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

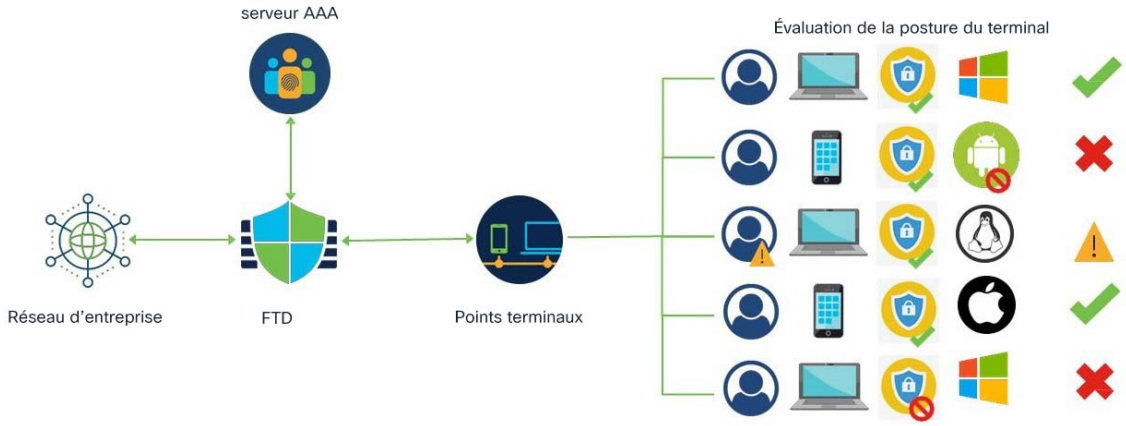
Dernière modification : 2025-04-29

Politique d'accès dynamique (Dynamic Access Policy) de Cisco Secure Firewall Threat DefenseCisco

Une politique d'accès dynamique (DAP) sur Cisco Secure Firewall Threat Defense (anciennement Firepower Threat Defense) vous permet de configurer l'autorisation pour répondre aux dynamiques des environnements VPN. Vous pouvez utiliser l'interface Web Cisco Secure Firewall Management Center (anciennement Cisco Firepower Management Center) pour créer un DAP en configurant un ensemble d'attributs de contrôle d'accès. Vous pouvez associer les attributs 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.

Le Threat Defense accorde l'accès VPN à une session utilisateur particulière en fonction de votre configuration DAP. Threat Defense sélectionne et regroupe les attributs d'un ou plusieurs enregistrements DAP, puis génère un DAP lors de l'authentification de l'utilisateur. Threat Defense sélectionne les enregistrements DAP en fonction des informations de sécurité de point terminal du périphérique distant et des informations AAA. Le Threat Defense applique ensuite l'enregistrement DAP au tunnel ou à la session d'utilisateur.

Illustration 1 : Exemple de politique d'accès dynamique



Composants de la configuration DAP

Une nouvelle configuration DAP nécessite la création d'une politique DAP, d'un enregistrement DAP et d'attributs de critères DAP :

- **Politique d'accès dynamique** : une configuration DAP se compose d'enregistrements.

- **Enregistrement DAP** : un enregistrement DAP se compose d'attributs d'évaluation de point d'accès de critères et d'autorisation d'utilisateur (AAA). Si l'enregistrement correspond, DAP définit les actions à appliquer à la session VPN.
- **Critères et attributs DAP** : les critères AAA, les critères de point terminal et les critères avancés contiennent des attributs de configuration granulaires pour l'accès au réseau.

Pour les étapes de configuration détaillées, consultez Configuration d'une politique d'accès dynamique, à la page 4.

Fonctionnement du VPN d'accès à distance Threat Defense avec DAP

1. Un utilisateur distant tente de se connecter au VPN en utilisant le client Secure Client à partir d'un périphérique de terminal.
2. Threat Defense effectue une évaluation de la posture sur les terminaux.
3. Threat Defense authentifie l'utilisateur par l'intermédiaire du serveur de comptabilité d'autorisation d'authentification (AAA). Le serveur AAA renvoie également des attributs d'autorisation de l'utilisateur.
4. Threat Defense applique des attributs d'autorisation AAA à la session et établit le tunnel VPN.
5. Le Threat Defense sélectionne les enregistrements DAP en fonction des informations d'autorisation AAA de l'utilisateur et des informations d'évaluation de la posture pour la session.
6. Threat Defense regroupe les attributs DAP des enregistrements DAP sélectionnés et crée la politique DAP.
7. Threat Defense applique la politique de groupe pour la session VPN d'accès à distance.

Pourquoi mettre en oeuvre la politique d'accès dynamique (DAP)?

Vous pouvez configurer les attributs DAP pour identifier un terminal de connexion et autoriser l'accès de l'utilisateur à diverses ressources réseau. Vous pouvez créer un DAP pour les scénarios suivants et faire plus avec les attributs DAP pour protéger vos terminaux et vos ressources réseau :

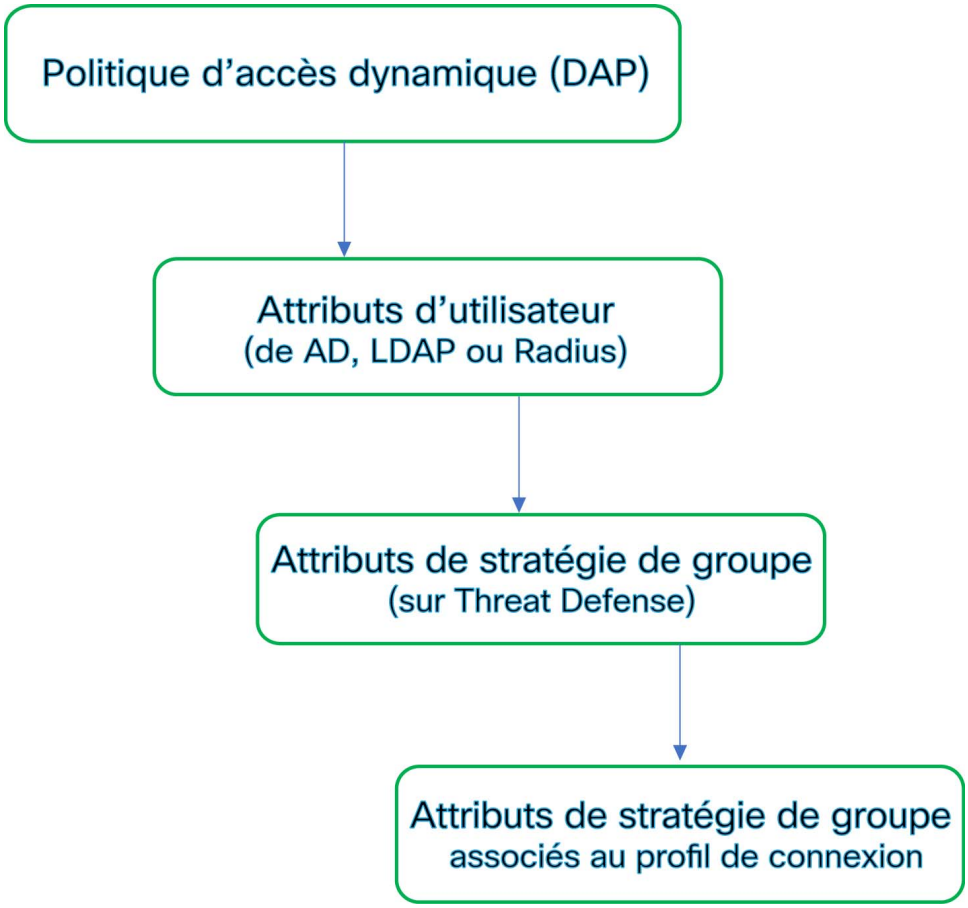
- Assurez-vous que les terminaux se connectant au VPN sont conformes aux politiques de sécurité d'une organisation, quels que soient le périphérique ou la plateforme de terminaux.
- Déterminez les systèmes d'exploitation, les divers logiciels de sécurité exécutés sur le terminal, les paramètres de registre, les versions de fichiers et les potentielles journalisations de saisie exécutés sur les terminaux.
- Détectez, appliquez la disponibilité et la mise à jour des applications sur les terminaux gérés par l'entreprise. Par exemple, les logiciels antivirus
- Déterminent les ressources de réseau auxquelles les utilisateurs autorisés peuvent accéder.

Application de la politique des autorisations et des attributs dans Threat Defense

Le périphérique Threat Defense 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 Threat Defense 457903, le serveur d'authentification externe et/ou le serveur d'autorisation AAA (RADIUS) ou à partir d'une politique de groupe sur le périphérique Threat Defense.

Si le périphérique Threat Defense reçoit des attributs de toutes les sources, Threat Defense évalue, fusionne et applique les attributs à la politique d'utilisateur. En cas de conflit entre les attributs provenant du DAP, du serveur AAA ou de la stratégie de groupe, les attributs obtenus à partir du DAP sont toujours prioritaires.

Illustration 2 : Flux d'application des politiques



1. **Attributs DAP sur le** Threat Defense : 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. **Stratégies de groupe configurées sur le** Threat Defense : si un serveur RADIUS renvoie la valeur de l'attribut de classe RADIUS IETF-Class-25 (OU = group-policy) pour l'utilisateur, le périphérique Threat

Defense place l'utilisateur dans la stratégie de groupe du même nom et applique les attributs de la stratégie de groupe qui ne sont pas renvoyés par le serveur.

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

Remarque Le périphérique Threat Defense ne prend pas en charge la transmission des attributs du système par défaut de la politique de groupe par défaut, *DfltGrpPolicy*. Les attributs de stratégie de groupe attribués à partir du profil de connexion sont utilisés pour la session utilisateur s'ils ne sont pas remplacés par les attributs de l'utilisateur ou la stratégie de groupe du serveur AAA.

Licences des politiques d'accès dynamique

Le Threat Defense doit avoir l'une des licences AnyConnect qui prennent en charge le VPN d'accès à distance :

- Secure Client Premier
- Secure Client Advantage
- Secure Client VPN Only

Les Management Center doivent avoir des fonctionnalités d'exportation contrôlées activées.

Pour en savoir plus sur les licences Threat Defense, consultez le chapitre *Attribuer des licences au système Firepower* du *Guide de configuration de Cisco Secure Firewall Management Center*.

Configuration d'une 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 prioriser les enregistrements DAP afin que les critères requis soient appliqués lorsqu'un utilisateur tente une connexion VPN.

Avant de commencer

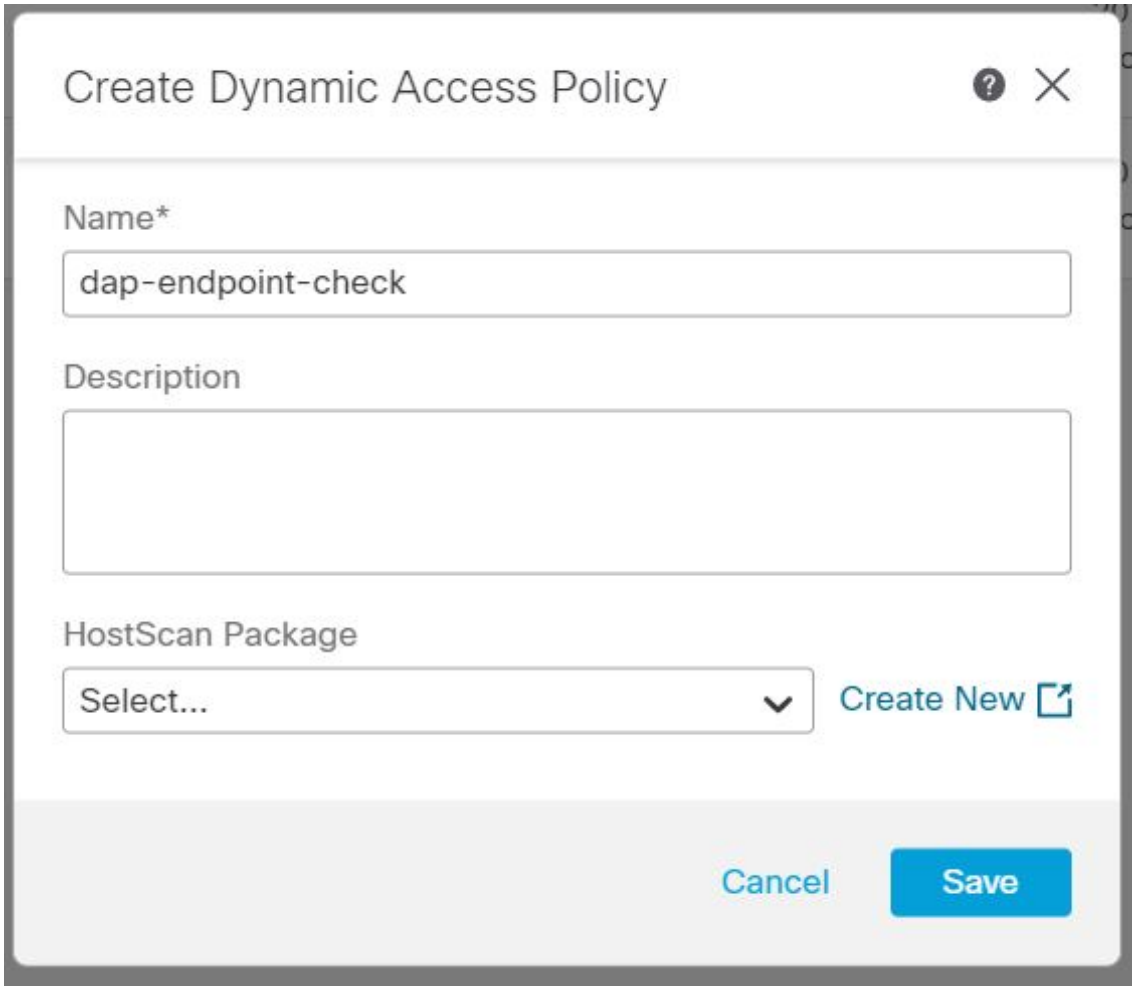
Assurez-vous de configurer les applications et les paramètres requis avant de créer une politique d'accès dynamique (DAP) :

- **Progiciel HostScan** : téléchargez la version 4.6 ou ultérieure du progiciel HostScan.
- **Serveur AAA** : configurez les serveurs AAA requis pour renvoyer les attributs corrects lors de l'authentification ou de l'autorisation des sessions VPN.
- **Secure Client** : téléchargez la dernière version du client Secure Client et ajoutez-la à votre configuration de VPN d'accès à distance.
- **Remote Access VPN** (Accès à distance du VPN) : configurez les paramètres de votre VPN d'accès à distance à l'aide de l'assistant de configuration de VPN d'accès à distance sous **Devices (Périphériques)** > **VPN** > **Remote Access (Accès à distance)**.

- Chargez le paquet HostScan dans **Objets** > **VPN** > **de gestion des objets** > **AnyConnect File (Fichier AnyConnect)**.

1. Configurez une nouvelle politique dynamique si vous ne l'avez pas encore fait.
   a) Choisissez **Devices (Périphériques)** > **Dynamic Access Policy (Politique d'accès dynamique)** > **Create Dynamic Access Policy (Créer une politique d'accès dynamique)**.

   Illustration 3 : Créer une politique d'accès dynamique



   b) Spécifiez un **nom** de politique d'accès dynamique et une **description** facultative.
   c) Sélectionnez le **progiciel HostScan** dans la liste déroulante ou cliquez sur **Create New (créer un nouveau)** pour ajouter un fichier de progiciel HostScan.
   Une politique d'accès dynamique contient un enregistrement DAP par défaut. Vous pouvez commencer à ajouter des enregistrements DAP avec les attributs requis sous les critères AAA, les critères de point terminal et les critères avancés à l'aide du script Lua.
   d) Cliquez sur **Save** (enregistrer).
2. Créez un enregistrement DAP et attribuez un numéro de priorité.

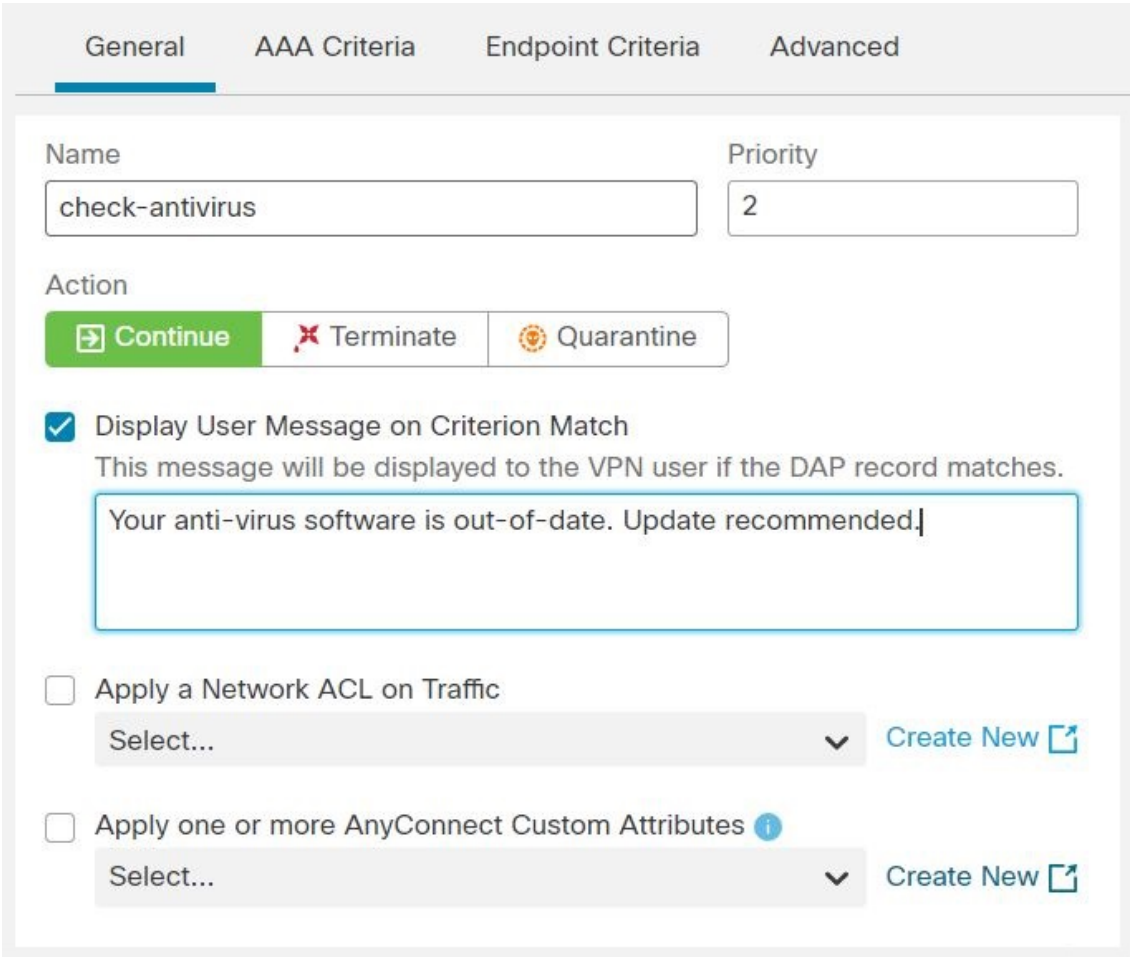
   Un enregistrement DAP contient les attributs de correspondance lorsqu'un utilisateur VPN tente d'établir une connexion VPN avec la passerelle VPN Threat Defense. Vous pouvez utiliser les paramètres

d'enregistrement DAP pour accorder, refuser ou restreindre l'accès au VPN en fonction des attributs de critères sélectionnés.

Le numéro de **priorité** indique l'ordre dans lequel un enregistrement correspond. Threat Defense utilise le numéro de priorité d'un enregistrement DAP pour séquencer et sélectionner l'enregistrement. Plus le numéro de priorité est faible, plus la priorité est élevée.

Remarque Si vous ne configurez pas d'enregistrement DAP pour un DAP, l'enregistrement **DAP par défaut** est appliqué. L'enregistrement DAP par défaut n'a pas de priorité.

a) Choisissez **Devices (Périphériques)** > **Dynamic Access Policy (Politique d'accès dynamique)**.
b) Modifiez une politique DAP existante ou créez-en une nouvelle.
c) Cliquez sur **Create DAP Record** (Créer un enregistrement DAP).



d) Précisez le **nom** de l'enregistrement DAP.
e) Saisissez le numéro de **priorité** de l'enregistrement DAP.
f) Sélectionnez une **action** à entreprendre si l'enregistrement DAP correspond à :

- **Continue** (Continuer) : cliquez pour appliquer les attributs de politique d'accès à la session et accepter l'utilisateur.

- **Terminate** (Mettre fin) : sélectionnez cette option pour mettre fin à la session.
- **Quarantine** (Quarantaine) : sélectionnez cette option pour mettre la connexion en quarantaine.

g) Sélectionnez **Display User Message on Criterion Match** (Afficher le message de l'utilisateur sur la correspondance des critères) et ajoutez le message dans la boîte.

Remarque Les utilisateurs de VPN reçoivent le message lorsque l'enregistrement DAP correspond.

h) Cochez la case **Apply a Network ACL on Traffic** (Appliquer une ACL réseau sur le trafic) et sélectionnez l'ACL dans la liste. Vous pouvez également créer une nouvelle ACL, puis la sélectionner.

L'ACL du réseau est appliquée à la session VPN lorsque cet enregistrement DAP correspond.

i) Sélectionnez **Apply one or more AnyConnect Custom Attributes** (Appliquer un ou plusieurs attributs personnalisés AnyConnect) et sélectionnez l'objet d'attributs personnalisés dans le menu déroulant.

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

Pour en savoir plus sur les attributs personnalisés de réseau et AnyConnect, consultez le dernier Cisco Secure Firewall Management Center Guide de configuration de.

k) Configurez les attributs DAP pour vérifier quand les utilisateurs et les terminaux se connectent au VPN.

- Configurer les paramètres des critères AAA pour une DAP, à la page 8
- Configurer les critères de sélection des attributs de point terminal dans une DAP, à la page 10
- Configurer les paramètres avancés d'une DAP, à la page 11

3. Reliez le DAP à une configuration VPN d'accès à distance.

Vous devez associer la politique d'accès dynamique (DAP) à la politique VPN d'accès à distance pour que les attributs DAP correspondent lors de l'authentification et de l'autorisation de session VPN.

a) Dans l'interface web Cisco Secure Firewall Management Center, choisissez **Devices (Périphériques)** > **VPN** > **Remote Access (Accès à distance)**.

b) Sélectionnez et modifiez la politique d'accès à distance où vous souhaitez ajouter un DAP.

a) Cliquez sur le lien d'association Dynamic Access Policy (Politique d'accès dynamique).

b) Sélectionner une **politique d'accès dynamique** dans la liste

c) Cliquez sur **Ok**.

Une fois que vous associez une DAP à un VPN d'accès à distance, le Threat Defense vérifie les enregistrements et les attributs DAP configurés lorsqu'un utilisateur tente de se connecter VPN. Le Threat Defense crée un DAP en fonction de la correspondance et prend l'action appropriée sur la session VPN.

4. Déployez le VPN d'accès à distance sur les appareils Threat Defense.

a) Dans la barre de menus Management Center, cliquez sur **Deploy** (déployer) puis sélectionnez **Deployment** (déploiement).

Vous pouvez afficher la liste de toutes les configurations obsolètes en attente de déploiement sur les périphériques Threat Defense.

b) Identifiez et choisissez les appareils sur lesquels vous souhaitez déployer le VPN d'accès à distance et d'autres modifications de configuration.
c) Cliquez sur **Deploy** (déployer).

Remarque Corrigez les erreurs avant de déployer la configuration.

Configurer les paramètres des critères AAA pour une DAP

Threat Defense utilise les attributs AAA associés à une session VPN par le serveur AAA pour correspondre à un utilisateur ou à un groupe d'utilisateurs.

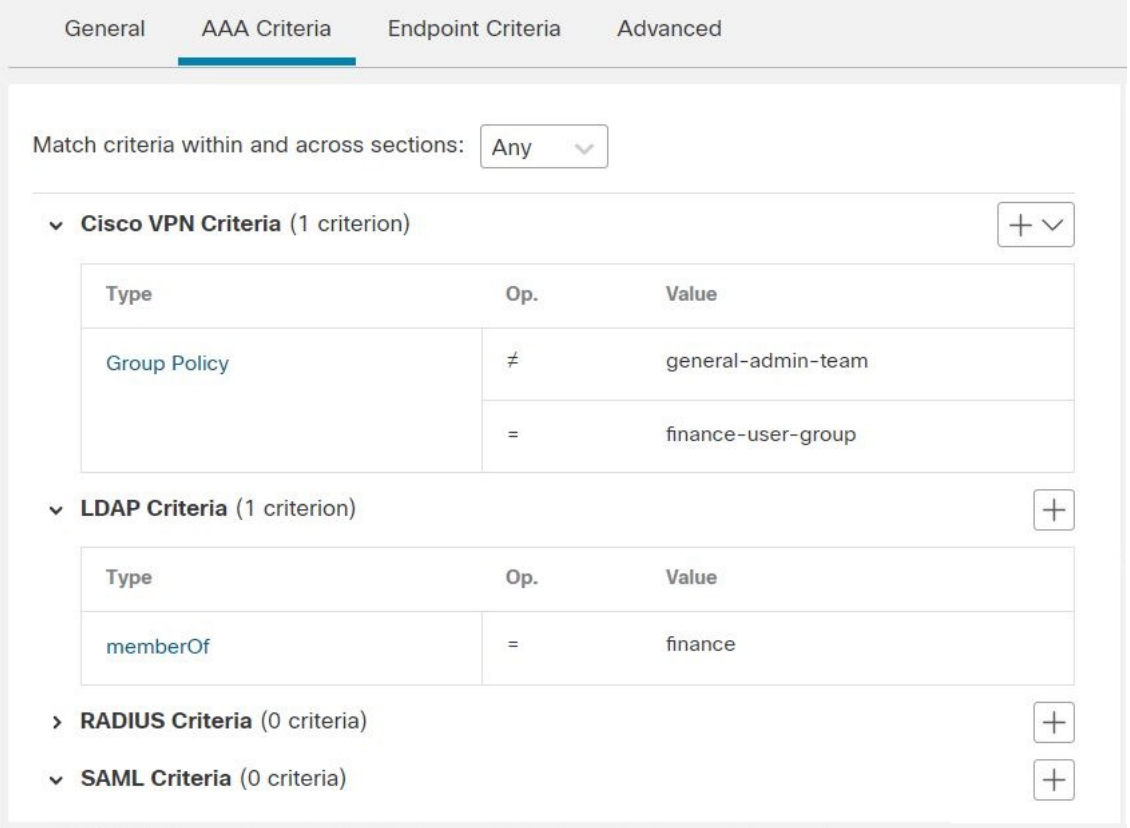
DAP complète les services AAA en fournissant un ensemble limité d'attributs d'autorisation pouvant remplacer les attributs fournis par AAA. Threat Defense sélectionne les enregistrements DAP en fonction des informations d'autorisation AAA et des informations d'évaluation de la posture pour une session VPN. Le Threat Defense peut choisir plusieurs enregistrements DAP en fonction de l'évaluation, puis de les agréger pour créer des attributs d'autorisation DAP.

Avant de commencer

Assurez-vous d'avoir configuré les serveurs AAA requis pour l'authentification, l'autorisation et la gestion des utilisateurs VPN. Les serveurs AAA doivent être accessibles à partir du périphérique Threat Defense, sur lequel vous souhaitez déployer votre VPN d'accès à distance.

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)** : correspond à l'un des critères.
- **All (Tous)** : correspond à tous les critères définis.
- **None (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 les stratégies 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 **Identifiant d'attribut** et un opérateur, puis spécifiez la **valeur** pour la correspondance.
b) Cliquez sur **Add another criteria** (ajouter un autre critère) pour ajouter d'autres critères AAA.
c) Cliquez sur **Save** (enregistrer).

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

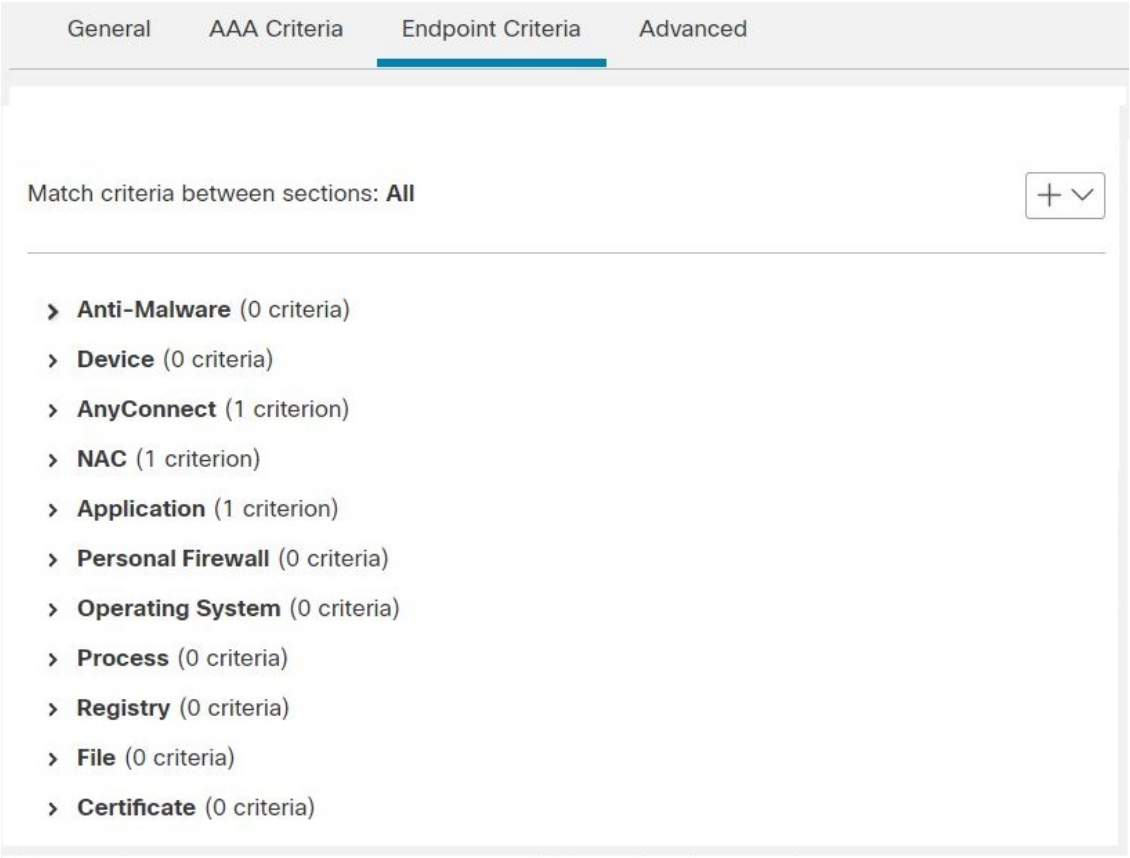
Vous pouvez définir ces attributs sur = ou – la valeur que vous saisissez. Vous pouvez ajouter n'importe quel enregistrement DAP.

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

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. Le Threat Defense génère dynamiquement un ensemble d'attributs de 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 terminal qui doivent être satisfaits pour que le Threat Defense le choisisse pour une session. Le Threat Defense sélectionne uniquement les enregistrements DAP qui satisfont toutes les conditions configurées.

Illustration 4 : Attributs des terminaux DAP



Procédure

Étape 1 Choisissez **Devices (Périphériques)** > **Dynamic Access Policy (Politique d'accès dynamique)** > **Create Dynamic Access Policy (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 d'extrémité requis parmi les types d'attributs suivants :

- Protection contre les programmes malveillants
- Périphérique
- Secure Client
- NAC
- Application
- Pare-feu
- Système d'exploitation
- Processus
- Registre
- Fichier
- Certificate (certificat)

Remarque
Vous pouvez créer plusieurs instances de chaque type d'attribut de point terminal. Vous pouvez également ajouter un nombre illimité d'attributs de terminal pour chaque enregistrement DAP.

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

Configurer les paramètres avancés d'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.

Créez des expressions logiques appropriées dans Lua et saisissez-les ici. Vous pouvez utiliser une fonction d'assertion dans le script Lua. Cette fonction renvoie l'argument comme « true » ou « condition du code ». Dans le cas contraire, elle affiche le message d'erreur d'assertion. Pour en savoir plus sur les fonctions d'assertion et les scripts Lua, consultez le manuel de référence de Lua.

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.

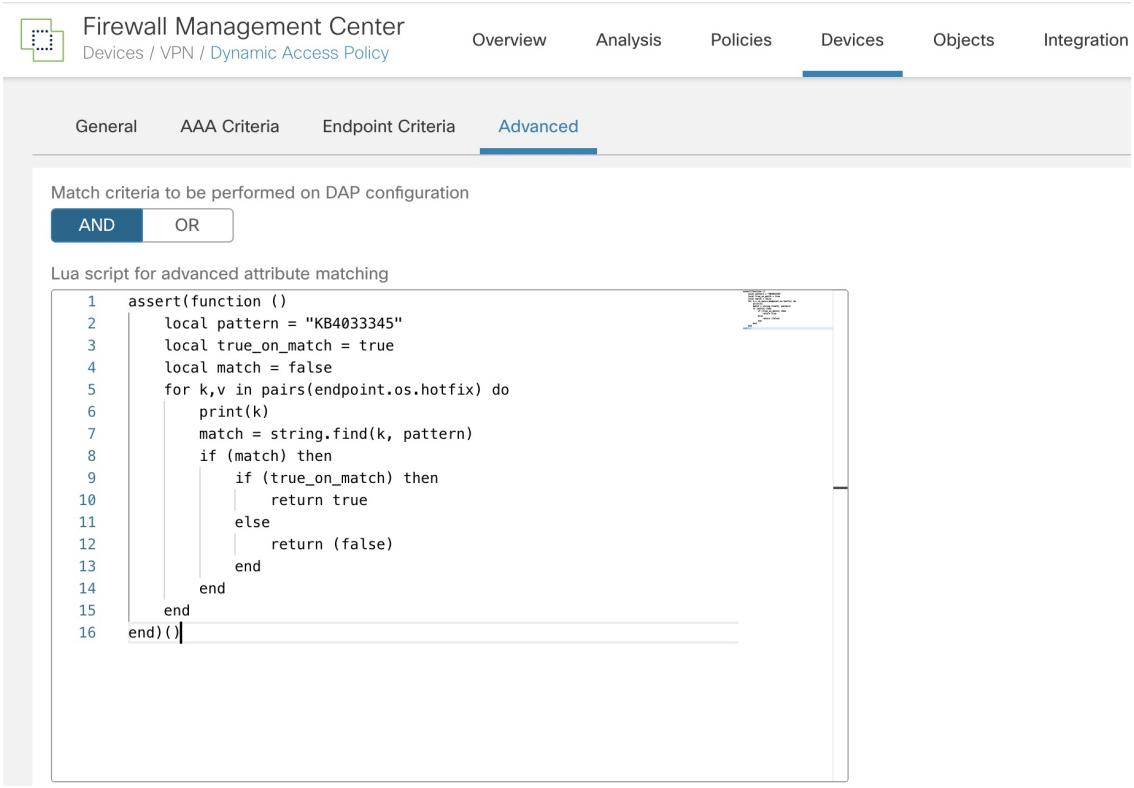
Étape 3 Cliquez sur l'onglet **Advanced (Avancé)**.

Étape 4 Sélectionnez **AND** (ET) ou **OR** (OU) comme critères de correspondance à correspondre dans la configuration DAP.

Étape 5 Ajoutez le script Lua dans le champ **Lua script for advanced attribute matching** (Script Lua pour la mise en correspondance avancée d'attributs).

Le script ci-dessous vérifie un type de correctif rapide dans le système d'exploitation du client (où Secure Client est installé) et renvoie la valeur true (vrai) ou false (faux).

Illustration 5 : Mise en correspondance des critères avancés à l'aide d'un script Lua



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

Dépannage des politiques d'accès dynamique

Avant de résoudre les problèmes de DAP :

- Activez le journal système du VPN dans la politique des paramètres de la plateforme.
- Consultez les journaux liés à DAP sous **Devices (Périphériques)** > **VPN** > **Troubleshooting (Dépannage)** > **.**

Problème 1 : impossible de sauvegarder la configuration DAP

Solution

Si vous n'êtes pas en mesure d'enregistrer la configuration DAP à partir de l'interface Web Management Center, consultez les journaux appropriés pour trouver la raison de la défaillance :

- `/var/opt/CSCOpx/MDC/log/operation/vmssharedsvcs.log.*`

- `/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log.*`

Vous pouvez utiliser le mot-clé `vpn` ou `sso` pour filtrer les journaux associés.

Problème 2 : Échec du déploiement de DAP

Solution :

Si le déploiement de DAP échoue, vérifiez les détails de la transcription de déploiement, puis vérifiez dans le fichier journal `/var/opt/CSCOpx/MDC/opération/vmsbevcs.log.*`

Exemples de politique d'accès dynamique

Cette section fournit des exemples de configurations de politique d'accès dynamique (DAP) pour autoriser ou bloquer l'accès VPN pour les utilisateurs VPN et leurs terminaux.

Remarque Les instructions fournies dans ce document sont des exemples de configuration. Vous pouvez utiliser divers paramètres DAP pour configurer un ou plusieurs enregistrements DAP en fonction de vos besoins. Les paramètres DAP comprennent les attributs des critères AAA, des critères de terminal et des paramètres avancés à l'aide du script Lua.

En fonction de vos exigences de sécurité, vous pouvez configurer un enregistrement DAP unique pour la correspondance de plusieurs critères, ou créer plusieurs enregistrements DAP et les classer par ordre de priorité.

Autoriser ou bloquer l'accès au VPN en fonction du système d'exploitation

Vous pouvez décider de l'accès VPN pour les terminaux en fonction du système d'exploitation. Utilisez le présent exemple pour bloquer les terminaux utilisant la version 7 du système d'exploitation Windows et n'ayant pas recours à l'ensemble de services SP1 Convenance Rollup.

Procédure

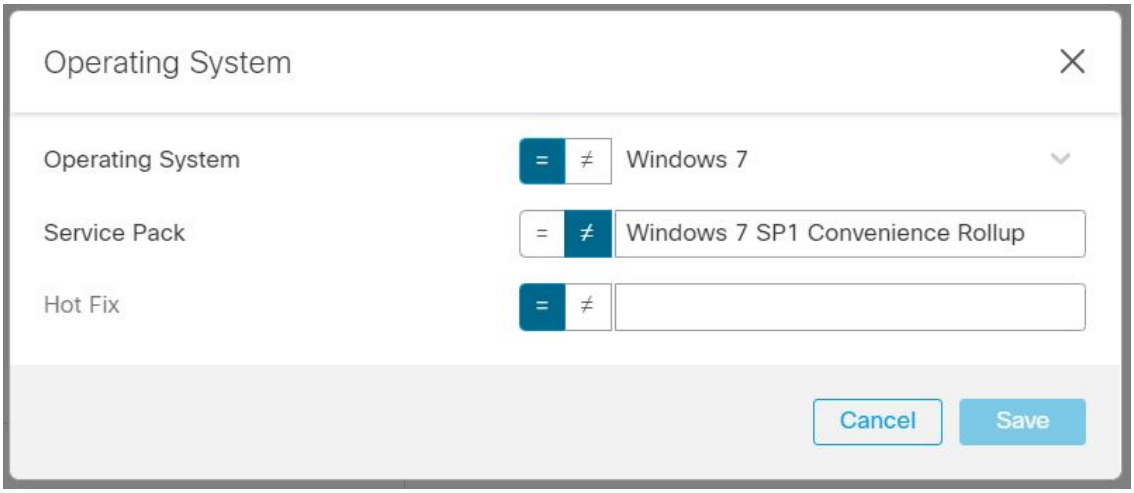
Étape 1 Créez un enregistrement DAP ou modifiez-en un et existant avec l'action **Terminate** (Terminer).

Étape 2 Choisissez **Endpoint Criteria (Critère de point terminal)** > **Operating System (Système d'exploitation)**.

Étape 3 Sélectionnez les critères de correspondance **All (Tous)** pour sélectionner les critères uniquement lorsque tous les attributs configurés correspondent.

Étape 4 Cliquez sur **Add (Ajouter)** pour ajouter des attributs de système d'exploitation.

Illustration 6 : Critères pour les terminaux du système d'exploitation DAP



Étape 5 Sélectionnez l'opérateur **Système d'exploitation** équivalent (=), puis sélectionnez *Windows 7*.

Étape 6 Sélectionnez l'opérateur **Service Pack** not equals (Paquet de service non équivalent) (≠), puis indiquez *SP1 Convenience Rollup*.

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

Bloquer le trafic en fonction d'attributs d'anti-maliciels sur les terminaux

Les étapes répertoriées ici vous permettent de configurer des attributs anti-maliciels pour vérifier lorsqu'un terminal tente de se connecter au VPN. Vous pouvez utiliser les attributs d'enregistrement DAP pour vérifier :

- si Cisco Cisco Secure Endpoint est installé et que l'analyse en temps réel est activée sur le terminal;
- si la version de Cisco Cisco Secure Endpoint est supérieure à 1.1 et que l'anti-maliciel est mis à jour dans les 15 jours.

Consultez Configuration d'une politique d'accès dynamique, à la page 4 pour obtenir des instructions détaillées sur la configuration d'un DAP sur Threat Defense.

Procédure

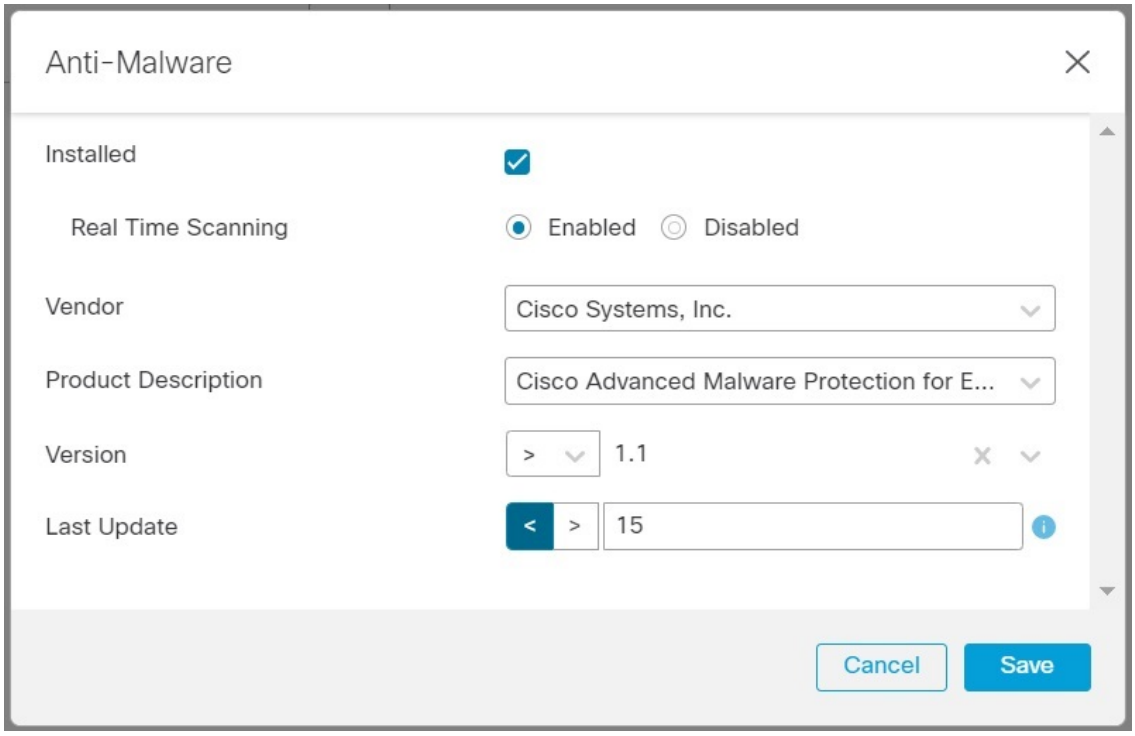
Étape 1 Créez un enregistrement DAP avec l'action **Terminate** (Terminer) ou modifiez un enregistrement DAP existant.

Étape 2 Choisissez **Endpoint Criteria** > **Anti-Malware** (Critère de point terminal > Anti-programme malveillant) dans l'enregistrement DAP.

Étape 3 Sélectionnez les critères de correspondance **All** (Tous) pour sélectionner des critères uniquement lorsque tous les attributs configurés correspondent ou **Any (N'importe)** pour sélectionner l'un des attributs.

Étape 4 Cliquez sur **Add** pour ajouter des attributs anti-programmes malveillants.

Illustration 7 : Critères de terminal anti-maliciels de DAP



Étape 5 Cliquez sur **Installed (installé)** pour indiquer si l'anti-programme malveillant est installé.

Étape 6 Choisissez **Enabled (activé)** pour vérifier si l'analyse des programmes malveillants en temps réel est active.

Étape 7 Sélectionnez le nom du **fournisseur** d'anti-programmes malveillants dans la liste.

Pour cet exemple, sélectionnez *Cisco Systems Inc.* comme fournisseur pour Cisco Cisco Secure Endpoint. Sélectionnez le fournisseur de votre choix.

Étape 8 Sélectionnez la **Description du produit** anti-programme malveillant, *CiscoCisco Secure Endpoint*.

Remarque
Sélectionnez un autre fournisseur et un autre produit de votre choix en fonction du produit anti-maliciels exécuté sur les terminaux se connectant à votre VPN.

Étape 9 Choisissez la **version** du produit anti-programme malveillant supérieure à 1.1.

Étape 10 Indiquez le Nombre de jours depuis la **dernière mise à jour**.

Indiquez qu'une mise à jour d'un anti-programme malveillant doit être antérieure à (<) 15 jours.

Étape 11 Cliquez sur **Save** (enregistrer).

Autoriser ou bloquer l'accès au réseau privé virtuel (VPN) pour une application d'accès à distance

Pour vérifier le type de connexion d'accès à distance afin d'autoriser ou de refuser l'accès VPN aux utilisateurs, utilisez les critères de terminal d'application dans un enregistrement DAP.

Procédure

Étape 1 Créez un enregistrement DAP ou modifiez un enregistrement existant à l'aide de l'action **Continue** (Continuer) ou **Terminate** (Terminer) selon les besoins.

Étape 2 Choisissez des **Critères** > **d'application terminal**.

Étape 3 Sélectionnez les critères de correspondance **All** (Tous) pour sélectionner des critères uniquement lorsque tous les attributs configurés correspondent ou **Any** (N'importe) pour sélectionner l'un des attributs.

Étape 4 Cliquez sur **Add** (Ajouter) pour ajouter des attributs de système d'exploitation.

Illustration 8 : Critères relatifs au terminal de l'application DAP

Remarque
Vous pouvez utiliser l'exemple pour autoriser ou bloquer les utilisateurs VPN se connectant à l'aide de l'application Secure Client.

Vous pouvez sélectionner uniquement les éléments que vous souhaitez vérifier et saisir les valeurs requises. Vous pouvez également choisir de combiner la vérification de l'appareil avec un autre enregistrement DAP avec plusieurs critères de point terminal ou AAA.

Étape 5 Sélectionnez l'opérateur est égal (=) ou n'est pas égal(≠), puis sélectionnez le **type de client** d'accès à distance.

Les types de clients répertoriés sont Clientless, Cut-Through-Proxy, Secure Client, IPsec, L2TP et IPsec-IKEv2-Generic-RA.

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

Vérifiez le périphérique de point terminal pour autoriser ou bloquer l'accès au VPN

Vous pouvez créer des critères DAP pour autoriser ou bloquer l'accès VPN pour un périphérique spécifique. Configurez les détails du périphérique pour vérifier lorsqu'une utilisation tente la connexion VPN.

Procédure

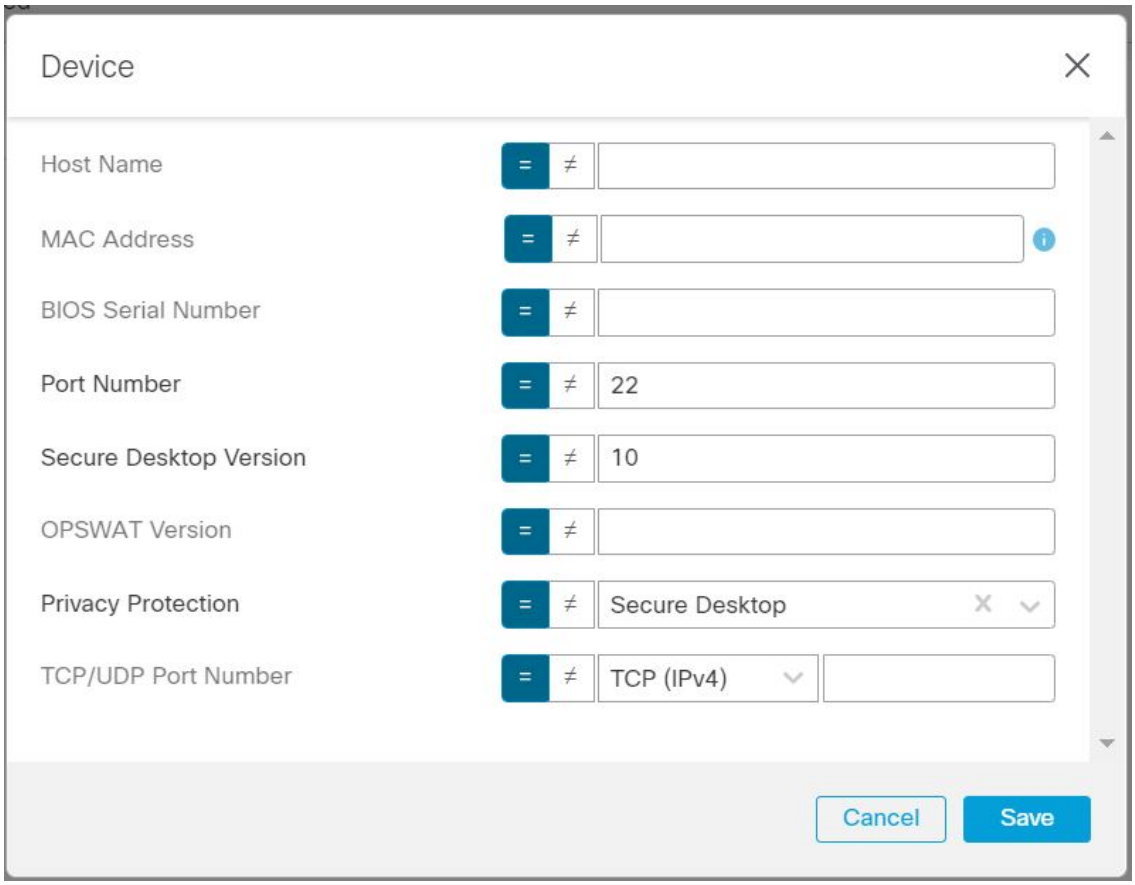
Étape 1 Créez un enregistrement DAP ou modifiez un enregistrement existant à l'aide de l'action **Continue (Continuer)** ou **Terminate (Terminer)** selon les besoins.

Étape 2 Choisissez **Endpoint Criteria** > **Device (Critère de point terminal de périphérique)**.

Étape 3 Sélectionnez les critères de correspondance **All** (Tous) pour sélectionner des critères uniquement lorsque tous les attributs configurés correspondent ou **Any (N'importe)** pour sélectionner l'un des attributs.

Étape 4 Cliquez sur **Add** (Ajouter) pour ajouter des attributs de système d'exploitation.

Illustration 9 : Exemple de critères pour les terminaux du périphérique DAP



Remarque
Utilisez cet exemple pour autoriser ou bloquer les terminaux se connectant par le biais du numéro de port 22, du bureau sécurisé version 10 et de la protection de la confidentialité du bureau Cisco Secure Desktop.

Vous pouvez sélectionner uniquement les éléments que vous souhaitez vérifier, puis saisir les valeurs requises. Vous pouvez également choisir de combiner la vérification de l'appareil avec un autre enregistrement DAP avec plusieurs critères de point terminal ou AAA.

Étape 5 Sélectionnez l'opérateur égal (=) ou non égal (≠), puis spécifiez les informations relatives à l'appareil. Sélectionnez les champs obligatoires et entrez les valeurs du nom de l'hôte, l'adresse MAC, le numéro de série BIOS, le numéro de port, la version de Secure Desktop et la version OPSWAT.

Étape 6 Sélectionnez l'opérateur égal (=) ou non égal( ), puis sélectionnez le numéro de port de protection de la confidentialité et TCP/UDP.

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

Utiliser le script Lua pour vérifier l'anti-programme malveillant sur les terminaux

L'exemple de configuration présenté dans cette section fournit le script Lua requis pour vérifier la présence d'un produit anti-programme malveillant sur les terminaux.

La construction d'expressions logiques à l'aide du script Lua nécessite une connaissance de LUA. Vous pouvez trouver des informations détaillées sur la programmation LUA à l'adresse suivante : http://www.lua.org/manual/5.1/manual.html..

Pour en savoir plus, consultez la section *Politiques d'accès dynamique de Cisco Secure Firewall Threat Defense* du *Guide de configuration de Cisco Secure Firewall Management Center*.

Procédure

Étape 1 Créer un enregistrement DAP on modifiez un enregistrement DAP existant.

Étape 2 Cliquez sur **Advanced (Avancé)** dans l'enregistrement DAP.

Étape 3 Sélectionnez les critères de correspondance **AND** (ET) ou **OR**(OU)

Étape 4 Copiez le script suivant dans la zone de script Lua :

```
assert(function()
local am_count = 0;
CheckAndMsg( true, "endpoint.av="..type(endpoint.am), nil)
for k,v in pairs(endpoint.am) do
am_count = am_count + 1
-- CheckAndMsg( true, "v.exists"..v.exists, nil)
-- CheckAndMsg( true, "v.description"..v.description, nil)
-- CheckAndMsg( true, "v.version"..v.version, nil)
-- CheckAndMsg( true, "v.activescan"..v.activescan, nil)
end
CheckAndMsg( true, "Your request has "..am_count.." Ams", nil)
return true
end)()
```

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

Attributs AAA et terminaux pris en charge dans DAP

Le périphérique Threat Defense utilise une politique DAP lorsque les attributs de l'utilisateur correspondent aux attributs de terminal et d'AAA configurés. Les modules d'analyse de l'hôte de Cisco Secure Client renvoient des informations au périphérique sur les attributs de terminal configurés. Le sous-système DAP utilise ces informations pour choisir un enregistrement DAP correspondant aux valeurs de ces attributs.

La plupart des programmes malveillants, des antivirus, des logiciels malveillants et des pare-feu personnels prennent en charge l'analyse active, ce qui signifie que les programmes résident dans la mémoire et sont donc toujours en cours d'exécution. Le balayage de l'hôte vérifie si un programme est installé sur un terminal et s'il est en mémoire, comme suit :

- Si le programme installé ne prend pas en charge l'analyse active, le balayage de l'hôte signale la présence du logiciel. Le système DAP sélectionne les enregistrements DAP qui donnent des renseignements sur le programme.

- Si le programme installé prend en charge l'analyse active et que l'analyse active est activée pour le programme, l'analyse de l'hôte signale la présence du logiciel. Une fois de plus, l'appareil de sécurité sélectionne les enregistrements DAP qui donnent des renseignements sur le programme.
- Si le programme installé prend en charge l'analyse active et que l'analyse active est désactivée pour le programme, l'analyse de l'hôte ignore la présence du logiciel. Les appareils de sécurité ne choisissent pas les enregistrements DAP qui donnent des renseignements sur le programme.

Attributs AAA pris en charge dans la DAP

Pour configurer les attributs AAA comme critères de sélection pour les 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 sur = ou sur != la valeur que vous saisissez. Il n'y a aucune limite au nombre d'attributs AAA pour chaque enregistrement DAP.

Critères VPN Cisco

Les critères du VPN Cisco font 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. Notamment

- **Group Policy (stratégies de groupe**) : nom de la stratégie de groupe associée à la session utilisateur du VPN. Peut être défini localement sur l'appareil de sécurité ou envoyé à partir d'un serveur RADIUS/LDAP en tant qu'attribut IETF-Class (25). Maximum de 64 caractères.
- **Adresse IPv4 attribuée** : saisissez l'adresse IPv4 que vous souhaitez spécifier pour la stratégie. L'adresse IP attribuée pour les clients VPN de tunnel complet (IPsec, L2TP/IPsec, SSL VPN AnyConnect).
- **Adresse IPv6 attribuée** : saisissez l'adresse IPv6 que vous souhaitez spécifier pour la stratégie.
- Connection Profile (Profil de connexion) : nom du profil de connexion VPN d'accès à distance. Maximum de 64 caractères.
- Username : le nom d'utilisateur principal de l'utilisateur authentifié. Maximum de 64 caractères. S'applique si vous utilisez Local, RADIUS, l'authentification/autorisation LDAP ou tout autre type d'authentification (par exemple, RSA/SDI), domaine NT, etc.
- Username2 : nom d'utilisateur secondaire de l'utilisateur authentifié. Maximum de 64 caractères.

Critères LDAP

Le client LDAP (appareil de sécurité) stocke toutes les paires de valeurs d'attribut 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 portant 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 (AD), le client LDAP AAA fournit une gestion spéciale 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 de la chaîne DN 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 d'autres attributs memberOf dans le message de réponse LDAP, le nom de groupe est extrait de ces attributs et est combiné avec l'attribut AAA memberOf antérieur pour former une chaîne de noms de groupes séparés par des virgules, également mise à jour dans la base de données des attributs de réponse.

Lorsque la session d'accès à distance VPN à un serveur d'authentification ou d'autorisation LDAP renvoie les trois groupes Active Directory suivants (énumérations memberOf), le périphérique Threat Defense traite trois groupes Active Directory :

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

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

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

Ce groupe peut être utilisé dans n'importe quelle combinaison comme critères de sélection aaa.ldap.

Les attributs LDAP sont composés d'une paire de noms d'attributs et de valeurs d'attributs 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 Service au lieu de ce que le serveur AD renvoie comme service, l'enregistrement DAP ne correspondra pas sur la base de ce paramètre d'attribut.

Remarque Pour saisir plusieurs valeurs dans le champ Value (valeur), utilisez le point-virgule (;) pour délimiter. Par exemple :

eng; vente; cn=VPN Augmented, ou=UTILISATEURS, o=OAG

Critères 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 portant 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 sont composés d'un numéro d'attribut et d'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 « Heures d'accès » a un ID Radius = 1, donc une valeur d'attribut DAP = 4096 + 1 = 4097.

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

Critères SAML

Vous pouvez configurer l'autorisation SAML et les sélections de stratégies de groupe à l'aide de DAP, sans avoir à vous fier 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 assertions d'authentification. Le composant du fournisseur de services SAML dans le périphérique de défense contre les menaces interprète les assertions SAML et effectue des sélections de stratégies d'autorisation ou de groupe en fonction des assertions reçues. Les attributs d'assertion sont traités à l'aide des règles DAP configurées dans le centre de gestion.

L'attribut des stratégies de groupe doit utiliser le nom d'attribut **cisco_group_policy**. Cet attribut ne dépend pas de la configuration d'une DAP. Cependant, si une DAP est configuré, elle peut être utilisée dans le cadre de la stratégie DAP.

Si un attribut avec le nom **cisco_group_policy** est reçu, la valeur correspondante est utilisée pour choisir la politique-groupe de connexion.

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

Attributs de terminal pris en charge dans une DAP

Pour obtenir la liste des fournisseurs d'anti-maliciels, de pare-feu et des applications que l'application HostScan peut détecter ainsi que les attributs de posture disponibles auprès des fournisseurs que nous prenons en charge, consultez le document HostScan Anti Malware and Firewall Support Graphiques (Graphiques de prise en charge d'anti-programmes malveillants et de pare-feu).

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.