur les serveurs Windows applicables. Il se peut que les utilisateurs doivent être authentifiés avant d'accéder aux fichiers, en fonction des exigences du réseau.

- **HTTP Proxy** (Proxy HTTP) : affecte le transfert d'un proxy HTTP vers le client. Le proxy est utile pour les technologies qui interfèrent avec une transformation appropriée du contenu, telles que Java, ActiveX et Flash. Il contourne la gestion tout en assurant l'utilisation continue du périphérique de sécurité. Le proxy transféré modifie automatiquement l'ancienne configuration du navigateur et redirige toutes les requêtes HTTP et HTTPS vers la nouvelle configuration du proxy. Il prend en charge virtuellement toutes les technologies côté client, y compris HTML, CSS, JavaScript, VBScript, ActiveX et Java. Le seul navigateur qu'il prend en charge est Microsoft Internet Explorer.
- **URL Entry** (Entrée URL) : autorise ou empêche un utilisateur d'entrer des URL HTTP ou HTTPS sur la page du portail. Si cette fonctionnalité est activée, les utilisateurs peuvent saisir des adresses Web dans la zone de saisie d'URL.

L'utilisation du VPN SSL ne garantit pas que la communication avec chaque site est sécurisée. Le VPN SSL garantit la sécurité de la transmission des données entre le PC ou le poste de travail de l'utilisateur distant et l'ASA sur le réseau de l'entreprise. Si un utilisateur accède ensuite à une ressource Web non HTTPS (située sur Internet ou sur le réseau interne), la communication de l'ASA d'entreprise avec le serveur Web de destination n'est pas sécurisée.

Dans une connexion VPN sans client, l'ASA agit comme proxy entre le navigateur Web de l'utilisateur final et les serveurs Web cibles. Lorsqu'un utilisateur se connecte à un serveur Web compatible avec le protocole SSL, l'ASA établit une connexion sécurisée et valide le certificat SSL du serveur. Le navigateur de l'utilisateur final ne reçoit jamais le certificat présenté, il ne peut donc pas examiner et valider le certificat. La mise en œuvre actuelle du VPN SSL ne permet pas la communication avec des sites qui présentent des certificats expirés. L'ASA n'effectue pas non plus la validation du certificat d'autorité de certification de confiance. Par conséquent, les utilisateurs ne peuvent pas analyser le certificat d'un serveur Web compatible avec le protocole SSL avant de communiquer avec celui-ci.

Pour limiter l'accès Internet pour les utilisateurs, choisissez Disable (Désactiver) dans le champ URL Entry (Entrée URL). Cela empêche les utilisateurs de VPN SSL de surfer sur le Web pendant une connexion VPN sans client.

- **Unchanged** (Non modifié) : cliquez pour utiliser les valeurs de la stratégie de groupe qui s'applique à cette session.
- **Enable/Disable** (Activer/Désactiver) : cliquez pour activer ou désactiver la fonctionnalité.
- **Auto-start** (Démarrage automatique) : cliquez pour activer le proxy HTTP et pour que l'enregistrement DAP démarre automatiquement les applets associées fonctionnalités.

Étape 5 Sélectionnez l'onglet **Port Forwarding Lists** pour configurer les listes de transfert de port pour les sessions utilisateur.

Le transfert de port permet aux utilisateurs distants du groupe d'accéder à des applications client/serveur qui communiquent sur les ports TCP/IP connus et fixes. Les utilisateurs distants peuvent utiliser des applications clientes installées sur leur ordinateur local et accéder en toute sécurité à un serveur distant qui prend en charge cette application. Cisco a testé les applications suivantes : Windows Terminal Services, Telnet, Secure FTP (FTP sur SSH), Perforce, Outlook Express et Lotus Notes. D'autres applications basées sur TCP peuvent également fonctionner, mais Cisco ne les a pas testées.

Remarque
Le transfert de port ne fonctionne pas avec certaines versions SSL/TLS.

Mise en garde
Assurez-vous que Sun Microsystems Java Runtime Environment (JRE) est installé sur les ordinateurs distants pour prendre en charge le transfert de port (accès aux applications) et les certificats numériques.

- **Port Forwarding** (Transfert de port) : sélectionnez une option pour les listes de transfert de port qui s'appliquent à cet enregistrement DAP. Les autres attributs dans ce champ ne sont activés que lorsque vous définissez le transfert de port sur activé ou sur démarrage automatique.
- **Unchanged** (Non modifié) : cliquez pour supprimer les attributs de la configuration en cours d'exécution.
- **Enable/Disable** (Activer/Désactiver) : cliquez pour activer ou désactiver le transfert de port.
- **Auto-start** (Démarrage automatique) : cliquez pour activer le transfert de port et pour que l'enregistrement DAP démarre automatiquement les applets de transfert de port associées listes de transfert de port.
- **Liste déroulante Port Forwarding List** (Liste de transfert de port) : sélectionnez les listes de transfert de port déjà configurées à ajouter à l'enregistrement DAP.
- **Nouveau...** : cliquez pour configurer de nouvelles listes de transfert de port.
- **Port Forwarding Lists** (sans étiquette) : affiche les listes de transfert de port pour l'enregistrement DAP.
- **Add** (Ajouter : cliquez pour ajouter la liste de transfert de port sélectionnée dans la liste déroulante à la liste Port Forwarding (Transfert de port) sur la droite.
- **Delete** (Supprimer) : cliquez pour supprimer la liste de transfert de port sélectionnée dans la liste Port Forwarding (Transfert de port). Vous ne pouvez pas supprimer une liste de transfert de port de l'ASA, sauf si vous l'avez d'abord supprimée des enregistrements DAP.

Étape 6 Sélectionnez l'onglet **Bookmarks** (Repères) pour configurer les signets pour certaines URL de session utilisateur.

- **Enable bookmarks** (Activer les signets) : cliquez pour les activer. Lorsque cette option n'est pas cochée, aucun signet ne s'affiche dans la page du portail pour la connexion.
- **Liste déroulante Bookmark** (Signet) : choisissez des signets déjà configurés à ajouter à l'enregistrement DAP.
- **Manage** (Gérer)... : cliquez pour ajouter, importer, exporter et supprimer des signets.
- **Bookmarks** (sans étiquette) : affiche les listes d'URL pour l'enregistrement DAP.
- **Add>>** (Ajouter>>) : cliquez pour ajouter le signet sélectionné dans la liste déroulante à la zone d'URL sur la droite.
- **Delete** (Supprimer) : cliquez pour supprimer le signet sélectionné dans la zone de liste d'URL. Vous ne pouvez pas supprimer un signet dans l'ASA, sauf si vous l'avez d'abord supprimé des enregistrements DAP.

Étape 7 Sélectionnez l'onglet **Access Method** (Méthode d'accès) pour configurer le type d'accès à distance autorisé.

- **Unchanged** (Non modifié) : continuez avec la méthode d'accès à distance actuelle.
- **Secure Client** : connexion à l'aide du module VPN AnyConnect de Cisco Secure Client

  .
- **Web-Portal** (Portail Web) : connexion avec le VPN sans client.
- **Both-default-Web-Portal** (Les deux par défaut—Portail Web) : connexion sans client ou via Secure Client, avec une valeur par défaut sans client.

- **Both-default-Secure Client** (Les deux par défaut) : connexion sans client ou via Secure Client, avec une valeur par défaut Secure Client.

Étape 8 Sélectionnez l'onglet **Secure Client** pour choisir l'état de l'indicateur VPN toujours activé.

- Always-On VPN for (VPN toujours activé pour) Secure Client :déterminez si le paramètre d'indicateur VPN toujours activé dans le profil de service Secure Client est inchangé, désactivé ou si le paramètre de profil Secure Client doit être utilisé.

  Ce paramètre nécessite une version de l'appareil Cisco Web Security qui fournit une prise en charge des licences de solution de mobilité sécu risée pour le module VPN AnyConnect de Cisco Secure Client. Il nécessite également une version Secure Client qui prend en charge les fonctionnalités de la « Secure Mobility Solution » (solution de mobilité sécurisée). Reportez-vous au *Guide de l'administrateur des clients VPN Cisco AnyConnect* pour obtenir plus d'informations.

Étape 9 Sélectionnez l'onglet **Custom Attributes** (Attributs personnalisés) Secure Client pour afficher et associer les attributs personnalisés définis précédemment à cette politique. Vous pouvez également définir des attributs personnalisés, puis les associer à cette politique.

Les attributs personnalisés sont envoyés à et utilisés par Secure Clientpour configurer des fonctionnalités telles que la mise à niveau retardée. Un attribut personnalisé a un type et une valeur nommée. Le type de l'attribut est défini en premier, puis une ou plusieurs valeurs nommées de ce type peuvent être définies. Pour en savoir plus sur les attributs personnalisés à configurer pour une fonctionnalité, consultez le *Guide de l'administrateur de Cisco* pour la version Secure Client que vous utilisez.

Les attributs personnalisés peuvent être prédéfinis dans **Configuration > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès au réseau [client]) > Advanced (Avancé) > Custom Attributes (Attributs personnalisés)** Secure Client et **Custom Attribute Names** (Noms d'attributs personnalisés Secure Client). Les attributs personnalisés prédéfinis sont utilisés par les politiques d'accès dynamique et les stratégies de groupe.

Configurer l'autorisation SAML

Vous pouvez configurer les sélections d'autorisation SAML et de stratégies de groupe à l'aide de DAP, sans avoir à faire appel à un serveur externe (RADIUS ou LDAP) pour récupérer les attributs d'autorisation.

Le fournisseur d'identité SAML peut être configuré pour envoyer des attributs d'autorisation en plus des réclamations d'authentification. Le composant fournisseur de services SAML dans ASA interprète les déclarations SAML et effectue des sélections d'autorisations ou de stratégies de groupe en fonction des déclarations reçues. Les attributs d'assertion sont traités à l'aide des règles DAP configurées par ASDM.

L'attribut de stratégie de groupe doit utiliser le nom d'attribut **cisco_group_policy**. Cet attribut ne dépend pas de la configuration du DAP. Toutefois, si une DAP est configurée, elle peut être utilisée dans la politique DAP.

Sélection de stratégie de groupe

Lorsqu'un attribut **cisco_group_policy** est reçu, la valeur correspondante est utilisée pour sélectionner la stratégie de groupe de connexion.

Lorsqu'une connexion est établie, les informations de stratégie de groupe peuvent être extraites de plusieurs sources et combinées pour former une stratégie de groupe efficace qui est appliquée à la connexion.

Les scénarios suivants sont possibles tout en combinant les informations de stratégie de groupe reçues :

Stratégie de groupe reçue dans l'authentification SAML, autorisation NON configurée

Dans ce scénario, la stratégie de groupe effective est déterminée comme suit dans l'ordre de priorité décroissante :

1. Stratégie de groupe spécifiée dans l'attribut SAML.
2. La stratégie de groupe est spécifiée dans le groupe de tunnels.
3. Stratégie de groupe par défaut.

Stratégie de groupe reçue dans l'authentification SAML, autorisation configurée

Dans ce scénario, la stratégie de groupe effective est déterminée comme suit dans l'ordre de priorité décroissante :

1. Stratégie de groupe spécifiée dans les attributs d'autorisation.
2. Stratégie de groupe d'utilisateurs : utilisez la valeur renvoyée par le serveur d'autorisation, le cas échéant.
3. Stratégie de groupe d'utilisateurs : utilisez la valeur renvoyée dans l'attribut SAML.
4. Stratégie de groupe spécifiée dans le groupe de tunnels.
5. Stratégie de groupe par défaut.

Procédure

Étape 1 Dans ASDM, sélectionnez **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies** > **Add/Edit Dynamic Access Policy** (Configuration > VPN d'accès à distance > Accès au réseau [client] > Politiques d'accès dynamique > Ajouter/Modifier une politique d'accès dynamique).

Étape 2 Dans la zone de sélection des attributs AAA, cliquez sur **Ajouter** (Ajouter).

a) Dans la liste déroulante **AAA Attribute Type** (Type d'attribut AAA), sélectionnez SAML.
b) Précisez *memberOf* comme **Attribute ID** (ID d'attribut).
c) Saisissez la valeur de l'attribut **Value** (Valeur) de *memberOf* ou cliquez sur **Get AD Group** (Obtenir le groupe AD) si les groupes de serveurs AD sont configurés.

Pour configurer des groupes de serveurs AD supplémentaires, accédez à **Configuration** > **Remote Access VPN (VPN d'accès distant)** > **AAA/Local Users (AAA/Utilisateurs locaux)** > **AAA Server Groups (Groupes de serveurs AAA)**.

Pour configurer les attributs de sélection de stratégie de groupe, sélectionnez les paramètres suivants dans la même politique DAP ou dans une autre politique DAP, selon les besoins :

- **AAA Attribute Type** (Type d'attribut AAA : SAML
- **Attribute ID** (ID d'attribut) : cisco_group_policy
- **Value** (Valeur) : Nom de la stratégie de groupe

Étape 3 Cliquez sur **OK**.

Étape 4 Cliquez sur **OK** pour enregistrer la politique DAP.

Effectuer un suivi DAP

Un suivi DAP affiche les attributs de point terminal DAP pour tous les périphériques connectés.

Procédure

Étape 1 Connectez-vous à l'ASA à partir d'un terminal SSH et passez en mode d'exécution privilégié.

En mode d'exécution privilégié, l'ASA invite : `hostname#`.

Étape 2 Activez les débogages DAP pour afficher tous les attributs DAP de la session dans la fenêtre du terminal :

```
hostname# debug dap trace
endpoint.anyconnect.clientversion="0.16.0021";
endpoint.anyconnect.platform="apple-ios";
endpoint.anyconnect.platformversion="4.1";
endpoint.anyconnect.devicetype="iPhone1,2";
endpoint.anyconnect.deviceuniqueid="dd13ce3547f2fa1b2c3d4e5f6g7h8i9j0fa03f75";
```

Étape 3 (Facultatif) Pour rechercher dans la sortie du suivi DAP, envoyez la sortie de la commande à un journal système. Pour en savoir plus sur la journalisation sur l'ASA, consultez *Configurer la journalisation* dans le *Guide de configuration ASDM des opérations générales Cisco ASA*.

Exemples de DAP

Utiliser DAP pour définir les ressources réseau

Cet exemple montre comment configurer les politiques d'accès dynamiques comme méthode de définition des ressources réseau pour un utilisateur ou un groupe. La politique DAP nommée Trusted_VPN_Access permet l'accès VPN sans client et l'accès au module VPN AnyConnect de Cisco Secure Client. La politique nommée Untrusted_VPN_Access autorise uniquement l'accès VPN sans client.

Procédure

Étape 1 Dans ASDM, accédez à **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Clientless SSL VPN Access (Accès VPN SSL sans client)** > **Dynamic Access Policies (Politiques d'accès dynamique)** > **Add/Edit Dynamic Access Policy (Ajouter/Modifier une politique d'accès dynamique)** > **Endpoint (Point terminal)**.

Étape 2 Configurez les attributs suivants pour chaque politique :

Attribut	Trusted_VPN_Access	Untrusted_VPN_Access
Politique de type d'attribut de point terminal	Fiable	Non fiable
Attributs de point terminal	ieexplore.exe	—
Évaluation avancée du point terminal	AntiVirus= attribut McAfee	
Emplacement CSD	Fiable	Non fiable
LDAP memberOf	Ingénierie, Responsables	Fournisseurs
ACL		ACL de type Web
Accès	**Secure Client** *et* **portail Web**	**Portail Web**

Utiliser DAP pour appliquer une ACL WebVPN

DAP peut appliquer directement un sous-ensemble d'attributs de politique d'accès, y compris les ACL réseau (pour IPsec et Secure Client), les listes d'URL et les fonctions. Elle ne peut pas appliquer directement, par exemple, une bannière ou la liste de tunnels fractionnés, que les stratégies de groupe appliquent. Les onglets Access Policy Attributes (Attributs de politique d'accès) dans le volet Add/Edit Dynamic Access Policy (Ajouter/modifier une politique d'accès dynamique) fournissent un menu complet des attributs appliqués directement par DAP.

Active Directory/LDAP stocke l'appartenance aux stratégies de groupe des utilisateurs sous la forme de l'attribut « memberOf » dans l'entrée utilisateur. Définissez une DAP de sorte que, pour un utilisateur du groupe AD (memberOf) = Engineering, l'ASA applique une ACL de type Web configurée.

Procédure

Étape 1 Dans ASDM, accédez au volet Add AAA Attributes (Ajouter des attributs AAA), **Configuration** > **Remote Access VPN (VPN d'accès à distance)** > **Clientless SSL VPN Access (Accès VPN SSL sans client)** > **Dynamic Access Policies (Politiques d'accès dynamique)** > **Add/Edit Dynamic Access Policy (Ajouter/modifier une politique d'accès dynamique)** > **section** > **AAA Attributes (Attributs AAA)** > **Add AAA Attribute (Ajouter un attribut AAA)**.

Étape 2 Pour le type d'attribut AAA, utilisez la liste déroulante pour choisir **LDAP**.

Étape 3 Dans le champ Attribute ID, saisissez memberOf, exactement comme vous le voyez ici. La casse est importante.

Étape 4 Dans le champ Value (Valeur), utilisez la liste déroulante pour choisir =, puis dans le champ adjacent, saisissez Engineering.

Étape 5 Dans la zone Access Policy Attributes (Attributs de politique d'accès) du volet, cliquez sur l'onglet Web-Type ACL Filters (Filtres ACL de type Web).

Étape 6 Utilisez la liste déroulante Web-Type ACL pour choisir l'ACL que vous souhaitez appliquer aux utilisateurs du groupe AD (memberOf) = Engineering.

Effectuer des vérifications CSD et appliquer les politiques via DAP

Cet exemple crée une DAP qui vérifie qu'un utilisateur appartient à deux groupes AD/LDAP spécifiques (Engineering et Employees) et à un groupe de tunnel ASA spécifique. Il applique ensuite une liste de contrôle d'accès à l'utilisateur.

Les listes de contrôle d'accès que DAP applique contrôlent l'accès aux ressources. Elles remplacent toute liste de contrôle d'accès définie dans la stratégie de groupe sur l'ASA. En outre, l'ASA applique les règles d'hérédité de Stratégie de groupe AAA et les attributs habituels pour ceux que DAP ne définit pas ou ne contrôle pas, comme les listes de tunnellisation fractionnée, les bannières et le DNS.

Procédure

Étape 1 Dans ASDM, allez au volet Ajouter des attributs AAA, **Configuration** > **Accès VPN à distance** > **Accès VPN SSL sans client** > **Politiques d'accès dynamique** > **Ajouter/Modifier une politique d'accès dynamique** > **section Attributs AAA** > **Ajouter un attribut AAA**.

Étape 2 Pour le type d'attribut AAA, utilisez la liste déroulante pour choisir LDAP.

Étape 3 Dans le champ Attribute ID (ID d'attribut), saisissez memberOf, exactement comme vous le voyez ici. La casse est importante.

Étape 4 Dans le champ Value (Valeur), utilisez la liste déroulante pour choisir =, puis dans le champ adjacent, saisissez Engineering.

Étape 5 Dans le champ Attribute ID (ID d'attribut), saisissez memberOf, exactement comme vous le voyez ici. La casse est importante.

Étape 6 Dans le champ Value (Valeur), utilisez la liste déroulante pour choisir =, puis dans le champ adjacent, saisissez Employees (Employés).

Étape 7 Pour le type d'attribut AAA, utilisez la liste déroulante pour choisir Cisco.

Étape 8 Cochez la case Tunnel group (Groupe de tunnels), utilisez la liste déroulante pour choisir =, puis dans la liste déroulante adjacente, choisissez le groupe de tunnels approprié (politique de connexion).

Étape 9 Dans l'onglet Network ACL Filters (Filtres ACL réseau) de la zone Access Policy Attributes (Attributs de politique d'accès), choisissez les listes de contrôle d'accès à appliquer aux utilisateurs qui répondent aux critères DAP définis dans les étapes précédentes.

Utiliser DAP pour vérifier la sécurité des jetons de session

Lorsque l'ASA authentifie une demande de connexion VPN à partir de Secure Client, l'ASA renvoie un jeton de session au client. À partir d'AnyConnect 4.9 (MR1), l'ASA et Secure Client prennent en charge un mécanisme qui offre une sécurité renforcée pour le jeton de session. Vous devez configurer une DAP pour vous assurer que Secure Client prend en charge la sécurité par jeton de session.

Utilisez cette DAP avec les paramètres d'attributs de point terminal et le script LUA pour rejeter les tentatives de connexion à partir de versions Secure Client qui ne prennent pas en charge la sécurité par jeton.

Procédure

Étape 1 Dans ASDM, sélectionnez **Configuration** > **Remote Access VPN** > **Network (Client) Access** > **Dynamic Access Policies** > **Add/Edit Dynamic Access Policy** (Configuration > VPN d'accès à distance > Accès au réseau [client] > Politiques d'accès dynamique > Ajouter/Modifier une politique d'accès dynamique).

Étape 2 Dans la zone de sélection des attributs de terminal, cliquez sur **Add** (Ajouter).

a) Dans la liste déroulante **Endpoint Attribute Type** (Type d'attribut de terminal), sélectionnez Application.
b) Pour **Client Type** (Type de client), sélectionnez l'opérateur equals (=) [égal à (=)], puis sélectionnez une valeur Secure Client dans la liste déroulante.
c) Cliquez sur **OK**.

Étape 3 Configurez les critères de sélection **Advanced** (Avancés) :

a) Sélectionnez l'opérateur **AND** (ET).
b) Ajoutez l'expression logique **Add the Logical Expression** (Ajouter l'expression logique).

```
(type(endpoint.anyconnect.session_token_security)~="string" or
EVAL(endpoint.anyconnect.session_token_security,"NE","true","string"))
```

Étape 4 Dans la zone **Action**, sélectionnez **Terminate** (Terminer).

Étape 5 Ajoutez un User Message (Message utilisateur) facultatif et cliquez sur **OK**.

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.