Présentation de l'identité de l'utilisateur

Les rubriques suivantes traitent de l'identité de l'utilisateur :

À propos des identités d'utilisateur

Les informations sur l'identité de l'utilisateur peuvent vous aider à identifier la source des violations de politique, des attaques ou des vulnérabilités du réseau et de les retracer jusqu'à des utilisateurs spécifiques. Par exemple, vous pourriez déterminer :

- À qui appartient l'hôte ciblé par un incident d'intrusion qui a le niveau d'impact Vulnérabilité (niveau 1 : rouge).
- Qui a lancé une attaque interne ou un balayage de ports.
- Qui tente d'accéder sans autorisation à un hôte déterminé.
- Qui consomme une quantité déraisonnable de bande passante.
- Qui n'a pas appliqué de mises à jour essentielles du système d'exploitation.
- Qui utilise un logiciel de messagerie instantanée ou des applications de partage de fichiers homologue à homologue en violation de la politique de l'entreprise.
- Qui est associé à chaque indication de compromission sur votre réseau.

Fort de ces informations, vous pouvez utiliser d'autres fonctionnalités du système pour atténuer les risques, effectuer un contrôle d'accès et prendre des mesures pour protéger les autres contre les perturbations. Ces fonctionnalités améliorent également considérablement les contrôles d'audit et la conformité réglementaire.

Après avoir configuré les sources d'identité des utilisateurs pour recueillir des données des utilisateurs, vous pouvez effectuer la sensibilisation et le contrôle des utilisateurs.

Pour plus d'informations sur les sources d'identité, consultez À propos des sources d'identité d'utilisateur, à la page 2.

Sujets connexes

Terminologie de l'identité, à la page 2

À propos des sources d'identité d'utilisateur, à la page 2

Déploiements d'identité, à la page 5
Comment configurer une politique d'identité, à la page 10

Terminologie de l'identité

Cette rubrique traite des termes courants pour l'identité et le contrôle utilisateur.

Sensibilisation des utilisateurs

l'identification des utilisateurs de votre réseau à l'aide de *sources d'identité* (telles que ou l'agent TS). La connaissance des utilisateurs vous permet d'identifier les utilisateurs à partir de sources *faisant autorité* (comme Active Directory) et *ne faisant pas autorité* (basées sur les applications). Pour utiliser Active Directory comme source d'identité, vous devez configurer un domaine et un répertoire. Pour en savoir plus, consultez À propos des sources d'identité d'utilisateur, à la page 2.

Contrôle de l'utilisateur

Configurer une *politique d'identité* que vous associez à une *politique de contrôle d'accès*. (La politique d'identité est alors appelée *sous-politique* de contrôle d'accès.) La politique d'identité spécifie la source d'identité et, éventuellement, les utilisateurs et les groupes appartenant à cette source.

En associant la politique d'identité à une politique de contrôle d'accès, vous déterminez s'il faut surveiller, approuver, bloquer ou autoriser les utilisateurs ou l'activité des utilisateurs dans le trafic sur votre réseau. Pour en savoir plus, consultez Politiques de contrôle d'accès.

Sources d'identité autorisées

Un serveur de confiance a validé la connexion de l'utilisateur (par exemple, Active Directory). Vous pouvez utiliser les données obtenues à partir de connexions faisant autorité pour sensibiliser et contrôler l'utilisateur. Les connexions d'utilisateurs faisant autorité sont obtenues à partir d'authentifications passives et actives :

- *Les authentifications passives* se produisent lorsqu'un utilisateur s'authentifie par l'intermédiaire d'une source externe. ISE/ISE-PIC et l'agent TS sont les méthodes d'authentification passives prises en charge par le système Firepower.
- *Les authentifications actives* se produisent lorsqu'un utilisateur s'authentifie à l'aide de périphériques gérés préconfigurés. Le portail captif et le VPN d'accès à distance sont les méthodes d'authentification active prises en charge par le système Firepower.

Sources d'identité ne faisant pas autorité

Un serveur inconnu ou non fiable a validé la connexion de l'utilisateur. La détection basée sur le trafic est la seule source d'identité ne faisant pas autorité prise en charge par le système Firepower. Vous pouvez utiliser les données obtenues à partir des connexions ne faisant pas autorité pour sensibiliser les utilisateurs.

À propos des sources d'identité d'utilisateur

Le tableau suivant fournit un bref aperçu des sources d'identité des utilisateurs prises en charge par le système. Chaque source d'identité fournit un magasin d'utilisateurs pour la sensibilisation des utilisateurs. Ces utilisateurs peuvent ensuite être contrôlés à l'aide de politiques de contrôle d'identité et d'accès.

Source d'identité de l'utilisateur	Politique	Exigences en termes de serveur	Type	Type d'authentification	Sensibilisation des utilisateurs?	Contrôle par l'utilisateur?	Pour plus de renseignements, consultez...
ISE/ISE-PIC	Identité	Microsoft Active Directory	Connexions faisant autorité	Passif	Oui	Oui	Source d'identité ISE/ISE-PIC
Agent TS	Identité	Microsoft Windows Terminal Server	Connexions faisant autorité	Passif	Oui	Oui	La source d'identité de l'agent des services de terminaux (TS)
Portail captif	Identité	OpenLDAP Microsoft Active Directory	Connexions faisant autorité	Actif	Oui	Oui	Source d'identité du portail captif
VPN d'accès à distance	Identité	OpenLDAP ou Microsoft Active Directory	Connexions faisant autorité	Actif	Oui	Oui	La source d'identité du VPN d'accès à distance
	Identité	RADIUS	Connexions faisant autorité	Actif	Oui	Non	
Détection basée sur le trafic	Détection du réseau	S.O.	Connexions ne faisant pas autorité	S.O.	Oui	Non	La source d'identité de détection basée sur le trafic

Tenez compte des éléments suivants lors de la sélection des sources d'identité à déployer :

- Vous devez utiliser la détection basée sur le trafic pour les connexions utilisateur non LDAP.
- Vous devez utiliser la détection basée sur le trafic ou le portail captif pour enregistrer les échecs de connexion ou d'authentification. Un échec de connexion ou d'authentification n'ajoute pas un nouvel utilisateur à la liste des utilisateurs dans la base de données.
- La source d'identité du portail captif nécessite un périphérique géré avec une interface routée. Vous *ne pouvez pas* utiliser une interface en ligne (également appelée mode Tap) avec un portail captif.

Les données de ces sources d'identité sont stockées dans la base de données des utilisateurs et dans la base de données d'activités des utilisateurs de Cisco Secure Firewall Management Center. Vous pouvez configurer le téléchargements d'utilisateurs par serveur centre de gestion pour télécharger automatiquement et régulièrement de nouvelles données utilisateur dans vos bases de données.

Après avoir configuré les règles d'identité en utilisant la source d'identité souhaitée, vous devez associer chaque règle à une politique de contrôle d'accès et déployer la politique sur les périphériques gérés pour que la politique ait un effet. Pour plus d'informations sur les politiques de contrôle d'accès et leur déploiement, consultez Association d'autres politiques au contrôle d'accès.

Pour obtenir des informations générales sur l'identité de l'utilisateur, consultez À propos des identités d'utilisateur, à la page 1.

Bonnes pratiques pour l'identité de l'utilisateur

Nous vous recommandons de consulter les informations suivantes avant de configurer vos politiques d'identité.

- Connaître les limites du nombre d'utilisateurs
- Créer un domaine par domaine AD
- Moniteur d'intégrité
- Utiliser la dernière version d'ISE/ISE-PIC, deux types de correction
- Suppression de la prise en charge des agents utilisateurs dans la 6.7
- Le portail captif nécessite une interface routée et plusieurs tâches individuelles

Active Directory, LDAP et domaines

Le système Firepower prend en charge Active Directory ou LDAP pour la sensibilisation et le contrôle de l'utilisateur. L'association entre un répertoire Active Directory ou LDAP et FMC est ce qu'on appelle un *realm* (domaine). Vous devez créer un domaine par serveur LDAP ou domaine Active Directory. Pour plus de détails sur les versions prises en charge, consultez Serveurs pris en charge pour les domaines.

La seule source d'identité d'utilisateur prise en charge par LDAP est le portail captif. Pour utiliser d'autres sources d'identité (à l'exception d'ISE/ISE-PIC), vous devez utiliser Active Directory.

Pour Active Directory uniquement :

- Créez un *répertoire* par contrôleur de domaine.

  Pour de plus amples renseignements, consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine.

- Les utilisateurs et les groupes dans les relations d'approbation entre deux domaines sont pris en charge à condition que vous ajoutiez tous les domaines Active Directory et les contrôleurs de domaine en tant que domaines et répertoires, respectivement.

  Pour en savoir plus, consultez Domaines et domaines de confiance.

Séquence du serveur mandataire

Une *séquence de serveur mandataire* comprend un ou plusieurs périphériques gérés qui peuvent être utilisés pour communiquer avec un serveur LDAP, Active Directory ou ISE/ISE-PIC. Cela n'est nécessaire que si Cisco Defense Orchestrator (CDO) ne peut pas communiquer avec votre serveur Active Directory ou ISE/ISE-PIC. (Par exemple, CDO peut être dans un nuage public, mais Active Directory ou ISE/ISE-PIC peut se trouver dans un nuage privé.

Bien que vous puissiez utiliser un périphérique géré comme séquence mandataire , nous vous recommandons fortement d'en configurer deux ou plus de sorte que, si un périphérique géré ne peut pas communiquer avec Active Directory ou ISE/ISE-PIC, un autre périphérique géré puisse prendre le relais.

Utiliser la dernière version d'ISE/ISE-PIC

Si vous prévoyez utiliser la source d'identité ISE ou ISE-PIC, nous vous recommandons fortement de toujours utiliser la version la plus récente pour vous assurer d'obtenir les dernières fonctionnalités et corrections de bogues.

pxGrid 2.0 (qui est utilisé par la version 2.6, correctif 6 ou ultérieure; ou 2.7 correctif 2 ou ultérieure) modifie également la correction utilisée par ISE/ISE-PIC de Endpoint Protection Service (EPS) à Adaptive Network Control (ANC). Si vous mettez à niveau un ISE/ISE-PIC, vous devez migrer vos politiques de médiation d'EPS vers ANC.

Vous trouverez plus d'informations sur l'utilisation d'ISE/ISE-PIC dans Lignes directrices et limites ISE/ISE-PIC.

Pour configurer la source d'identité ISE/ISE-PIC, consultez Comment configurer ISE/ISE-PIC pour le contrôle utilisateur.

Informations sur le portail captif

Le portail captif est la seule source d'identité utilisateur pour laquelle vous pouvez utiliser LDAP ou Active Directory. En outre, vos périphériques gérés doivent être configurés pour utiliser une interface routée.

Des directives supplémentaires sont fournies dans Lignes directrices et limites relatives au portail captif.

La configuration d'un portail captif nécessite l'exécution de plusieurs tâches indépendantes. Pour en savoir plus, consultez Configurer le portail captif pour le contrôle utilisateur.

Renseignements sur les agents TS

La source d'identité de l'utilisateur de l'agent TS est requise pour identifier les sessions utilisateur sur un serveur de terminaux Windows. Le logiciel Agent TS doit être installé sur le serveur de terminaux, comme indiqué dans le *Guide des agents pour les services de terminaux de Cisco*. En outre, vous devez synchroniser l'heure de votre serveur d'agent TS avec celle de centre de gestion.

Les données des agents TS sont visibles dans les tableaux Utilisateurs, Activité des utilisateurs et Événement de connexion et peuvent être utilisées pour la sensibilisation et le contrôle de l'utilisateur.

Pour en savoir plus, consultez Directives pour les agents TS.

Associer la politique d'identité à une politique de contrôle d'accès

Après avoir configuré votre domaine, votre répertoire et votre source d'identité d'utilisateur, vous devez configurer des règles d'identité dans une politique d'identité. Pour que la politique prenne effet, vous devez associer la politique d'identité à une politique de contrôle d'accès.

Pour plus d'informations sur la création d'une politique d'identité, consultez Créer une politique d'identité.

Pour plus d'informations sur la création de règles d'identité, consultez Créer une règle d'identité.

Pour associer une politique d'identité à une politique de contrôle d'accès, consultez Association d'autres politiques au contrôle d'accès.

Déploiements d'identité

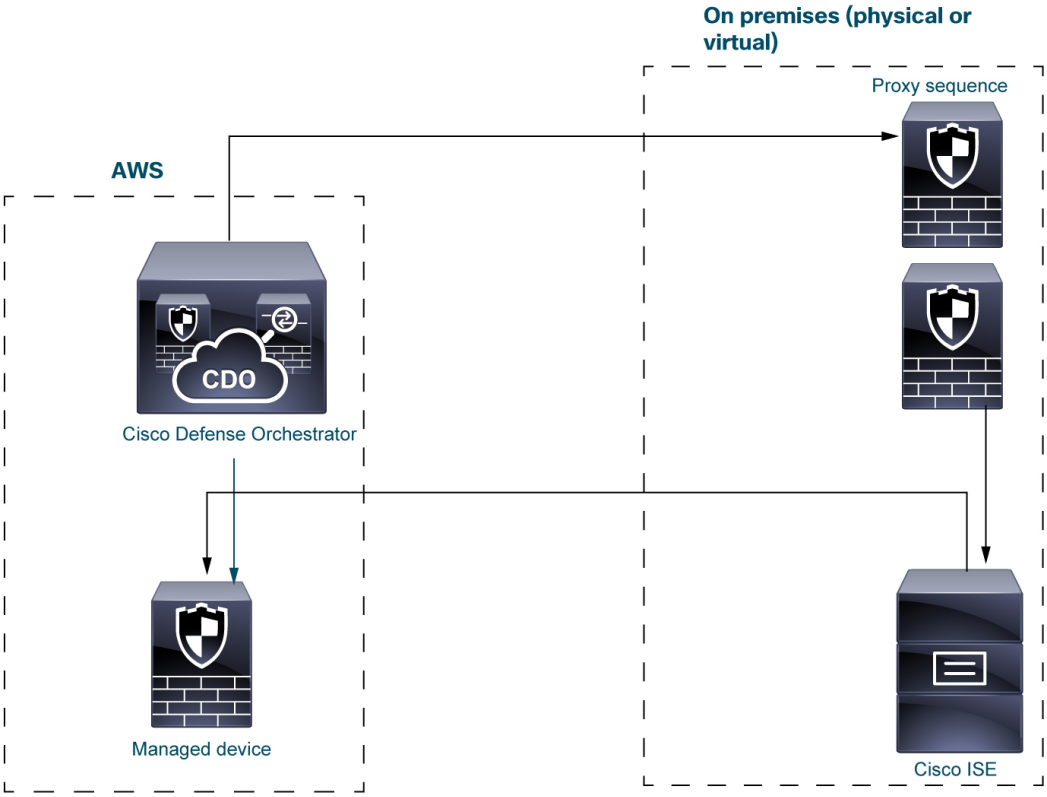
Lorsque le système détecte des données d'utilisateur provenant d'une connexion d'utilisateur, quelle que soit la source d'identité, l'utilisateur de la connexion est vérifié par rapport à la liste des utilisateurs dans la base de données d'utilisateurs centre de gestion . Si l'utilisateur de connexion correspond à un utilisateur existant,

les données de la connexion sont affectées à l'utilisateur. Les connexions qui ne correspondent pas à des utilisateurs existants entraînent la création d'un nouvel utilisateur, sauf si les connexions font partie du trafic SMTP. Les connexions non correspondantes dans le trafic SMTP sont rejetées.

Le groupe auquel l'utilisateur appartient est associé à l'utilisateur dès qu'il est vu par centre de gestion.

Exemples de déploiements d'identité

Les exemples de déploiement décrits dans cette section sont basés sur le système de la figure suivante.



Dans la figure précédente, CDO et un périphérique géré sont déployés sur AWS et les autres périphériques sont situés sur place. Ces périphériques peuvent être physiques ou virtuels; ils doivent simplement pouvoir communiquer entre eux.

Les deux périphériques gérés sur site sont destinés à être utilisés comme séquence mandataire. Vous devez également ajouter ces périphériques à CDO.

Une *séquence de serveur mandataire* comprend un ou plusieurs périphériques gérés qui peuvent être utilisés pour communiquer avec un serveur LDAP, Active Directory ou ISE/ISE-PIC. Cela n'est nécessaire que si Cisco Defense Orchestrator (CDO) ne peut pas communiquer avec votre serveur Active Directory ou ISE/ISE-PIC. (Par exemple, CDO peut être dans un nuage public, mais Active Directory ou ISE/ISE-PIC peut se trouver dans un nuage privé.

LDAP ou Active Directory sont nécessaires uniquement pour l'agent TS et le portail captif, comme l'expliquent les paragraphes suivants.

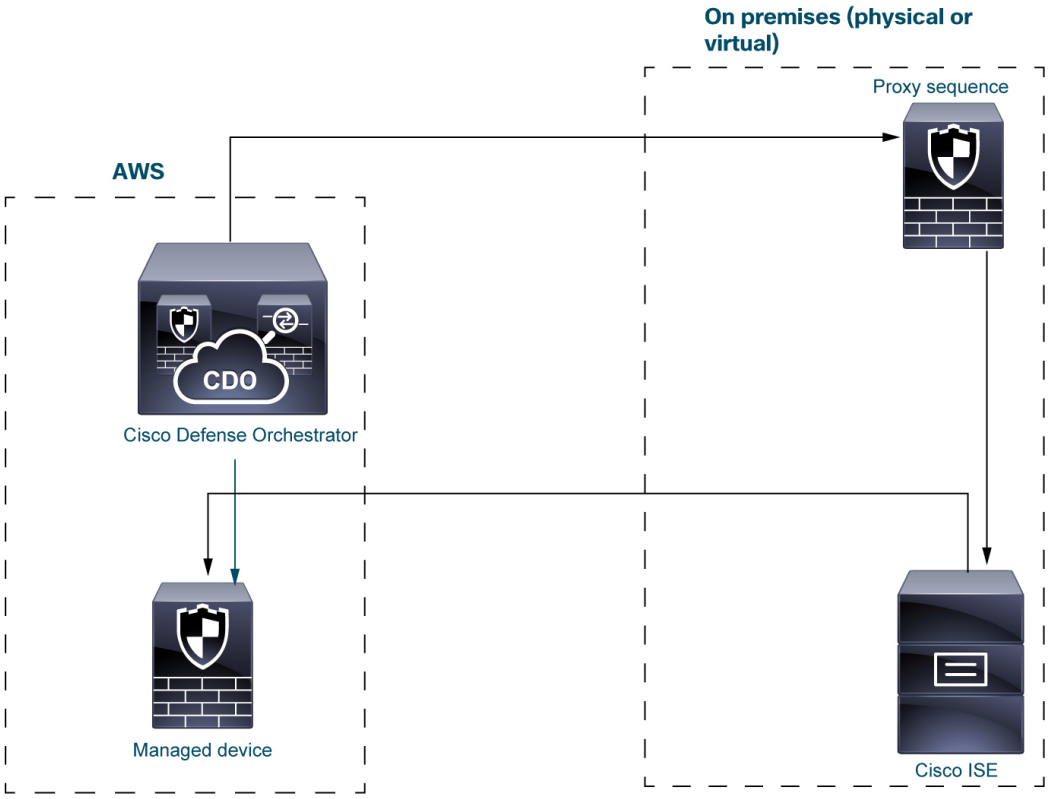
Pour plus d'informations sur la configuration d'un système comme celui-ci, consultez Comment configurer une politique d'identité, à la page 10.

Source d'identité ISE/ISE-PIC

Lorsque vous déployez la source d'identité ISE/ISE-PIC, CDO communique avec la séquence de serveur mandataire si CDO ne peut pas communiquer directement avec le serveur ISE/ISE-PIC. Les utilisateurs, les groupes et les abonnements sont envoyés du serveur ISE/ISE-PIC au périphérique géré dans AWS.

Vous pouvez éventuellement avoir un serveur LDAP dans un déploiement ISE/ISE-PIC, mais comme il est facultatif, il n'est pas illustré dans la figure suivante.

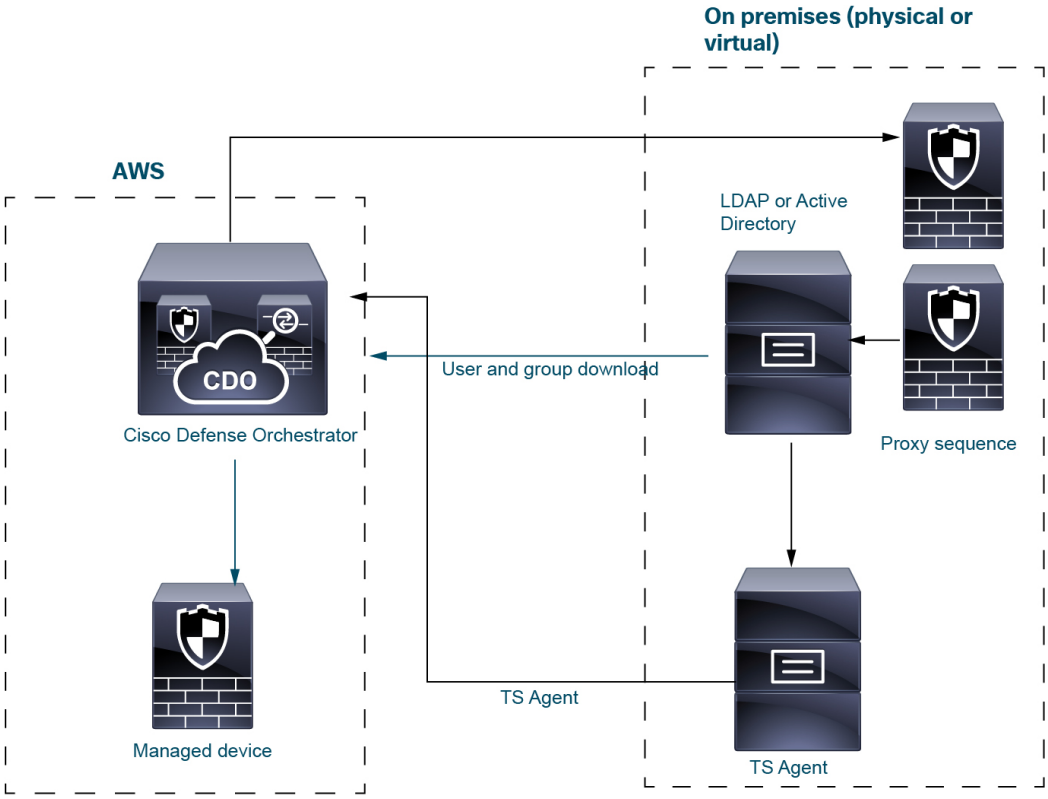
Pour plus d'informations sur ISE/ISE-PIC, consultez Source d'identité ISE/ISE-PIC.



Source d'identité de l'agent TS

L'agent des services de terminaux (TS) fonctionne sur un serveur Microsoft et envoie des informations sur l'utilisateur CDO en fonction de la plage de ports avec laquelle les utilisateurs se connectent au serveur. L'agent TS obtient les informations sur l'identité de l'utilisateur de LDAP ou d'Active Directory et les envoie à CDO.

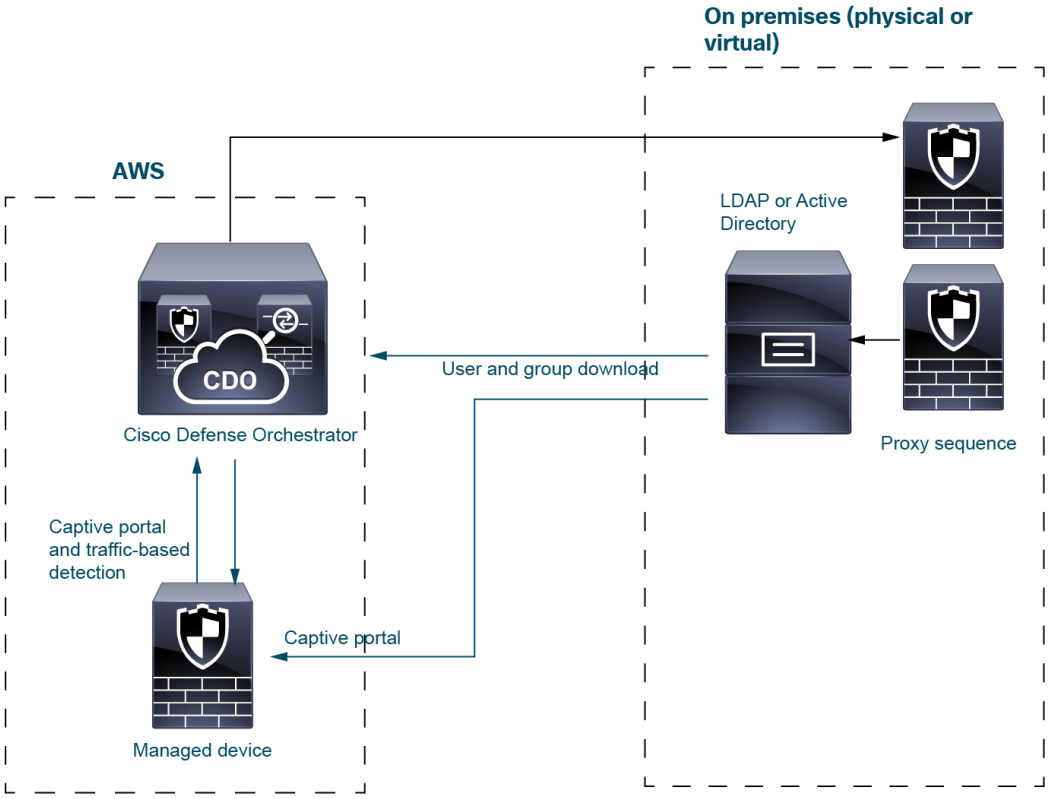
Pour en savoir plus sur la source d'identité de l'agent TS, consultez La source d'identité de l'agent des services de terminaux (TS).



Source d'identité du portail captif

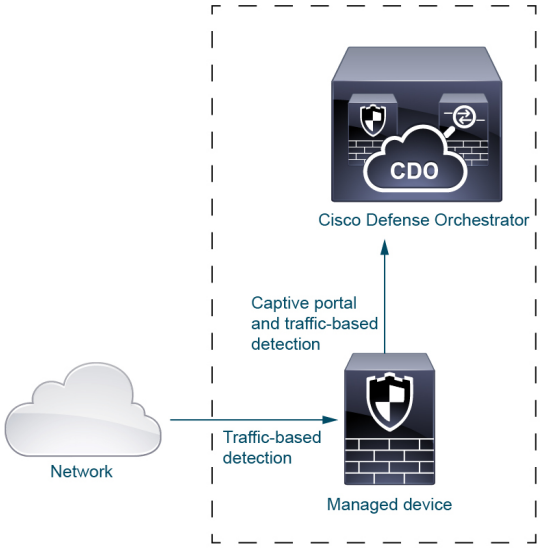
Le portail captif est la seule source d'identité à prendre en charge LDAP en plus d'Active Directory. La source d'identité du portail captif est déclenchée lorsqu'un utilisateur tente d'accéder aux ressources réseau à l'aide d'un périphérique géré dans AWS, à l'aide d'une adresse IP ou d'un nom d'hôte. Le portail captif obtient des informations sur les utilisateurs de LDAP ou d'Active Directory en utilisant la séquence mandataire et les envoie à CDO.

Pour plus d'informations sur la source d'identité du portail captif, consultez Source d'identité du portail captif.



Détection basée sur le trafic

La détection basée sur le trafic est conçue uniquement pour détecter les applications sur le réseau et n'a donc pas besoin d'un référentiel d'utilisateurs comme Active Directory ou d'une séquence mandataire. Pour plus d'informations , consultez À propos de la détection des données de l'hôte, de l'application et de l'utilisateur.



Comment configurer une politique d'identité

Cette rubrique fournit un aperçu général de la configuration d'une politique d'identité à l'aide de n'importe quelle source d'identité utilisateur disponible : agent TS, ISE/ISE-PIC, portail captif ou VPN d'accès à distance.

Procédure

	Commande ou action	Objectif
Étape 1	(Facultatif) Créez une séquence de serveur mandataire.	Une *séquence de serveur mandataire* comprend un ou plusieurs périphériques gérés qui peuvent être utilisés pour communiquer avec un serveur LDAP, Active Directory ou ISE/ISE-PIC. Cela n'est nécessaire que si Cisco Defense Orchestrator (CDO) ne peut pas communiquer avec votre serveur Active Directory ou ISE/ISE-PIC. (Par exemple, CDO peut être dans un nuage public, mais Active Directory ou ISE/ISE-PIC peut se trouver dans un nuage privé. Bien que vous puissiez utiliser un périphérique géré comme séquence mandataire , nous vous recommandons fortement d'en configurer deux ou plus de sorte que, si un périphérique géré ne peut pas communiquer avec Active Directory ou ISE/ISE-PIC, un autre périphérique géré puisse prendre le relais. Consultez Créer une séquence de serveur mandataire.
Étape 2	(Facultatif) Créez un domaine et un répertoire, un domaine pour chaque domaine de l'ensemble qui contient des utilisateurs que vous souhaitez utiliser dans le contrôle d'utilisateur. Créez également un répertoire pour chaque contrôleur de domaine. Seuls les utilisateurs et les groupes auxquels des domaines et des répertoires centre de gestion correspondent peuvent être utilisés dans les politiques d'identité.	La création d'un domaine, d'un répertoire de domaine d'une séquence de serveur mandataire est facultative si l'une des conditions suivantes est remplie : • Vous utilisez les conditions d'attribut SGT ISE, mais pas les conditions d'utilisateur, de groupe, de domaine, d'emplacement de point terminal ou de profil de point terminal. • Vous utilisez une politique d'identité uniquement pour filtrer le trafic réseau. • Une séquence proxy (de serveur mandataire) est nécessaire uniquement si vous utilisez Cisco Defense Orchestrator (CDO) et qu'elle ne peut pas communiquer directement avec Active Directory ou ISE/ISE-PIC.

	Commande ou action	Objectif
		Le *domaine* est un magasin d'utilisateurs et de groupes de confiance, généralement un référentiel Microsoft Active Directory. centre de gestion télécharge les utilisateurs et les groupes à des intervalles que vous spécifiez. Vous pouvez inclure ou exclure des utilisateurs et des groupes du téléchargement. Consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine. Pour en savoir plus sur les options de création d'un domaine, consultez Champs de domaine. Un *annuaire* est un contrôleur de domaine Active Directory qui organise les informations sur les utilisateurs et les partages réseau d'un réseau informatique. Un contrôleur Active Directory fournit des services d'annuaire pour le domaine. Active Directory répartit les objets d'utilisateur et de groupe sur plusieurs contrôleurs de domaine, qui sont des homologues qui propagent les modifications locales entre eux à l'aide des services d'annuaire. Pour en savoir plus, consultez le glossaire des spécifications techniques Active Directory sur MSDN. Vous pouvez spécifier plusieurs répertoires pour un domaine, auquel cas chaque contrôleur de domaine est interrogé dans l'ordre indiqué dans la page à onglet **Directory** (Répertoire) du domaine pour correspondre aux informations d'authentification de l'utilisateur et du groupe pour le contrôle de l'utilisateur. **Remarque** La configuration d'un domaine ou d'une séquence de domaine est facultative si vous prévoyez de configurer des conditions d'attribut ISE de la plateforme SGT, mais pas les conditions d'un utilisateur, d'un groupe, d'un domaine, d'un emplacement de point terminal ou de profil de point terminal.
Étape 3	Synchroniser les utilisateurs et les groupes du domaine.	Pour pouvoir contrôler les utilisateurs et les groupes, vous devez les synchroniser avec centre de gestion. Vous pouvez les synchroniser avec des utilisateurs et des

	Commande ou action	Objectif
		groupes quand vous le souhaitez, ou vous pouvez configurer le système pour les synchroniser à un intervalle précis. Lorsque vous synchronisez des utilisateurs et des groupes, vous pouvez spécifier des exceptions. par exemple, vous pouvez exclure le groupe d'ingénierie de tout contrôle utilisateur pour ce domaine, ou vous pouvez exclure l'utilisateur **`jean.dupont`** des contrôles utilisateur qui s'appliquent au groupe d'ingénierie. Reportez-vous à Synchroniser les utilisateurs et les groupes
Étape 4	(Facultatif) Créer une séquence de domaine.	Une séquence de domaine est une liste ordonnée de domaines qui, lorsqu'elle est utilisée dans une politique d'identité, amène le système à rechercher les domaines dans l'ordre spécifié pour trouver les utilisateurs correspondant à la règle. Consultez Créer une séquence de domaine.
Étape 5	Créez une méthode pour récupérer les données d'utilisateurs et de groupe (la *source d'identité*).	Définissez une source d'identité avec sa configuration unique pour pouvoir contrôler les utilisateurs et les groupes à l'aide des données stockées dans le domaine. Les sources d'identité comprennent l'agent TS, le portail captif ou le VPN distant. Consultez l'un des éléments suivants : • Configurer le portail captif pour le contrôle utilisateur • Configurer ISE/ISE-PIC pour le contrôle utilisateur • Configurer un VPN d'accès à distance pour le contrôle utilisateur
Étape 6	Créez une politique d'identité	Une politique d'identité contient une ou plusieurs règles d'identité, éventuellement organisées en catégories. Consultez Créer une politique d'identité.

	Commande ou action	Objectif
		Remarque La configuration d'un domaine ou d'une séquence de domaine est facultative si vous prévoyez de configurer des conditions d'attribut SGT ISE, mais pas les conditions d'utilisateur, de groupe, de domaine, d'emplacement de point terminal ou de profil de point terminal; ou si vous utilisez votre politique d'identité uniquement pour filtrer le trafic réseau.
Étape 7	Créez une ou plusieurs règles d'identité.	Les règles d'identité vous permettent de préciser un certain nombre de critères de correspondance, notamment le type d'authentification, les zones réseau, les réseaux ou la géolocalisation, les domaines, les séquences de domaines, etc. Consultez Créer une règle d'identité.
Étape 8	Associez votre politique d'identité à une politique de contrôle d'accès.	Une politique de contrôle d'accès filtre et inspecte éventuellement le trafic. Une politique d'identité doit être associée à une politique de contrôle d'accès pour avoir un effet. Consultez Association d'autres politiques au contrôle d'accès.
Étape 9	Déployez la politique de contrôle d'accès sur au moins un périphérique géré.	Pour utiliser votre politique de contrôle de l'activité des utilisateurs, la politique doit être déployée sur les périphériques gérés auxquels les clients se connectent. Consultez Déployer les modifications de configuration.
Étape 10	Suivre les activités de l'utilisateur	Afficher une liste des sessions actives, rassemblée par les sources d'identité des utilisateurs, ou une liste des informations sur les utilisateurs rassemblée par les sources d'identité des utilisateurs. . Une politique d'identité n'est pas requise si les conditions suivantes sont réunies : • Vous utilisez la source d'identité ISE/ISE-PIC. • Vous n'utilisez pas d'utilisateurs ni de groupes dans les politiques de contrôle d'accès. • Vous utilisez les balises de groupe de sécurité (SGT) dans les politiques de contrôle d'accès. Pour en savoir plus,

	Commande ou action	Objectif
		consultez Conditions de règle ISE SGT ou règle SGT personnalisée.

Sujets connexes

Configuration de la détection d'utilisateurs basée sur le trafic

Base de données sur les activités des utilisateurs

La base de données d'activités des utilisateurs du Cisco Secure Firewall Management Center contient des enregistrements des activités des utilisateurs sur votre réseau détectées ou signalées par toutes vos sources d'identité configurées. Le système consigne les événements dans les circonstances suivantes :

- Lorsqu'il détecte des connexions ou des déconnexions individuelles.
- Lorsqu'il détecte un nouvel utilisateur.
- Lorsqu'un administrateur système supprime manuellement un utilisateur.
- Lorsque le système détecte un utilisateur qui n'est pas dans la base de données, mais ne peut pas l'ajouter, car vous avez atteint votre limite d'utilisateurs.
- Lorsque vous résolvez une question d'indication de compromission associée à un utilisateur, ou activez ou désactivez les règles d'indication de compromission pour un utilisateur.

Remarque Si l'agent TS surveille les mêmes utilisateurs qu'une autre source d'identité avec authentification passive (telle que l'ISE/ISE-PIC), le centre de gestion priorise les données de l'agent TS. Si l'agent TS et une autre source passive signalent une activité identique à partir de la même adresse IP, seules les données de l'agent TS sont enregistrées dans centre de gestion.

Vous pouvez afficher l'activité des utilisateurs détectée par le système à l'aide de Cisco Secure Firewall Management Center. (**Analyse** > **Utilisateurs** > **Activité de l'utilisateur**.)

La base de données des utilisateurs

La base de données des utilisateurs sur Cisco Secure Firewall Management Center contient un enregistrement pour chaque utilisateur détecté ou signalé par toutes vos sources d'identité configurées. Vous pouvez utiliser les données obtenues auprès d'une source autorisée pour le contrôle utilisateur.

Consultez À propos des sources d'identité d'utilisateur, à la page 2 pour plus d'informations sur les sources d'identité faisant autorité, ne faisant pas autorité et prises en charge.

Le nombre total d'utilisateurs que Cisco Secure Firewall Management Center peut stocker dépend du modèle de Cisco Secure Firewall Management Center. Une fois la limite d'utilisateurs atteinte, le système priorise les données utilisateur non détectées précédemment en fonction de leur source d'identité, comme suit :

- Si le nouvel utilisateur provient d'une source d'identité ne faisant pas autorité, le système n'ajoute pas l'utilisateur à la base de données. Pour permettre l'ajout de nouveaux utilisateurs, vous devez supprimer les utilisateurs manuellement ou en purgeant la base de données.

- Si le nouvel utilisateur provient d'une source d'identité faisant autorité, le système supprime l'utilisateur ne faisant pas autorité qui est reste inactif pendant la plus longue période et ajoute le nouvel utilisateur à la base de données.

Si une source d'identité est configurée pour exclure des noms d'utilisateurs spécifiques, les données d'activités des utilisateurs pour ces noms d'utilisateur ne sont pas signalées à Cisco Secure Firewall Management Center. Ces noms d'utilisateurs exclus restent dans la base de données, mais ne sont pas associés aux adresses IP.

Si la haute disponibilité centre de gestion est configurée et que le périphérique principal tombe en panne, aucune connexion signalée par un portail captif, un ISE/ISE-PIC, un agent TS ou un périphérique VPN d'accès à distance ne peut être identifiée pendant le temps d'arrêt pour le basculement, même si les utilisateurs ont déjà été vus et téléchargés dans centre de gestion. Les utilisateurs non identifiés sont connectés en tant qu'utilisateurs inconnus sur centre de gestion. Après le temps d'arrêt, les utilisateurs inconnus sont réidentifiés et traités selon les règles de votre politique d'identité.

Remarque Si l'agent TS surveille les mêmes utilisateurs qu'une autre source d'identité avec authentification passive (ISE/ISE-PIC), centre de gestion priorise les données de l'agent TS. Si l'agent TS et une autre source passive signalent une activité identique à partir de la même adresse IP, seules les données de l'agent TS sont enregistrées dans centre de gestion.

Lorsque le système détecte une nouvelle session utilisateur, les données de la session utilisateur restent dans la base de données des utilisateurs jusqu'à ce que l'un des événements suivants se produise :

- Un utilisateur sur centre de gestion supprime manuellement la session utilisateur.
- Une source d'identité signale la déconnexion de cette session utilisateur.
- Un domaine met fin à la session utilisateur comme spécifié par le paramètre **Délai d'expiration de la session de l'utilisateur : Utilisateurs authentifiés**, **Délai d'expiration de la session utilisateur : Échec de l'authentification des utilisateurs**, or **Délai d'expiration de la session de l'utilisateur : Utilisateurs invités** .

Limites d'hôtes et d'utilisateurs de Cisco Defense Orchestrator

Limite d'hôtes Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Le Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) ajoute un hôte à la cartographie du réseau lorsqu'il détecte une activité associée à une adresse IP dans votre réseau surveillé (comme défini dans votre politique de découverte de réseau).

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) peut stocker un maximum de 600 000 hôtes dans sa base de données d'hôtes, mais nous vous recommandons ce qui suit.

Nombre de périphériques gérés par CDO	Nombre d'hôtes recommandés
1 à 50	100 000

Nombre de périphériques gérés par CDO	Nombre d'hôtes recommandés
51 à 300	300 000
30 à 1000	600 000

Vous ne pouvez pas afficher les données contextuelles des hôtes qui ne figurent pas dans la cartographie du réseau. Cependant, vous pouvez effectuer un contrôle d'accès. Par exemple, vous pouvez effectuer un contrôle des applications sur le trafic vers et à partir d'un hôte qui ne se trouve pas dans la cartographie du réseau, même si vous ne pouvez pas utiliser une liste de conformité autoriser pour surveiller la conformité du réseau de l'hôte.

Remarque Le système compte séparément les hôtes MAC uniquement des hôtes identifiés par des adresses IP et des adresses MAC. Toutes les adresses IP associées à un hôte sont comptées pour un seul hôte.

Atteinte de la limite d'hôte et suppression d'hôtes

La politique de découverte de réseau contrôle ce qui se passe lorsque vous détectez un nouvel hôte après avoir atteint la limite d'hôtes; vous pouvez supprimer le nouvel hôte ou remplacer l'hôte inactif depuis le plus longtemps. Vous pouvez également définir le délai au bout duquel le système supprime un hôte de la cartographie du réseau en raison de son inactivité. Bien que vous puissiez supprimer manuellement un hôte, un sous-réseau entier ou tous vos hôtes de la cartographie du réseau, si le système détecte une activité associée à un hôte supprimé, il rajoute l'hôte.

Dans un déploiement multidomaine, chaque domaine descendant a sa propre politique de découverte de réseau. Par conséquent, chaque domaine descendant régit son propre comportement lorsque le système découvre un nouvel hôte.

Limite d'utilisateurs de Cisco Defense OrchestratorCloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage)

Un utilisateur est ajouté à la base de données d'utilisateurs Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) dans les cas suivants :

- Le téléchargement de l'utilisateur se fait à partir d'un domaine.
- Un utilisateur de portail captif ou du VPN d'accès à distance se connecte.
- Un utilisateur est détecté à partir de n'importe quelle source d'identité (par exemple, un agent TS).

Un Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) peut stocker un maximum de 600 000 utilisateurs dans sa base de données hôte, mais nous vous recommandons ce qui suit.

Nombre de périphériques gérés par CDO	Nombre d'utilisateurs recommandé
1 à 50	100 000
51 à 300	300 000
30 à 1000	600 000

Seuls les utilisateurs faisant autorité sont disponibles pour le contrôle des utilisateurs avec des politiques de contrôle d'accès.

Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage) peut stocker 600 000 sessions dans sa base de données d'utilisateurs.

Lorsque le système détecte un nouvel utilisateur non détecté précédemment une fois la limite atteinte, il priorise les données de l'utilisateur en fonction de sa source d'identité :

- Si le nouvel utilisateur provient d'une source ne faisant pas autorité, le système ne l'ajoute pas à la base de données. Pour permettre l'ajout de nouveaux utilisateurs, vous devez supprimer des utilisateurs manuellement ou purger la base de données.
- Si le nouvel utilisateur provient d'une source d'identité faisant autorité, le système supprime l'utilisateur ne faisant pas autorité qui est reste inactif pendant la plus longue période et ajoute le nouvel utilisateur faisant autorité à la base de données.

  S'il n'y a que des utilisateurs faisant autorité, le système supprime l'utilisateur faisant autorité qui est devenu inactif le plus longtemps et ajoute le nouvel utilisateur à la base de données.

Vous trouverez des renseignements de dépannage dans Dépannage du contrôle d'utilisateur.

Astuces Notez que si vous utilisez la détection basée sur le trafic, vous pouvez restreindre la journalisation des utilisateurs par protocole pour aider à réduire l'encombrement lié aux noms d'utilisateur et à préserver de l'espace dans la base de données. Par exemple, vous pourriez empêcher le système d'ajouter les utilisateurs détectés dans le trafic AIM, POP3 et IMAP, car vous ne souhaitez pas surveiller le trafic de sous-traitants ou de visiteurs en particulier.

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.