Politiques d'accès dynamique

Les politiques d'accès dynamique (DAP) vous permettent de configurer une autorisation qui traite de la dynamique des environnements VPN. 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.

À propos de la politique d'accès dynamique Cisco Secure Firewall Threat Defense

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 tentatives de connexion 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.

Vous pouvez créer 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'appartenances à plusieurs groupes et de sécurité des points terminaux. défense contre les menaces accorde l'accès à un utilisateur particulier pour une session particulière en fonction des politiques que vous définissez. Le périphérique défense contre les menaces génère une DAP lors de l'authentification de l'utilisateur 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, le périphérique applique l'enregistrement DAP au tunnel ou à la session d'utilisateur.

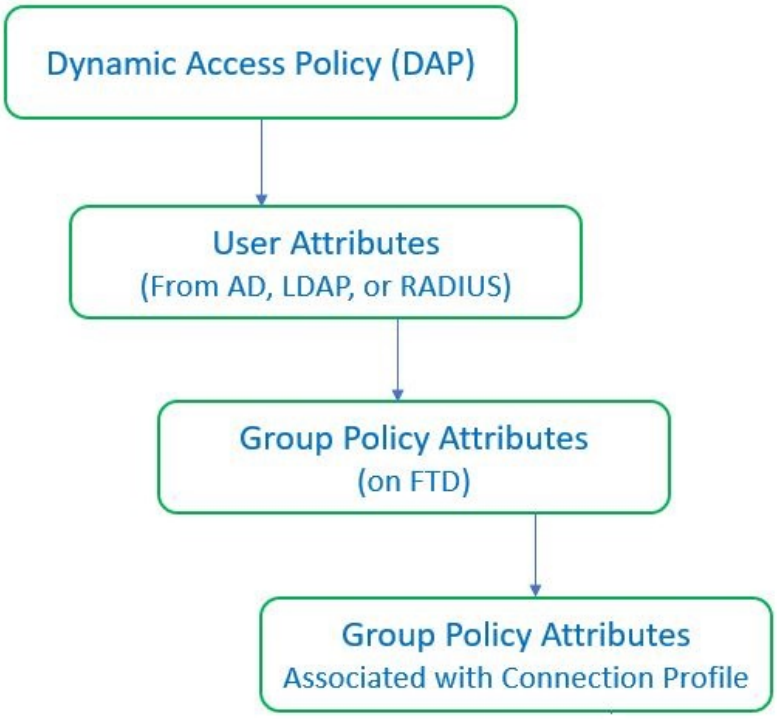
Hiérarchisation de l'application des politiques des autorisations et des attributs dans Défense contre les menaces

Le périphérique défense contre les menaces prend en charge l'application d'attributs d'autorisation d'utilisateur, également appelés droits ou autorisations d'utilisateur, aux connexions VPN. Les attributs sont appliqués à partir d'une DAP sur le défense contre les menaces , le serveur d'authentification externe et/ou le serveur d'autorisation AAA (RADIUS) ou à partir d'une politique de groupe sur le périphérique défense contre les menaces .

Si le périphérique défense contre les menaces reçoit des attributs de toutes les sources, il évalue, fusionne et applique les attributs à la politique d'utilisateur. S'il y a des conflits entre les attributs provenant du DAP, du serveur AAA ou de la politique de groupe, les attributs du DAP prévalent toujours.

Le périphérique défense contre les menaces applique les attributs dans l'ordre suivant :

Illustration 1 : Flux d'application des politiques



1. **Attributs DAP sur FTD** : les attributs DAP prévalent sur tous les autres.
2. **Attributs de l'utilisateur sur le serveur AAA externe** : le serveur renvoie ces attributs une fois l'authentification ou l'autorisation de l'utilisateur réussie.
3. **Politique de groupe configurée sur FTD** : si un serveur RADIUS renvoie la valeur de l'attribut de classe RADIUS IETF-Class-25 (OU = group-policy) pour l'utilisateur, le périphérique défense contre les menaces place l'utilisateur dans la politique de groupe du même nom et applique les attributs de la politique de groupe qui ne sont pas renvoyés par le serveur.

4. **Politiques de groupe affectées par le profil de connexion (également appelées groupes de tunnels)** : le profil de connexion contient les paramètres préliminaires pour la connexion et comprend une politique de groupe par défaut qui est appliquée à l'utilisateur avant l'authentification.

Remarque Le périphérique défense contre les menaces ne prend pas en charge la transmission des attributs du système par défaut de la politique de groupe par défaut, *DfltGrpPolicy*. Pour la session utilisateur, le périphérique utilise les attributs de la politique de groupe que vous affectez au profil de connexion, sauf si les attributs utilisateur ou la politique de groupe du serveur AAA les remplacent.

Licences des politiques d'accès dynamique

Défense contre les menaces doit comporter l'une des licences Secure Client (services client sécurisés) suivantes :

- Secure Client Premier
- Secure Client Advantage
- VPN client sécurisé uniquement

La licence Essentielle doit permettre l'utilisation de fonctionnalités contrôlées par l'exportation.

Conditions préalables à la politique d'accès dynamique

Tableau 1 :

Type de préalable	Description

Licence	• Défense contre les menaces doit avoir au moins une des licences Secure Client (services client sécurisés) suivantes :
	  • Secure Client Premier
	  • Secure Client Advantage
	  • VPN client sécurisé uniquement
	• La licence défense contre les menaces Essentielle doit autoriser la fonctionnalité dont l'exportation est contrôlée.

Type de préalable	Description
Configurations	Pour en savoir plus sur les conditions préalables à l'installation de DAP, consultez la section *Politiques d'accès dynamique Cisco Secure Firewall Threat Defense* du *Guide de configuration du centre de gestion Cisco Firepower Management Center*. Pour en savoir plus sur les conditions préalables et la configuration du VPN d'accès à distance, consultez la section *Cisco Secure Firewall Threat DefenseVPN d'accès à distance* du *Guide de configuration du centre de gestion Cisco Firepower Management Center*.

Lignes directrices et limites pour les politiques d'accès dynamique

- La correspondance des attributs AAA dans une DAP ne fonctionnera que si un serveur AAA est configuré pour renvoyer les attributs corrects lors de l'authentification ou de l'autorisation d'une session VPN d'accès à distance.
- La version minimale de Secure Client et la version HostScan prise en charge pour une DAP est 46. Mais il est fortement recommandé d'utiliser la dernière version de Secure Client.

Configurer une politique d'accès dynamique (DAP)

Créer une politique d'accès dynamique

Avant de commencer

Assurez-vous de disposer de l'ensemble HostScan avant de configurer la politique d'accès dynamique. Vous pouvez ajouter le fichier HostScan à **Objects** > **Object Management** > **VPN** > **Secure Client File**.

Procédure

Étape 1 Choisissez **Devices** > **Dynamic Access Policy** > **Create Dynamic Access Policy** (Périphériques > Politique d'accès dynamique > Créer une politique d'accès dynamique).

Étape 2 Spécifiez le **nom** de la politique d'accès dynamique et une **description** facultative .

Étape 3 Sélectionnez **HostScan Package** dans la liste.

Étape 4 Cliquez sur **Save** (enregistrer).

Prochaine étape

Pour configurer l'enregistrement de politique d'accès dynamique, consultez Créer un enregistrement de politique d'accès dynamique

Créer un enregistrement de politique d'accès dynamique

Une politique d'accès dynamique (DAP) peut contenir plusieurs enregistrements DAP, dans lesquels vous configurez les attributs d'utilisateur et de point terminal. Vous pouvez classer par ordre de priorité les enregistrements DAP au sein d'une DAP de sorte que le défense contre les menaces puisse sélectionner et séquencer les critères requis lorsqu'un utilisateur tente une connexion VPN.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **Dynamic Access Policy (Politique d'accès dynamique)**.

Étape 2 Modifiez une politique d'accès dynamique existante ou créez-en une nouvelle, puis modifiez la politique.

Étape 3 Précisez le **nom** de l'enregistrement DAP.

Étape 4 Saisissez la **priorité** de l'enregistrement DAP.

Plus le numéro de priorité est faible, plus la priorité est élevée.

Étape 5 Sélectionnez l'une des actions suivantes à effectuer lorsqu'un enregistrement DAP correspond :

- **Continue** (Continuer) : cliquez pour appliquer les attributs de politique d'accès à la session.
- **Terminate** (Mettre fin) : sélectionnez cette option pour mettre fin à la session.
- **Quarantine** (Quarantaine) : sélectionnez cette option pour mettre la connexion en quarantaine.

Étape 6 Cochez la case **Display User Message on Criterion match** (afficher le message d'utilisateur sur la correspondance de critères) et ajoutez le message de l'utilisateur.

Le défense contre les menaces affiche ce message à l'utilisateur lorsque l'enregistrement DAP correspond.

Étape 7 Cochez la case **Apply a Network ACL on Traffic** (appliquer une liste de contrôle d'accès réseau sur le trafic), puis sélectionnez la liste de contrôle d'accès dans le menu déroulant.

Étape 8 Cochez la case **Apply one or more Secure Client Custom Attributes** (Appliquer un ou plusieurs attributs personnalisés Secure Client) et sélectionnez l'objet attributs personnalisés dans la liste déroulante.

Étape 9 Cliquez sur **Save** (enregistrer).

Configurer les paramètres des critères AAA pour une DAP

DAP complète les services AAA en fournissant un ensemble limité d'attributs d'autorisation qui peuvent remplacer les attributs fournis par AAA. défense contre les menaces 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. défense contre les menaces peut choisir plusieurs enregistrements DAP en fonction de ces informations, qu'il regroupe ensuite pour créer des attributs d'autorisation DAP.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **Dynamic Access Policy (Politique d'accès dynamique)**.

Étape 2 Modifiez une politique DAP existante ou créez-en une nouvelle, puis modifiez la politique.

Étape 3 Sélectionnez un enregistrement DAP ou créez-en un nouveau, puis modifiez l'enregistrement DAP.

Étape 4 Cliquez sur **Critères AAA**.

Étape 5 Sélectionnez l'un des **critères de correspondance entre les sections**.

- Any (n'importe quel) : correspond à n'importe lequel des critères.
- All (tout) : correspond à tous les critères.
- Aucun : ne correspond à aucun des critères définis.

Étape 6 Cliquez sur **Add** (ajouter) pour ajouter les **critères VPN de Cisco** requis .

Les critères VPN de Cisco comprennent des attributs pour la politique de groupe, l'adresse IPv4 attribuée, l'adresse IPv6 attribuée, le profil de connexion, le nom d'utilisateur, le nom d'utilisateur 2 et le protocole SCEP requis.

a) Sélectionnez un attribut et spécifiez la **Valeur**.

b) Cliquez sur **Add another threat** (ajouter un autre critères) pour ajouter d'autres critères.

c) Cliquez sur **Save** (enregistrer).

SCEP exigé

Étape 7 Sélectionner **Critères LDAP**, **Critères RADIUS**ou **Critères SAML** et préciser la **valeur** et l' **ID de l'attribut**.

Étape 8 Cliquez sur **Save** (enregistrer).

Configurer les critères de sélection des attributs de point terminal dans 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. Le défense contre les menaces 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 défense contre les menaces le choisisse pour une session. Le défense contre les menaces sélectionne uniquement les enregistrements DAP qui satisfont toutes les conditions configurées.

Procédure

Étape 1 Choisissez **Devices** > **Dynamic Access Policy** > **Create Dynamic Access Policy** (Périphériques > Politique d'accès dynamique > Créer une politique d'accès dynamique).

Étape 2 Modifiez une politique DAP, puis un enregistrement DAP.

Remarque Créez une politique DAP et un enregistrement DAP si ce n'est déjà fait.

Étape 3 Cliquez sur **Endpoint Criteria** (Critère de point terminal) et configurez les attributs de critères de point terminal suivants :

Remarque 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-maliciels à une DAP
- Ajouter un attribut de point terminal de périphérique à une DAP
- Ajouter les attributs de point terminal Secure Client à une DAP, à la page 8
- Ajouter un attribut de point terminal NAC à une DAP
- Ajouter un attribut d'application à une DAP
- Ajouter un attribut de point terminal Personal Firewall à une DAP
- Ajouter un attribut de point terminal de système d'exploitation à une DAP
- Ajouter un attribut de point terminal de processus à une DAP
- Ajouter un attribut de point terminal de registre à une DAP
- Ajouter un attribut de point terminal de fichier à une DAP
- Ajouter des attributs d'authentification de certificat à une DAP (Politique d'accès dynamique)

Étape 4 Cliquez sur **Save** (enregistrer).

Ajouter un attribut de point terminal anti-maliciels à une DAP

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **ECritère de point terminal** > **Anti-programmes malveillants**.

Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).

Étape 3 Cliquez sur **Add** pour ajouter des attributs anti-programmes malveillants.

Étape 4 Cliquez sur **Installed** pour indiquer si l'attribut de point terminal sélectionné et les qualificateurs qui l'accompagnent sont installés ou non installés.

Étape 5 Choisissez **Enabled** ou **Disabled** pour activer ou désactiver l'analyse en temps réel contre les programmes malveillants.

Étape 6 Sélectionnez le nom du **fournisseur** d'anti-programmes malveillants dans la liste.

Étape 7 Sélectionnez la **Description du produit** anti-programme malveillant .

Étape 8 Choisissez la **version** du produit anti-programme malveillant.

Étape 9 Indiquez le Nombre de jours depuis la **dernière mise à jour**.

Vous pouvez indiquer qu'une mise à jour du logiciel anti-programme malveillant doit se produire dans un délai inférieur à (<) ou supérieur (>) au nombre de jours que vous spécifiez.

Étape 10 Cliquez sur **Save** (enregistrer).

Ajouter un attribut de point terminal de périphérique à une DAP

Procédure

Étape 1 Modifiez un enregistrement DAP et choisissez **Critères du point terminal** > **Périphérique**.

Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).

Étape 3 Cliquez sur **Add** (ajouter) et sélectionnez l'opérateur **=** ou **≠** pour vérifier que l'attribut est égal ou différent par rapport à la valeur que vous saisissez pour les attributs suivants :

- **Host Name** (Nom d'hôte) : 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).
- **MAC Address** (adresse MAC) : Adresse MAC de la carte d'interface réseau que vous testez. L'adresse MAC doit être au format XX-XX-XX-XX-XX-XX, où chaque X est un caractère hexadécimal.
- **BIOS Serial Number**(numéro de série du BIOS) : valeur du numéro de série du BIOS du périphérique que vous testez. Le format des numéros dépend du fabricant.
- **Port Number** (Numéro de port) : Numéro du port d'écoute du périphérique.
- **Secure Desktop Version** (Version de Secure Desktop) : Version de l'image de balayage de l'hôte exécutée sur le point terminal.
- **OPSWAT Version** (Version OPSWAT) : version du client OPSWAT.
- **Privacy Protection** (Protection de la vie privée) : aucune, nettoyeur de cache, Secure Desktop.
- **TCP/UDP Port Number** (Numéro de port TCP/UDP) : Port TCP ou UDP dans l'état d'écoute que vous testez.

Étape 4 Cliquez sur **Save** (enregistrer).

Ajouter les attributs de point terminal Secure Client à une DAP

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **Critère de point terminal** > **Secure Client**.

Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).

Étape 3 Cliquez sur **Add** (ajouter) et sélectionnez l'opérateur **=** ou **≠** pour vérifier que l'attribut est égal ou différent de la valeur que vous saisissez.

Étape 4 Sélectionnez la **version** et la **plateforme** du client.

Étape 5 Sélectionnez la **version de la plateforme** et précisez le **type de périphérique** et l'**ID unique de périphérique**.

Étape 6 Ajoutez les **adresses** MAC au ensemble d'adresses MAC.

Remarque L'adresse MAC doit être au format XX-XX-XX-XX-XX-XX, où chaque X est un caractère hexadécimal. Vous pouvez cliquer sur **Add another MAC Address** (ajouter une autre adresse MAC) pour ajouter d'autres adresses.

Étape 7 Cliquez sur **Save** (enregistrer).

Ajouter les attributs de point terminal NAC à une DAP

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **Endpoint Criteria** > **NAC** (Critère de point terminal).

Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).

Étape 3 Cliquez sur **Add** (Ajouter) pour ajouter des attributs NAC.

Étape 4 Définissez l'opérateur comme égal à = ou différent de ≠ à la chaîne du jeton de posture. Saisissez la chaîne du jeton de posture dans la zone **Posture Status** (État de la posture).

Étape 5 Cliquez sur **Save** (enregistrer).

Ajouter un attribut d'application à une DAP

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **Endpoint Criteria (Critères de point terminal)** > **Application**.

Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).

Étape 3 Cliquez sur **Add** (Ajouter) pour ajouter des attributs d'application.

Étape 4 Choisissez est égal (=) ou différent (≠) et spécifiez le **Type de client** pour indiquer le type de connexion d'accès à distance.

Étape 5 Cliquez sur **Save** (enregistrer).

Ajouter un attribut de point terminal Personal Firewall à une DAP

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **Endpoint Criteria** > **Personal Firewall** (Critère de point terminal > Pare-feu personnel).

Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).

Étape 3 Cliquez sur **Add** pour ajouter des attributs personnels de pare-feu.

Étape 4 Cliquer sur **Installed** (installé) pour indiquer si l'attribut de terminal de pare-feu personnel et les qualificateurs qui l'accompagnent (champs sous la colonne Nom/Opération/Valeur) sont installés ou non installés.

Étape 5 Choisissez **Enabled** ou **Disabled** pour activer ou désactiver la protection par pare-feu.

Étape 6 Sélectionnez le nom du **fournisseur** de pare-feu dans la liste.

Étape 7 Sélectionnez la **description du produit** du pare-feu.

Étape 8 Sélectionnez l'opérateur égal (=) ou différent (≠) et choisissez la **version** du pare-feu personnel.

Étape 9 Cliquez sur **Save** (enregistrer).

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

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **Endpoint Criteria** > **Operating System** (Critères de point terminal > Système d'exploitation).

Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).

Étape 3 Cliquez sur **Add** pour ajouter des attributs de point terminal.

Étape 4 Sélectionnez l'opérateur égal (=) ou différent (≠), puis sélectionnez le **système d'exploitation**.

Étape 5 Sélectionnez l'opérateur égal (=) ou différent (≠), puis la **version** du système d'exploitation.

Étape 6 Cliquez sur **Save** (enregistrer).

Ajouter un attribut de point terminal de processus à une DAP

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **Critères de point terminal** > **Processus**.

Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).

Étape 3 Cliquez sur **Add** pour ajouter les attributs de processus.

Étape 4 Sélectionnez **Existe** ou **n'existe pas**.

Étape 5 Précisez le **nom du processus**.

Étape 6 Cliquez sur **Save** (enregistrer).

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 point terminal de registre, définissez la clé de registre que vous souhaitez analyser dans la fenêtre d'analyse de l'hôte de Cisco Secure Desktop.

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **Critère de point terminal** > **Registre**.
Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).
Étape 3 Cliquez sur **Add** pour ajouter des attributs de registre.
Étape 4 Sélectionnez le **chemin d'entrée** pour le registre et spécifiez le chemin.
Étape 5 Choisissez l'existence du registre, **Existe** ou **N'existe pas**.
Étape 6 Sélectionnez le **type** de registre dans la liste.
Étape 7 Sélectionnez l'opérateur égal (=) ou différent (≠) et saisissez la **valeur** de la clé de registre.
Étape 8 Sélectionnez **Insensible à la casse** pour ignorer la casse de l'entrée de registre lors de l'analyse.
Étape 9 Cliquez sur **Save** (enregistrer).

Ajouter un attribut de point terminal de fichier à une DAP

Procédure

Étape 1 Modifiez un enregistrement DAP et sélectionnez **Endpoint Criteria (Critères du point terminal)** > **File (Fichier)**.
Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).
Étape 3 Cliquez sur **Add** (Ajouter) pour ajouter des attributs de fichier.
Étape 4 Spécifiez le **chemin d'accès du fichier**.
Étape 5 Choisissez **Existe** ou **n'existe pas** pour indiquer la présence du fichier.
Étape 6 Sélectionnez inférieur à (<) ou supérieur à (>) et précisez les jours de **dernière modification** pour le fichier.
Étape 7 Sélectionnez l'opérateur égal (=) ou différent de ≠ et saisissez la **somme de contrôle**.
Étape 8 Cliquez sur **Save** (enregistrer).

Ajouter des attributs d'authentification de certificat à une DAP (Politique d'accès dynamique)

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 Modifiez un enregistrement DAP et sélectionnez **Endpoint Criteria (Critère de point terminal)** > **Certificate (Certificat)**.
Étape 2 Sélectionnez les critères de correspondance **All** (Tous) ou **Any** (N'importe lequel).
Étape 3 Cliquez sur **Add** (Ajouter) pour ajouter des attributs de certificat.
Étape 4 Sélectionnez le certificat **Cert1** ou **Cert2**.
Étape 5 Sélectionnez l' **objet** et spécifiez la valeur de l'objet.

Étape 6 Sélectionnez l'**émetteur** et précisez la valeur de l'émetteur.

Étape 7 Sélectionnez **autre nom du sujet** et précisez la valeur.

Étape 8 Précisez le **numéro de série**.

Étape 9 Choisissez **Magasin de certificats** : Aucun, Machine ou Utilisateur.

Le client VPN envoie les renseignements du magasin de certificats.

Étape 10 Cliquez sur **Save** (enregistrer).

Configurer les paramètres avancés pour une DAP

Vous pouvez utiliser l'onglet Avancé pour ajouter des critères de sélection autres que ce qui est possible dans les zones attributaires AAA et du point terminal. Par exemple, alors que vous pouvez configurer défense contre les menaces pour utiliser des attributs AAA qui satisfont un, tous ou aucun des critères spécifiés, les attributs de point terminal sont cumulatifs et doivent tous satisfaire. Pour permettre aux périphériques 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.

Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **Dynamic Access Policy (Politique d'accès dynamique)**.

Étape 2 Modifiez une politique DAP, puis modifiez un enregistrement DAP.

Remarque Créez une politique DAP et un enregistrement DAP si ce n'est déjà fait.

Étape 3 Cliquez sur l'onglet **Advanced (Avancé)**.

Étape 4 Sélectionnez **AND** ou **OR** comme critères de correspondance à utiliser dans la configuration DAP.

Étape 5 Ajoutez le script Lua dans le champ **Lua script for advanced attribute matching**.

Étape 6 Cliquez sur **Save** (enregistrer).

Associer une politique d'accès dynamique au VPN d'accès à distance

Vous pouvez associer la politique d'accès dynamique (DAP) à la politique VPN d'accès à distance pour que les attributs de la politique d'accès dynamique correspondent lors de l'authentification et de l'autorisation de session VPN. Vous pouvez ensuite déployer le VPN d'accès à distance sur défense contre les menaces .

Procédure

Étape 1 Choisissez **Périphériques** > **Accès à distance**.

Étape 2 Cliquez sur **Edit** (modifier) à côté de la politique VPN d'accès à distance à laquelle vous souhaitez associer la politique d'accès dynamique.

Étape 3 Cliquer sur le lien dans VPN d'accès à distance pour sélectionner la politique d'accès dynamique.

Étape 4 Sélectionnez la politique dans la liste déroulante **Politique d'accès dynamique** ou cliquez sur **Créer une politique d'accès dynamique** pour configurer une nouvelle politique d'accès dynamique.

Étape 5 Cliquez sur **OK**.

Étape 6 Cliquez sur **Save** pour enregistrer la politique VPN d'accès à distance.

Lorsque l'utilisateur du VPN d'accès à distance tente de se connecter, le VPN vérifie les enregistrements et les attributs de politique d'accès dynamique configurés. Le VPN crée une politique d'accès dynamique basée sur les enregistrements de politique d'accès dynamique correspondants et prend les mesures appropriées sur la session VPN.

Historique de la politique d'accès dynamique

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Politique d'accès dynamique	7.0	N'importe lequel	Cette fonctionnalité a été introduite.

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.