Politiques d'identité de l'utilisateur

Les rubriques suivantes expliquent comment créer et gérer des règles et des politiques d'identité :

À propos des politiques d'identité

Les politiques d'identité contiennent des règles d'identité. Les règles d'identité associent des ensembles de trafic à un domaine et à une méthode d'authentification : authentification passive, authentification active ou aucune authentification.

À l'exception près indiquée dans les paragraphes suivants, vous devez configurer les domaines et les méthodes d'authentification que vous prévoyez utiliser avant de pouvoir les appeler dans vos règles d'identité :

- Vous configurez les domaines en dehors de votre politique d'identité, au **domaine d'** > **intégration** > **systèmes**. Pour en savoir plus, consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine.
- Pour configurer ISE/ISE-PIC, une source d'identité pour authentification passive, **consultez Sources d'identité** > **l'intégration** > **de systèmes**.
- Vous configurez l'agent TS, une source d'identité d'authentification passive, en dehors du système. Pour en savoir plus, consultez le *Guide de l'agent pour les services Cisco Terminal Services (TS)*.
- Vous configurez le portail captif, une source d'identité d'authentification active, dans la politique d'identité. Pour en savoir plus, consultez Configurer le portail captif pour le contrôle utilisateur.
- Vous configurez le VPN d'accès à distance, une source d'identité d'authentification active, dans les politiques de VPN d'accès à distance. Pour en savoir plus, consultez Authentification du VPN d'accès à distance.

Après avoir ajouté plusieurs règles d'identité à une politique d'identité unique, organisez les règles. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. La première règle qui correspond au trafic est la règle qui gère ce trafic.

Vous pouvez éventuellement configurer une politique d'identité pour filtrer le trafic par objet réseau, ce qui limite le réseau surveillé par chaque appareil dans le cas où vos périphériques ont atteint ou près de leurs limites de mémoire. Les périphériques doivent exécuter défense contre les menaces, version 6.7 ou ultérieure, pour leur appliquer le filtrage de réseau.

Après avoir configuré une ou plusieurs politiques d'identité, vous devez associer une politique d'identité à votre politique de contrôle d'accès. Lorsque le trafic sur votre réseau correspond aux conditions de votre règle d'identité, le système associe le trafic au domaine spécifié et authentifie les utilisateurs dans le trafic à l'aide de la source d'identité spécifiée.

Si vous ne configurez pas de politique d'identité, le système n'effectue pas l'authentification des utilisateurs.

Exception à la création d'une politique d'identité

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, consultez Conditions de règle ISE SGT ou règle SGT personnalisée.

Sujets connexes

Comment configurer une politique d'identité

Exigences de licence pour les politiques d'identité

Licence de défense contre les menaces

N'importe lequel

Licence traditionnelle

Contrôle

Exigences et conditions préalables pour les politiques d'identité

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

Créer une politique d'identité

Cette tâche explique comment créer une politique d'identité.

Avant de commencer

Une politique d'identité est requise pour utiliser les utilisateurs et les groupes d'un domaine dans les politiques de contrôle d'accès. Créez et activez un ou plusieurs domaines, comme décrit dans Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine.

(Facultatif) Si un périphérique géré particulier surveille un grand nombre de groupes d'utilisateurs, le système peut abandonner les mappages d'utilisateurs en fonction des groupes en raison des limites de mémoire du périphérique géré. Par conséquent, les règles assorties de conditions de domaine ou d'utilisateur peuvent ne pas fonctionner comme prévu. À condition que les périphériques exécutent la version 6.7 ou une version ultérieure, vous pouvez configurer la règle d'identité pour surveiller le trafic au moyen d'un seul objet de réseau ou de groupe de réseaux. Pour créer un objet réseau, consultez Création d'objets réseau.

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, consultez Conditions de règle ISE SGT ou règle SGT personnalisée.

Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Identity (identité)** et cliquez sur **New Policy** (Nouvelle politique).

Étape 3 Saisissez un **Name** (nom) et une **Description** facultative.

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

Étape 5 Pour ajouter une règle à la politique, cliquez sur **Add Rule** (ajouter une règle), comme décrit en Créer une règle d'identité, à la page 12.

Étape 6 Pour créer une catégorie de règles, cliquez sur **Add Category** (Ajouter une catégorie).

Étape 7 Pour configurer l'authentification active du portail captif, cliquez sur **Active Authentication** (Authentification active) et consultez Configurer le portail captif, partie 2 : créer une politique d'identité et une règle d'authentification active.

Étape 8 (Facultatif) Pour filtrer le trafic par objet réseau, cliquez sur l'onglet **Identity Source** (source d'identité). Dans la liste, cliquez sur l'objet réseau à utiliser pour filtrer le trafic pour cette politique d'identité. Cliquez sur **Ajouter** (+) pour créer un nouvel objet réseau.

Étape 9 Cliquez sur **Save** (Enregistrer) pour enregistrer la politique d'identité.

Prochaine étape

- Ajoutez des règles à votre politique d'identité qui précisent les utilisateurs à mettre en correspondance et d'autres options. voir Créer une règle d'identité, à la page 12.
- Associez la politique d'identité à une politique de contrôle d'accès pour autoriser ou empêcher les utilisateurs sélectionnés d'accéder à des ressources spécifiées; voir Association d'autres politiques au contrôle d'accès.
- Déployez les modifications de configuration sur les périphériques gérés; voir Déployer les modifications de configuration.

Si vous rencontrez des problèmes, consultez Dépannage du contrôle d'utilisateur, à la page 15.

Sujets connexes

Configurer le portail captif, partie 2 : créer une politique d'identité et une règle d'authentification active
Créer un filtre de mappage d'identité, à la page 4
Champs du portail captif
Dépannage du contrôle d'utilisateur, à la page 15

Créer un filtre de mappage d'identité

Un filtre de mappage d'identité peut être utilisé pour limiter les réseaux auxquels une règle d'identité s'applique. Par exemple, si votre centre de gestion gère des FTD qui ont une quantité de mémoire limitée, vous pouvez limiter les réseaux qu'ils surveillent.

Vous pouvez également exclure des sous-réseaux de la réception des mappages utilisateur-IP et de la balise de groupe de sécurité (SGT)-IP d'ISE. Vous devez généralement effectuer cette opération pour les périphériques gérés disposant de moins de mémoire afin d'éviter les erreurs de mémoire du moniteur d'intégrité d'identité Snort.

Avant de commencer

Effectuez les tâches suivantes :

1. Créez un domaine, qui est requis pour une politique d'identité. Consultez Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine.
2. Créez une politique d'identité Consultez Créer une politique d'identité, à la page 3.
3. (Facultatif) Créez un objet de réseau ou un groupe de réseaux comme décrit dans le Création d'objets réseau. L'objet ou le groupe de réseau que vous créez doit définir le réseau que les périphériques gérés doivent surveiller dans les politiques d'identité.

   Cette étape est facultative, car vous pouvez en créer une lorsque vous configurez le filtre de mappage d'identité.

Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Policies** > **Identity** (Politiques d'identité).

Étape 3 Cliquez sur **Modifier** ( ).

Étape 4 Cliquez sur l'onglet **Identity Source** (source d'identité).

Étape 5 Dans la liste du **filtre de mappage d'identité**, choisissez le nom d'un objet réseau à utiliser comme filtre ou cliquez sur **Plus** ( ) pour en créer un nouveau.

Pour créer un nouvel objet réseau, consultez Création d'objets réseau.

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

Étape 7 Déployez les modifications de configuration sur les périphériques gérés; voir Déployer les modifications de configuration.

Prochaine étape

Associez la politique d'identité à une politique de contrôle d'accès, comme indiqué dans Association d'autres politiques au contrôle d'accès.

Pour vérifier ou modifier les filtres de mappage d'identité d'ISE (également appelés *filtres de sous-réseau*), utilisez les commandes suivantes :

```
show identity-subnet-filter
configure identity-subnet-filter { add | remove } subnet
```

Conditions des règles d'identité

Les conditions de règles vous permettent d'affiner votre politique d'identité pour cibler les utilisateurs et les réseaux que vous souhaitez contrôler. Voir l'une des sections suivantes pour plus d'informations.

Sujets connexes

Conditions des règles de zone de sécurité
Conditions des règles de réseau
Conditions de règle des balises VLAN
Conditions de règle de port
Conditions des règles de domaine et de paramètres, à la page 9

Conditions des règles de zone de sécurité

Les zones de sécurité segmentent votre réseau pour vous aider à gérer et à classer le flux de trafic en regroupant les interfaces sur plusieurs périphériques.

Les conditions de règles de zone contrôlent le trafic en fonction de ses zones de sécurité de source et de destination. Si vous ajoutez des zones de source et de destination à une condition de zone, le trafic correspondant doit provenir d'une interface de l'une des zones de source et passer par une interface de l'une des zones de destination pour correspondre à la règle.

Tout comme toutes les interfaces d'une zone doivent être du même type (en ligne, passives, commutées ou routées), toutes les zones utilisées dans une condition de zone doivent être du même type. Comme les périphériques déployés de manière passive ne transmettent pas le trafic, vous ne pouvez pas utiliser une zone avec des interfaces passives comme zone de destination.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Astuces Restreindre les règles par zone est l'un des meilleurs moyens d'améliorer les performances du système. Si une règle ne s'applique pas au trafic via l'une des interfaces de périphérique, cette règle n'affecte pas les performances de ce périphérique.

Conditions des zones de sécurité et de la multilocalisation de détention

Dans un déploiement multidomaine, une zone créée dans un domaine ascendant peut contenir des interfaces qui résident sur des périphériques dans différents domaines. Lorsque vous configurez une condition de zone dans un domaine descendant, vos configurations s'appliquent uniquement aux interfaces que vous pouvez voir.

Conditions des règles de réseau

Les conditions des règles de réseau contrôlent le trafic en fonction de son adresse IP de source et de destination, à l'aide d'en-têtes internes. Les règles de tunnel, qui utilisent des en-têtes externes, ont des conditions de point terminal de tunnel au lieu de conditions de réseau.

Vous pouvez utiliser des objets prédéfinis pour créer des conditions de réseau ou spécifier manuellement des adresses IP individuelles ou des blocs d'adresses.

Remarque vous *ne pouvez pas* utiliser des objets réseau FDQN dans les règles d'identité.

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation d'adresses IP littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Conditions de règles de réseau pour la redirection vers le nom d'hôte

(Snort 3.0 uniquement) : vous pouvez utiliser un objet réseau qui contient le nom d'hôte complet (FQDN) de l'interface que le portail captif peut utiliser pour les demandes d'authentification actives.

Le nom de domaine complet doit correspondre à l'adresse IP de l'une des interfaces d'un périphérique géré. En utilisant un nom de domaine complet, vous pouvez attribuer un certificat pour l'authentification active que le client reconnaîtra, évitant ainsi que les utilisateurs reçoivent un avertissement de certificat non fiable lorsqu'ils sont redirigés vers une adresse IP.

Le certificat peut préciser un nom de domaine complet, un nom de domaine complet générique ou plusieurs noms de domaine complets sous les autres noms de l'objet (SAN) du certificat.

Si une règle d'identité requiert une authentification active pour un utilisateur, mais que vous ne précisez pas de nom de domaine complet de redirection, l'utilisateur sera redirigé vers le port du portail captif de l'interface de connexion.

Si vous ne pouvez pas fournir un nom de domaine complet de redirection vers l'hôte (Redirect to Host Name), les méthodes d'authentification HTTP de base, la page de réponse HTTP et NTLM redirigent l'utilisateur vers le portail captif en utilisant l'adresse IP de l'interface. Toutefois, pour la négociation HTTP, l'utilisateur est redirigé à l'aide du nom DNS complet *firewall-hostname.directory-server-domain-name*. Pour utiliser la négociation HTTP sans nom de domaine complet de redirection vers l'hôte (Redirect to Host Name), vous devez également mettre à jour votre serveur DNS pour mapper ce nom avec les adresses IP de toutes les interfaces internes pour lesquelles une authentification active est requise. Sinon, la redirection ne peut pas être terminée et les utilisateurs ne peuvent pas s'authentifier.

Nous vous recommandons de toujours fournir un nom de domaine complet de redirection vers le nom d'hôte (Redirect to Host Name) pour assurer un comportement cohérent, quelle que soit la méthode d'authentification.

Conditions de règle des balises VLAN

Remarque Les balises VLAN dans les règles d'accès s'appliquent uniquement aux ensembles en ligne. Les règles d'accès avec des balises VLAN ne correspondent pas au trafic sur les interfaces de pare-feu.

Les conditions de règles VLAN contrôlent le trafic balisé VLAN, y compris le trafic Q-in-Q (VLAN empilés). Le système utilise la balise VLAN la plus à l'intérieur pour filtrer le trafic VLAN, à l'exception de la politique de préfiltre, qui utilise la balise VLAN la plus à l'extérieur dans ses règles.

Notez les éléments suivants :

- Défense contre les menaces sur les périphériques Firepower 4100/9300 : ne prend pas en charge Q-in-Q (ne prend pas en charge une seule balise VLAN).
- Défense contre les menaces Pour tous les autres modèles :
  - Ensembles en ligne et interfaces passives : prend en charge Q-in-Q, jusqu'à 2 balises VLAN.
  - Interfaces de pare-feu : ne prennent pas en charge Q-in-Q (ne prend en charge qu'une seule balise VLAN).

Vous pouvez utiliser des objets prédéfinis pour créer des conditions VLAN ou saisir manuellement une balise VLAN entre 1 et 4094. Utilisez un tiret pour spécifier une plage de balises VLAN.

Dans une grappe, si vous rencontrez des problèmes de correspondance VLAN, modifiez les options avancées de la politique de contrôle d'accès, les paramètres de préprocesseur de transport/réseau, et sélectionnez l'option **Ignore the VLAN header when tracking connections** (Ignorer l'en-tête VLAN lors du suivi des connexions).

Remarque Le système crée une carte réseau distincte pour chaque domaine enfant. Dans un déploiement multidomaine, l'utilisation de balises VLAN littérales pour limiter cette configuration peut avoir des résultats inattendus. L'utilisation d'objets de substitution permet aux administrateurs de domaines descendants d'adapter les configurations globales à leurs environnements locaux.

Conditions de règle de port

Les conditions de port vous permettent de contrôler le trafic en fonction de ses ports source et de destination.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Bonnes pratiques pour les règles basées sur le port

La définition des ports est la façon traditionnelle de cibler des applications. Cependant, les applications peuvent être configurées pour utiliser des ports uniques afin de contourner les blocages de contrôle d'accès. Ainsi, chaque fois que cela est possible, utilisez les critères de filtrage des applications plutôt que les critères de port pour cibler le trafic.

Le filtrage des applications est également recommandé pour les applications, comme FTD, qui ouvrent des canaux distincts de manière dynamique pour le contrôle par rapport au flux de données. L'utilisation de règles de contrôle d'accès par port peut empêcher ce type d'applications de fonctionner correctement et peut entraîner le blocage des connexions souhaitables.

Utilisation des contraintes de ports source et de destination

Si vous ajoutez des ports source et de destination à une condition, vous ne pouvez ajouter que des ports partageant un seul protocole de transport, TCP ou UDP). Par exemple, si vous ajoutez DNS sur TCP comme port source, vous pouvez ajouter Cisco Messenger Voice Chat (TCP) comme port de destination, mais pas Cisco Messenger Voice Chat (UDP).

Si vous ajoutez uniquement des ports sources ou uniquement des ports de destination, vous pouvez ajouter des ports qui utilisent différents protocoles de transport. Par exemple, vous pouvez ajouter DNS sur TCP et DNS sur UDP comme conditions de port source dans une seule règle de contrôle d'accès.

Conditions de règle de port, de protocole et de code ICMP

Les conditions des ports correspondent au trafic en fonction des ports de source et de destination. Selon le type de règle, le « port » peut signifier l'un des éléments suivants :

- TCP et UDP : vous pouvez contrôler le trafic TCP et UDP en fonction du port. Le système représente cette configuration à l'aide du numéro de protocole entre parenthèses, ainsi que d'un port ou d'une plage de ports facultatif. Par exemple : TCP(6)/22.
- ICMP : vous pouvez contrôler le trafic ICMP et ICMPv6 (IPv6-ICMP) en fonction de son protocole de couche Internet, ainsi que d'un type et d'un code facultatifs. Par exemple : ICMP(1):3:3.
- Protocol (protocole) : Vous pouvez contrôler le trafic à l'aide d'autres protocoles qui n'utilisent pas de ports.

Dans la mesure du possible, laissez les critères de correspondance vides, en particulier ceux pour les zones de sécurité, les objets réseau et les objets de port. Lorsque vous précisez plusieurs critères, le système doit être en correspondance avec l'ensemble des contenus du critères que vous précisez.

Bonnes pratiques pour les règles basées sur le port

La définition des ports est la façon traditionnelle de cibler des applications. Cependant, les applications peuvent être configurées pour utiliser des ports uniques afin de contourner les blocages de contrôle d'accès. Ainsi, chaque fois que cela est possible, utilisez les critères de filtrage des applications plutôt que les critères de port pour cibler le trafic. Notez que le filtrage des applications n'est pas disponible dans les règles de préfiltre.

Le filtrage des applications est également recommandé pour les applications, comme FTP, qui ouvrent des canaux distincts de manière dynamique pour le contrôle par rapport au flux de données. L'utilisation de règles de contrôle d'accès par port peut empêcher ce type d'applications de fonctionner correctement et peut entraîner le blocage des connexions souhaitables.

Utilisation des contraintes de ports source et de destination

Si vous ajoutez des ports source et de destination à une condition, vous ne pouvez ajouter que des ports partageant un seul protocole de transport, TCP ou UDP). Par exemple, si vous ajoutez DNS sur TCP comme port source, vous pouvez ajouter Cisco Messenger Voice Chat (TCP) comme port de destination, mais pas Cisco Messenger Voice Chat (UDP).

Si vous ajoutez uniquement des ports sources ou uniquement des ports de destination, vous pouvez ajouter des ports qui utilisent différents protocoles de transport. Par exemple, vous pouvez ajouter DNS sur TCP et DNS sur UDP comme conditions de port de destination dans une seule règle de contrôle d'accès.

Mise en correspondance du trafic non TCP avec les conditions du port

Vous pouvez mettre en correspondance des protocoles non basés sur les ports. Par défaut, si vous ne spécifiez pas de condition de port, vous faites correspondre le trafic IP. Bien que vous puissiez configurer des conditions de port pour qu'elles correspondent au trafic non-TCP, il existe certaines restrictions :

- Access control Rules : Pour les périphériques classiques, vous pouvez faire correspondre le trafic encapsulé en GRE avec une règle de contrôle d'accès en utilisant le protocole GRE (47) comme condition de port de destination. À une règle soumise à des contraintes GRE, vous pouvez ajouter uniquement des conditions basées sur le réseau : zone, adresse IP, port et balise VLAN. En outre, le système utilise des en-têtes externes pour faire correspondre **tout** le trafic dans les politiques de contrôle d'accès avec les règles contraintes de GRE. Pour les périphériques défense contre les menaces, utilisez les règles de tunnel dans la politique de préfiltre pour contrôler le trafic encapsulé GRE.
- Règlesdedéchiffrement : ces règles prennent uniquement en charge les conditions de port TCP.
- ÉCHO IMCP : un port ICMP de destination avec le type défini à 0 ou un port ICMPv6 de destination avec le type défini à 129 correspond uniquement aux réponses écho non sollicitées. Les réponses ECHO ICMP envoyées en réponse aux demandes ECHO ICMP sont ignorées. Pour qu'une règle corresponde à n'importe quel écho ICMP, utilisez ICMP de type 8 ou ICMPv6 de type 128.

Conditions des règles de domaine et de paramètres

La page à onglet **Domaine et paramètres** vous permet de choisir un domaine ou une séquence de domaines auxquels appliquer la règle d'identité. Si vous utilisez un portail captif, vous avez des options supplémentaires.

Domaine d'authentification

Dans la liste **Realm** (Domaine), cliquez sur un domaine ou une séquence de domaines.

Le domaine ou la séquence de domaines contenant les utilisateurs sur lesquels vous souhaitez effectuer l'**action** spécifiée. Vous devez configurer entièrement un domaine ou une séquence de domaines avant de le sélectionner comme domaine dans une règle d'identité.

Remarque Si le VPN d'accès à distance est activé et que votre déploiement utilise un groupe de serveurs RADIUS pour l'authentification VPN, veillez à préciser le domaine associé à ce groupe de serveurs RADIUS.

Authentification active uniquement : autres options

Si vous choisissez l'**authentification active** comme type d'authentification ou si vous cochez la case **Use active authentication if passive or VPN identity cannot be established** (Utiliser l'authentification active si l'identité passive ou VPN ne peut être établie.), vous avez les options suivantes.

Utiliser une authentification active si une identité passive ou VPN ne peut pas être établie

(Règle d'authentification passive uniquement.) La sélection de cette option authentifie les utilisateurs à l'aide de l'authentification active du portail captif si une authentification passive ou VPN ne parvient pas à les identifier. Vous devez configurer une règle d'authentification active dans votre politique d'identité pour sélectionner cette option. (C'est-à-dire que les utilisateurs doivent s'authentifier à l'aide du portail captif.)

Si vous désactivez cette option, les utilisateurs qui n'ont pas d'identité VPN ou que l'authentification passive ne peut pas identifier sont identifiés comme inconnus.

Consultez également l'explication de la liste des domaines d'**authentification** plus loin dans cette rubrique,

Reconnaître par identités spéciales ou invité si l'authentification ne peut pas reconnaître l'utilisateur

La sélection de cette option permet aux utilisateurs qui échouent à l'authentification active sur le portail captif le nombre de fois spécifié d'accéder à votre réseau en tant qu'invité. Ces utilisateurs apparaissent dans centre de gestion identifiés par leur nom d'utilisateur (si leur nom d'utilisateur existe sur le serveur AD ou LDAP) ou par le nom **Invité** (si leur nom d'utilisateur est inconnu). Leur domaine est le domaine spécifié dans la règle d'identité. (Par défaut, le nombre de connexions échouées est de 3.)

Ce champ s'affiche uniquement si vous configurez l'**authentification active** (c'est-à-dire l'authentification du portail captif) comme **action** de règle.

Authentication Protocol (Protocole d'authentification)

La méthode à utiliser pour effectuer l'authentification active sur le portail captif. .

Les sélections varient selon le type de domaine, LDAP ou AD :

- Choisissez **HTTP de base** si vous souhaitez authentifier les utilisateurs à l'aide d'une connexion d'authentification de base HTTP (BA) non chiffrée. Les utilisateurs se connectent au réseau en utilisant la fenêtre contextuelle d'authentification par défaut de leur navigateur.

  La plupart des navigateurs Web mettent en cache les informations d'authentification des connexions **HTTP de base** et utilisent les informations d'authentification pour commencer en toute transparence une nouvelle session après l'expiration d'une ancienne session.

- Choisissez **NTLM** pour authentifier les utilisateurs à l'aide d'une connexion NT LAN Manager (NTLM). Cette sélection est uniquement disponible lorsque vous sélectionnez un domaine AD. Si l'authentification transparente est configurée dans le navigateur d'un utilisateur, l'utilisateur est automatiquement connecté. Si l'authentification transparente n'est pas configurée, les utilisateurs se connectent au réseau à l'aide de la fenêtre contextuelle d'authentification par défaut de leur navigateur.
- Choisissez **Kerberos** pour authentifier les utilisateurs à l'aide d'une connexion Kerberos. Cette sélection est disponible uniquement lorsque vous sélectionnez un domaine AD pour un serveur pour lequel la sécurisation LDAP (LDAPS) est activée. Si l'authentification transparente est configurée dans le navigateur d'un utilisateur, l'utilisateur est automatiquement connecté. Si l'authentification transparente n'est pas configurée, les utilisateurs se connectent au réseau à l'aide de la fenêtre contextuelle d'authentification par défaut de leur navigateur.

Remarque Le **domaine** que vous sélectionnez doit être configuré avec un nom d'**utilisateur AD Join** et un **mot de passe AD Join** pour effectuer l'authentification active sur le portail captif Kerberos.

Remarque Si vous créez une règle d'identité pour effectuer le portail captif Kerberos et que vous avez configuré la résolution DNS, vous devez configurer votre serveur DNS pour résoudre le nom de domaine complet (FQDN) du périphérique du portail captif. Le nom de domaine complet (FQDN) doit correspondre au nom d'hôte que vous avez fourni lors de la configuration du DNS.

Pour les périphériques défense contre les menaces, le nom de domaine complet doit résoudre l'adresse IP de l'interface routée utilisée pour le portail captif.

- Choisissez **HTTP Negotiate** (négocier HTTP) pour permettre au serveur de portail captif de choisir entre HTTP de base, Kerberos ouNTLM pour la connexion d'authentification. Ce type est uniquement disponible lorsque vous sélectionnez un domaine AD.

Remarque Le **domaine** que vous choisissez doit être configuré avec un nom d'**utilisateur AD Join** et un **mot de passe AD Join** pour que **HTTP Negociate** choisisse l'authentification active sur le portail captif Kerberos.

Remarque Si vous créez une règle d'identité pour effectuer une **négociation HTTP HTTP Negotiate** sur le portail captif et que la résolution DNS est configurée, vous devez configurer votre serveur DNS pour résoudre le nom de domaine complet (FQDN) du périphérique du portail captif. Le nom de domaine complet du périphérique que vous utilisez pour le portail captif doit correspondre au nom d'hôte que vous avez fourni lors de la configuration du DNS.

- Choisissez **HTTP Response Page** (PAge de réponse HTTP) pour permettre aux utilisateurs de choisir un domaine auquel se connecter.

  Vous pouvez éventuellement personnaliser la page de réponse; Par exemple, pour se conformer aux normes de style de l'entreprise.

Créer une règle d'identité

Pour en savoir plus sur les options de configuration des règles d'identité, consultez Champs de la règle d'identité, à la page 13.

Avant de commencer

Vous devez créer et activer un domaine ou une séquence de domaine.

- Créez un domaine et un répertoire de domaine Microsoft Active Directory, comme indiqué dans Créer un domaine LDAP ou un domaine Active Directory et un répertoire de domaine.
- (Facultatif) Créez une séquence de domaine comme indiqué dans Créer une séquence de domaine.

⚠

Mise en garde Ajout de la première ou suppression de la dernière règle d'authentification active lorsque le déchiffrement TLS/SSL est désactivé (c'est-à-dire lorsque la politique de contrôle d'accès ne comprend pas de règles d'authentification). u de déchiffrement) redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort pour obtenir de plus amples renseignements.

Notez qu'une règle d'authentification active comporte soit une action de règle d'authentification active (**Active Authentication**), soit une action de règle d'authentification passive (**Passive Authentication**) dont l'option **Use active authentication if passive or VPN identity cannot be established** (utiliser l'authentification active si l'identité passive ou VPN ne peut pas être établie) est sélectionnée.

Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Identity (identité)** .

Étape 3 Cliquez sur **Edit** (✎) à côté de la politique d'identité à laquelle ajouter la règle d'identité.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Add Rule** (ajouter une règle).

Étape 5 Saisissez un **Nom**.

Étape 6 Si la règle spécifiée s'applique, cochez la case **Enabled**(Activé).

Étape 7 Pour ajouter la règle à une catégorie existante, indiquez l'endroit où vous souhaitez **insérer** la règle. Pour ajouter une nouvelle catégorie, cliquez sur **Add Catégorie** (Ajouter une catégorie).

Étape 8 Choisissez une **action** de règle dans la liste.

Étape 9 Si vous configurez un portail captif, consultez Configurer le portail captif pour le contrôle utilisateur.

Étape 10 (Facultatif) Pour ajouter des conditions à la règle d'identité, consultez Conditions des règles d'identité, à la page 5.

Étape 11 Cliquez sur **Add** (ajouter).

Étape 12 Dans l'éditeur de politique, définissez la position de la règle. Cliquez dessus et faites-la glisser ou utilisez le menu contextuel pour la couper et la coller. Les règles sont numérotées à partir de 1. Le système fait correspondre le trafic aux règles en ordre descendant par numéro de règle croissant. La première règle qui correspond au trafic est la règle qui gère ce trafic. Un bon ordre des règles réduit les ressources nécessaires pour traiter le trafic réseau et empêche la préemption des règles.

Étape 13 Cliquez sur **Save** (enregistrer).

Prochaine étape

- Déployer les changements de configuration.

Champs de la règle d'identité

Utilisez les champs suivants pour configurer les règles d'identité.

Activé

L'activation de cette option active la règle d'identité dans la politique d'identité. Désélectionner cette option désactive la règle d'identité.

Action

Précisez le type d'authentification que vous souhaitez effectuer sur les utilisateurs dans le domaine spécifié : **Passive Authentication** (par défaut), **Active Authentication** ou **No Authentication** (Authentification passive, active ou absence d'authentification). Vous devez configurer entièrement la méthode d'authentification, ou la *source d'identité*, avant de la sélectionner comme action dans une règle d'identité.

En outre, si le VPN est activé (configuré sur au moins un périphérique géré), les sessions d'accès à distance sont authentifiées activement par le VPN. Les autres sessions utilisent la règle Action. Cela signifie que, si VPN est activé, la détermination de l'identité VPN est effectuée en premier pour toutes les sessions, quelle que soit l'action sélectionnée. Si une identité VPN est trouvée dans le domaine spécifié, il s'agit de la source d'identité utilisée. Aucune authentification active supplémentaire sur le portail captif n'est effectuée, même si cette option est sélectionnée.

Si la source d'identité VPN est introuvable, le processus se poursuit selon l'action spécifiée. Vous ne pouvez pas restreindre la politique d'identité à l'authentification VPN uniquement, car si l'identité VPN est introuvable, la règle est appliquée en fonction de l'action sélectionnée.

⚠

Mise en garde Ajout de la première ou suppression de la dernière règle d'authentification active lorsque le déchiffrement TLS/SSL est désactivé (c'est-à-dire lorsque la politique de contrôle d'accès ne comprend pas de règles d'authentification). redémarre le processus Snort lorsque vous déployez des modifications de configuration, interrompant temporairement l'inspection du trafic. Pendant cette interruption, la diminution de trafic ou son passage sans inspection dépend de la façon dont l'appareil cible gère le trafic. Consultez Comportement du trafic au redémarrage de Snort pour obtenir de plus amples renseignements.)

Notez qu'une règle d'authentification active comporte soit une action de règle d'authentification active (**Active Authentication**), soit une action de règle d'authentification passive (**Passive Authentication**) dont l'option **Use active authentication if passive or VPN identity cannot be established** (utiliser l'authentification active si l'identité passive ou VPN ne peut pas être établie) est sélectionnée.

Pour en savoir plus sur les méthodes d'authentification passive et active prises en charge dans votre version du système, consultez À propos des sources d'identité d'utilisateur.

Gérer une politique d'identité

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Identity (identité)** .

Étape 3 Pour supprimer une politique, cliquez sur **Supprimer** ( ). Si les contrôles sont grisés, la configuration est soit héritée d'une politique ancêtre ou vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Pour modifier une politique, cliquez sur **Edit** ( ) à côté de la politique et apportez les modifications comme décrit dans Créer une politique d'identité, à la page 3. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 5 Pour copier une politique, cliquez sur **Copier** ( ).

Étape 6 Pour générer un rapport pour la politique, cliquez sur **Rapport** ( ) comme décrit dans Générer des rapports sur les politiques appliquées.

Étape 7 Pour comparer les politiques, consultez Comparer les stratégies.

Étape 8 Pour créer un dossier dans lequel organiser les politiques, cliquez sur **Ajouter une catégorie**.

Prochaine étape

Déployer les changements de configuration.

Gérer une règle d'identité

Procédure

Étape 1 Connectez-vous au centre de gestion.

Étape 2 Cliquez sur **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Identity (identité)** .

Étape 3 Cliquez sur **Edit** ( ) (Modifier) à côté de la politique que vous souhaitez modifier. Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Pour modifier une règle d'identité, cliquez sur **Edit** ( ) et apportez les modifications nécessaires comme décrit dans Créer une politique d'identité, à la page 3.

Étape 5 Pour supprimer une règle d'identité, cliquez sur **Supprimer** ( ).

Étape 6 Pour créer une catégorie de règles, cliquez sur **Add Catégorie** (ajouter une catégorie), puis choisissez la position et la règle.

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

Prochaine étape

- Déployer les changements de configuration.

Dépannage du contrôle d'utilisateur

Si vous remarquez un comportement inattendu des règles d'utilisateur, envisagez de modifier le réglage de vos configurations de règles, de source d'identité ou de domaine. Pour d'autres renseignements de dépannage, consultez :

- Dépanner les problèmes ISE/ISE-PIC ou Cisco TrustSec
- Dépannage de la source d'identité de l'agent TS
- Dépannage de la source d'identité du portail captif
- Résoudre les problèmes liés aux domaines et aux téléchargements d'utilisateurs

Les règles ciblant les domaines, les utilisateurs ou les groupes d'utilisateurs ne correspondent pas au trafic

Si vous configurez un agent TS ou un périphérique ISE/ISE-PIC pour surveiller un grand nombre de groupes d'utilisateurs, ou si vous avez un très grand nombre d'utilisateurs mappés aux hôtes de votre réseau, le système peut supprimer les enregistrements d'utilisateurs en raison de votre limite d'utilisateurs Cisco Secure Firewall Management Center. Par conséquent, les règles avec des conditions utilisateur peuvent ne pas correspondre au trafic comme prévu.

Les règles ciblant des groupes d'utilisateurs ou des utilisateurs au sein de groupes d'utilisateurs ne correspondent pas au trafic attendu

Si vous configurez une règle avec une condition de groupe d'utilisateurs, votre serveur LDAP ou Active Directory doit avoir des groupes d'utilisateurs configurés. Le système ne peut pas effectuer le contrôle des groupes d'utilisateurs si le serveur organise les utilisateurs selon une hiérarchie d'objets de base.

Les règles ciblant les utilisateurs des groupes secondaires ne correspondent pas au trafic attendu

Si vous configurez une règle avec une condition de groupe d'utilisateurs qui inclut ou exclut les utilisateurs membres d'un groupe secondaire sur votre serveur Active Directory, votre serveur limite peut-être le nombre d'utilisateurs qu'il signale.

Par défaut, les serveurs Active Directory limitent le nombre d'utilisateurs des groupes secondaires. Vous devez personnaliser cette limite de sorte que tous les utilisateurs de vos groupes secondaires soient signalés à Cisco Secure Firewall Management Center et puissent être utilisés dans les règles avec conditions utilisateur.

Les règles ne correspondent pas aux utilisateurs lorsqu'elles sont vues pour la première fois

Après avoir détecté l'activité d'un utilisateur qui n'avait pas été vu auparavant, le système récupère les informations le concernant auprès du serveur. Tant que le système n'a pas réussi à récupérer ces informations, l'activité vue par cet utilisateur n'est *pas* gérée par les règles de correspondance. Au lieu de cela, la session utilisateur est gérée par la prochaine règle à laquelle elle correspond (ou l'action par défaut de la politique, le cas échéant).

Par exemple, cela pourrait expliquer quand :

- Les utilisateurs qui sont membres de groupes d'utilisateurs ne font pas correspondre les règles avec les conditions du groupe d'utilisateurs.
- Les utilisateurs qui ont été signalés par un agent TS ou un périphérique ISEou ISE-PIC ne correspondent pas aux règles lorsque le serveur utilisé pour la récupération des données d'utilisateur est un serveur Active Directory.

Notez que le système pourrait également retarder l'affichage des données utilisateur dans les vues des événements et les outils d'analyse.

Les règles ne correspondent pas à tous les utilisateurs ISE

Il s'agit du comportement attendu. Vous pouvez effectuer le contrôle utilisateur sur les utilisateurs ISE qui ont été authentifiés par un contrôleur de domaine Active Directory. Vous ne pouvez pas effectuer le contrôle utilisateur sur les utilisateurs ISE qui ont été authentifiés par un contrôleur de domaine LDAP, RADIUS ou RSA.

Les règles ne correspondent pas à tous les utilisateurs ISE/ISE-PIC

Il s'agit du comportement attendu. Vous pouvez effectuer le contrôle utilisateur sur les utilisateurs ISE/ISE-PIC qui ont été authentifiés par un contrôleur de domaine Active Directory. Vous ne pouvez pas effectuer le contrôle utilisateur sur les utilisateurs ISE/ISE-PIC qui ont été authentifiés par un contrôleur de domaine LDAP, RADIUS ou RSA.

Utilisateurs et groupes utilisant trop de mémoire

Si le traitement des utilisateurs et des groupes utilise trop de mémoire, des alertes d'intégrité s'affichent. N'oubliez pas que toutes les sessions utilisateur sont transmises à tous les périphériques gérés par centre de

gestion. Si votre centre de gestion gère des périphériques avec différentes quantités de mémoire, le périphérique avec la mémoire la plus basse déterminera le nombre de sessions d'utilisateur que le système peut gérer sans erreur.

Si ces problèmes persistent, vous avez les possibilités suivantes :

- Séparer les périphériques gérés de capacité inférieure sur les sous-réseaux et configurer ISE/ISE-PIC pour ne pas signaler les données d'authentification passive à ces sous-réseaux.

  Consultez le chapitre sur la gestion des périphériques réseau dans le *Guide de l'administrateur de Cisco Identity Services Engine*.

- Se désinscrire des balises de groupes de sécurité (SGT).

  Pour en savoir plus, consultez Configurer ISE/ISE-PIC pour le contrôle utilisateur.

- Mettre à niveau votre périphérique géré vers un modèle comportant plus de mémoire.

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.