CSM 3.x : Configurer les autorisations et rôles utilisateur

Contenu

Introduction

Ce document décrit comment configurer les autorisations et les rôles pour les utilisateurs dans Cisco Security Manager (CSM).

Conditions préalables

Conditions requises

Ce document suppose que le CSM est installé et fonctionne correctement.

Components Used

Les informations de ce document sont basées sur CSM 3.1.

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurer les autorisations utilisateur

Cisco Security Manager authentifie votre nom d'utilisateur et votre mot de passe avant de vous connecter. Une fois qu'ils ont été authentifiés, Security Manager établit votre rôle au sein de l'application. Ce rôle définit vos autorisations (également appelées privilèges), qui sont l'ensemble des tâches ou opérations que vous êtes autorisé à effectuer. Si vous n'êtes pas autorisé pour certaines tâches ou certains périphériques, les éléments de menu, les éléments de table des matières et les boutons associés sont masqués ou désactivés. En outre, un message vous indique que vous n'êtes pas autorisé à afficher les informations sélectionnées ou à effectuer l'opération sélectionnée.

L'authentification et l'autorisation de Security Manager sont gérées soit par le serveur CiscoWorks, soit par le serveur Cisco Secure Access Control Server (ACS). Par défaut, CiscoWorks gère l'authentification et l'autorisation, mais vous pouvez passer à Cisco Secure ACS à l'aide de la page Configuration du mode AAA dans CiscoWorks Common Services.

Les principaux avantages de l'utilisation de Cisco Secure ACS sont la possibilité de créer des rôles d'utilisateurs hautement granulaires avec des jeux d'autorisations spécialisés (par exemple, permettre à l'utilisateur de configurer certains types de politiques mais pas d'autres) et la possibilité de restreindre les utilisateurs à certains périphériques en configurant des groupes de périphériques réseau (NDG).

Les rubriques suivantes décrivent les autorisations utilisateur :

- Autorisations Security Manager
- Présentation des rôles CiscoWorks
- Comprendre les rôles Cisco Secure ACS
- Associations par défaut entre les autorisations et les rôles dans Security Manager

Autorisations Security Manager

Security Manager classe les autorisations dans les catégories suivantes :

1. **View** : permet d'afficher les paramètres actuels. Pour plus d'informations, consultez Autorisations d'affichage.
2. **Modify** : permet de modifier les paramètres actuels. Pour plus d'informations, consultez Modifier les autorisations.
3. **Affecter** : permet d'affecter des stratégies aux périphériques et aux topologies VPN. Pour plus d'informations, consultez Affecter des autorisations
4. **Approuver** - Permet d'approuver les modifications de stratégie et les tâches de déploiement. Pour plus d'informations, consultez Approuver les autorisations.

5. **Import** : permet d'importer les configurations déjà déployées sur des périphériques dans Security Manager.
6. **Deploy** - Permet de déployer des modifications de configuration sur les périphériques de votre réseau et d'effectuer une restauration pour revenir à une configuration précédemment déployée.
7. **Control** : vous permet d'émettre des commandes aux périphériques, telles que ping.
8. **Submit** : vous permet d'envoyer vos modifications de configuration pour approbation.

- Lorsque vous sélectionnez les autorisations de modification, d'affectation, d'approbation, d'importation, de contrôle ou de déploiement, vous devez également sélectionner les autorisations d'affichage correspondantes ; sinon, Security Manager ne fonctionnera pas correctement.
- Lorsque vous sélectionnez Modifier les autorisations de stratégie, vous devez également sélectionner les autorisations d'affectation et d'affichage de stratégie correspondantes.
- Lorsque vous autorisez une stratégie qui utilise des objets de stratégie dans sa définition, vous devez également accorder des autorisations d'affichage à ces types d'objets. Par exemple, si vous sélectionnez l'autorisation de modification des stratégies de routage, vous devez également sélectionner les autorisations d'affichage des objets réseau et des rôles d'interface, qui sont les types d'objets requis par les stratégies de routage.
- Il en va de même lorsque vous autorisez un objet qui utilise d'autres objets dans sa définition. Par exemple, si vous sélectionnez l'autorisation de modifier des groupes d'utilisateurs, vous devez également sélectionner les autorisations d'affichage des objets réseau, des objets ACL et des groupes de serveurs AAA.

Afficher les autorisations

Les autorisations d'affichage (lecture seule) dans Security Manager sont divisées en catégories, comme illustré :

- Afficher les autorisations des stratégies
- Afficher les autorisations d'objets
- Autorisations d'affichage supplémentaires

Afficher les autorisations des stratégies

Security Manager inclut les autorisations d'affichage suivantes pour les stratégies :

1. **Affichage > Stratégies > Pare-feu.** Permet d'afficher les stratégies de service de pare-feu (situées dans le sélecteur de stratégie sous Pare-feu) sur les périphériques PIX/ASA/FWSM, les routeurs IOS et les périphériques Catalyst 6500/7600. Les règles d'accès, les règles AAA et les règles d'inspection sont des exemples de stratégies de service de pare-feu.
2. **Affichage > Politiques > Système de prévention des intrusions.** Permet d'afficher les stratégies IPS (situées dans le sélecteur de stratégies sous IPS), y compris les stratégies IPS s'exécutant sur les routeurs IOS.
3. **Affichage > Stratégies > Image.** Vous permet de sélectionner un package de mise à jour de signature dans l'Assistant Appliquer les mises à jour IPS (situé sous Outils > Appliquer la mise à jour IPS), mais ne vous permet pas d'affecter le package à des périphériques spécifiques, sauf si vous disposez également de l'autorisation Modifier > Stratégies > Image.

4. **Affichage > Stratégies > NAT**. Permet d'afficher les stratégies de traduction d'adresses réseau sur les périphériques PIX/ASA/FWSM et les routeurs IOS. Les règles statiques et les règles dynamiques sont des exemples de politiques NAT.
5. **View > Policies > Site-to-Site VPN**. Permet d'afficher les stratégies VPN de site à site sur les périphériques PIX/ASA/FWSM, les routeurs IOS et les périphériques Catalyst 6500/7600. Les propositions IKE, les propositions IPsec et les clés pré-partagées sont des exemples de politiques VPN de site à site.
6. **View > Policies > Remote Access VPN**. Permet d'afficher les stratégies VPN d'accès à distance sur les périphériques PIX/ASA/FWSM, les routeurs IOS et les périphériques Catalyst 6500/7600. Les propositions IKE, les propositions IPsec et les politiques PKI sont des exemples de politiques VPN d'accès à distance.
7. **View > Policies > SSL VPN**. Permet d'afficher les stratégies VPN SSL sur les périphériques PIX/ASA/FWSM et les routeurs IOS, comme l'assistant VPN SSL.
8. **Affichage > Stratégies > Interfaces**. Permet d'afficher les stratégies d'interface (situées dans le sélecteur de stratégies sous Interfaces) sur les périphériques PIX/ASA/FWSM, les routeurs IOS, les capteurs IPS et les périphériques Catalyst 6500/7600.Sur les périphériques PIX/ASA/FWSM, cette autorisation couvre les ports matériels et les paramètres d'interface.Sur les routeurs IOS, cette autorisation couvre les paramètres d'interface de base et avancés, ainsi que d'autres stratégies d'interface, telles que les stratégies DSL, PVC, PPP et de numérotation.Sur les capteurs IPS, cette autorisation couvre les interfaces physiques et les cartes récapitulatives.Sur les périphériques Catalyst 6500/7600, cette autorisation couvre les interfaces et les paramètres VLAN.
9. **Affichage > Stratégies > Pontage**. Permet d'afficher les stratégies de table ARP (situées dans le sélecteur de stratégies sous Plateforme > Pontage) sur les périphériques PIX/ASA/FWSM.
10. **Affichage > Stratégies > Administration des périphériques**. Permet d'afficher les stratégies d'administration des périphériques (situées dans le sélecteur de stratégies sous Platform > Device Admin) sur les périphériques PIX/ASA/FWSM, les routeurs IOS et les périphériques Catalyst 6500/7600 :Sur les périphériques PIX/ASA/FWSM, les exemples incluent les politiques d'accès aux périphériques, les politiques d'accès aux serveurs et les politiques de basculement.Sur les routeurs IOS, les exemples incluent les politiques d'accès aux périphériques (y compris l'accès aux lignes), les politiques d'accès aux serveurs, AAA et Secure Device Provisioning.Sur les capteurs IPS, cette autorisation couvre les stratégies d'accès aux périphériques et aux serveurs.Sur les périphériques Catalyst 6500/7600, cette autorisation couvre les paramètres IDSM et les listes d'accès VLAN.
11. **Affichage > Stratégies > Identité**. Permet d'afficher les stratégies d'identité (situées dans le sélecteur de stratégies sous Plateforme > Identité) sur les routeurs Cisco IOS, y compris les stratégies 802.1x et NAC (Network Admission Control).
12. **Affichage > Stratégies > Journalisation**. Permet d'afficher les stratégies de journalisation (situées dans le sélecteur de stratégies sous Plateforme > Journalisation) sur les périphériques PIX/ASA/FWSM, les routeurs IOS et les capteurs IPS. Les stratégies de journalisation incluent la configuration de la journalisation, la configuration du serveur et les stratégies de serveur syslog.
13. **Affichage > Stratégies > Multidiffusion**. Permet d'afficher les stratégies de multidiffusion (situées dans le sélecteur de stratégies sous Plateforme > Multidiffusion) sur les périphériques PIX/ASA/FWSM. Parmi les exemples de politiques de multidiffusion figurent le routage de multidiffusion et les politiques IGMP.
14. **Affichage > Stratégies > QoS**. Permet d'afficher les stratégies QoS (situées dans le

sélecteur de stratégies sous Plateforme > Qualité de service) sur les routeurs Cisco IOS.
15. **Affichage > Stratégies > Routage**. Permet d'afficher les stratégies de routage (situées dans le sélecteur de stratégies sous Plateforme > Routage) sur les périphériques PIX/ASA/FWSM et les routeurs IOS. Les politiques de routage OSPF, RIP et statique sont des exemples de politiques de routage.
16. **Affichage > Stratégies > Sécurité**. Permet d'afficher les stratégies de sécurité (situées dans le sélecteur de stratégies sous Plateforme > Sécurité) sur les périphériques PIX/ASA/FWSM et les capteurs IPS :Sur les périphériques PIX/ASA/FWSM, les stratégies de sécurité incluent des paramètres d'anti-spoofing, de fragment et de délai d'attente.Sur les capteurs IPS, les stratégies de sécurité incluent les paramètres de blocage.
17. **Affichage > Stratégies > Règles de stratégie de service**. Permet d'afficher les stratégies de règles de stratégie de service (situées dans le sélecteur de stratégies sous Plateforme > Règles de stratégie de service) sur les périphériques PIX 7.x/ASA. Exemples : files d'attente prioritaires et règles IPS, QoS et de connexion.
18. **Affichage > Stratégies > Préférences utilisateur**. Permet d'afficher la stratégie de déploiement (située dans le sélecteur de stratégie sous Plateforme > Préférences utilisateur) sur les périphériques PIX/ASA/FWSM. Cette stratégie contient une option permettant de supprimer toutes les traductions NAT lors du déploiement.
19. **Affichage > Stratégies > Périphérique virtuel**. Permet d'afficher les stratégies de capteur virtuel sur les périphériques IPS. Cette stratégie est utilisée pour créer des capteurs virtuels.
20. **Affichage > Stratégies > FlexConfig**. Permet d'afficher les configurations FlexConfigs, qui sont des commandes et des instructions CLI supplémentaires pouvant être déployées sur des périphériques PIX/ASA/FWSM, des routeurs IOS et des périphériques Catalyst 6500/7600.

Afficher les autorisations d'objets

Security Manager inclut les autorisations d'affichage suivantes pour les objets :

1. **Affichage > Objets > Groupes de serveurs AAA**. Permet d'afficher les objets de groupe de serveurs AAA. Ces objets sont utilisés dans les stratégies qui nécessitent des services AAA (authentification, autorisation et comptabilité).
2. **Affichage > Objets > Serveurs AAA**. Permet d'afficher les objets serveur AAA. Ces objets représentent des serveurs AAA individuels qui sont définis comme faisant partie d'un groupe de serveurs AAA.
3. **Affichage > Objets > Listes de contrôle d'accès - Standard/Étendu**. Permet d'afficher les objets de liste de contrôle d'accès standard et étendue. Les objets ACL étendus sont utilisés pour diverses politiques, telles que NAT et NAC, et pour établir l'accès VPN. Les objets ACL standard sont utilisés pour des politiques telles que OSPF et SNMP, ainsi que pour établir un accès VPN.
4. **Affichage > Objets > Listes de contrôle d'accès** - Web. Permet d'afficher les objets de liste de contrôle d'accès Web. Les objets ACL Web sont utilisés pour effectuer le filtrage de contenu dans les stratégies VPN SSL.
5. **Affichage > Objets > Groupes d'utilisateurs ASA**. Permet d'afficher les objets de groupe d'utilisateurs ASA. Ces objets sont configurés sur des appliances de sécurité ASA dans des configurations Easy VPN, VPN d'accès à distance et VPN SSL.
6. **Affichage > Objets > Catégories**. Permet d'afficher des objets de catégorie. Ces objets vous

aident à identifier facilement les règles et les objets dans les tables de règles à l'aide de couleurs.

7. **Affichage > Objets > Informations d'identification**. Permet d'afficher les objets d'informations d'identification. Ces objets sont utilisés dans la configuration Easy VPN lors de l'authentification étendue IKE (Xauth).
8. **Affichage > Objets > Configurations flexibles**. Permet d'afficher les objets FlexConfig. Ces objets, qui contiennent des commandes de configuration avec des instructions de langage de script supplémentaires, peuvent être utilisés pour configurer des commandes qui ne sont pas prises en charge par l'interface utilisateur de Security Manager.
9. **Voir > Objets > Propositions IKE**. Permet d'afficher les objets de proposition IKE. Ces objets contiennent les paramètres requis pour les propositions IKE dans les stratégies VPN d'accès à distance.
10. **View > Objects > Inspect - Class Maps** - DNS. Permet d'afficher les objets de mappage de classe DNS. Ces objets correspondent au trafic DNS avec des critères spécifiques afin que des actions puissent être effectuées sur ce trafic.
11. **View > Objects > Inspect - Class Maps - FTP**. Permet d'afficher les objets de mappage de classe FTP. Ces objets correspondent au trafic FTP avec des critères spécifiques afin que des actions puissent être effectuées sur ce trafic.
12. **View > Objects > Inspect - Class Maps - HTTP**. Permet d'afficher les objets de mappage de classe HTTP. Ces objets correspondent au trafic HTTP avec des critères spécifiques afin que des actions puissent être effectuées sur ce trafic.
13. **Affichage > Objets > Inspect - Class Maps - IM**. Permet d'afficher les objets de mappage de classe de messagerie instantanée. Ces objets correspondent au trafic de messagerie instantanée avec des critères spécifiques afin que des actions puissent être effectuées sur ce trafic.
14. **View > Objects > Inspect - Class Maps - SIP**. Permet d'afficher les objets de mappage de classe SIP. Ces objets correspondent au trafic SIP avec des critères spécifiques afin que des actions puissent être effectuées sur ce trafic.
15. **Affichage > Objets > Inspecter - Cartes de stratégie - DNS.** Permet d'afficher les objets de mappage de stratégie DNS. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic DNS.
16. **Affichage > Objets > Inspecter - Cartes de stratégie - FTP.** Permet d'afficher les objets de mappage de stratégie FTP. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic FTP.
17. **Affichage > Objets > Inspect - Policy Maps - GTP**. Permet d'afficher les objets de mappage de stratégie GTP. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic GTP.
18. **View > Objects > Inspect - Policy Maps - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Permet d'afficher les objets de mappage de stratégie HTTP créés pour les périphériques ASA/PIX 7.1.x et les routeurs IOS. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic HTTP.
19. **View > Objects > Inspect - Policy Maps - HTTP (ASA7.2/PIX7.2)**. Permet d'afficher les objets de mappage de stratégie HTTP créés pour les périphériques ASA 7.2/PIX 7.2. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic HTTP.
20. **View > Objects > Inspect - Policy Maps - IM (ASA7.2/PIX7.2)**. Permet d'afficher les objets de mappage de stratégie de messagerie instantanée créés pour les périphériques ASA 7.2/PIX 7.2. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic de messagerie instantanée.
21. **Affichage > Objets > Inspect - Policy Maps - IM (IOS)**. Permet d'afficher les objets de

mappage de stratégie de messagerie instantanée créés pour les périphériques IOS. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic de messagerie instantanée.

22. **View > Objects > Inspect - Policy Maps - SIP**. Permet d'afficher les objets de mappage de stratégie SIP. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic SIP.
23. **Affichage > Objets > Inspecter - Expressions régulières**. Permet d'afficher des objets d'expression régulière. Ces objets représentent des expressions régulières individuelles définies comme faisant partie d'un groupe d'expressions régulières.
24. **Affichage > Objets > Inspecter - Groupes d'expressions régulières**. Permet d'afficher les objets de groupe d'expressions régulières. Ces objets sont utilisés par certaines cartes de classe et inspectent les cartes pour faire correspondre du texte à l'intérieur d'un paquet.
25. **View > Objects > Inspect - TCP Maps**. Permet d'afficher des objets de mappage TCP. Ces objets personnalisent l'inspection sur le flux TCP dans les deux directions.
26. **Affichage > Objets > Rôles d'interface**. Permet d'afficher les objets de rôle d'interface. Ces objets définissent des modèles de noms qui peuvent représenter plusieurs interfaces sur différents types de périphériques. Les rôles d'interface vous permettent d'appliquer des stratégies à des interfaces spécifiques sur plusieurs périphériques sans avoir à définir manuellement le nom de chaque interface.
27. **Affichage > Objets > Jeux de transformations IPsec**. Permet d'afficher les objets de jeu de transformation IPsec. Ces objets comprennent une combinaison de protocoles de sécurité, d'algorithmes et d'autres paramètres qui spécifient exactement comment les données du tunnel IPsec seront cryptées et authentifiées.
28. **Affichage > Objets > Cartes d'attributs LDAP**. Permet d'afficher les objets de mappage d'attribut LDAP. Ces objets sont utilisés pour mapper des noms d'attribut personnalisés (définis par l'utilisateur) à des noms d'attribut LDAP Cisco.
29. **Affichage > Objets > Réseaux/Hôtes**. Permet d'afficher les objets réseau/hôte. Ces objets sont des ensembles logiques d’adresses IP qui représentent des réseaux, des hôtes ou les deux. Les objets réseau/hôte vous permettent de définir des stratégies sans spécifier chaque réseau ou hôte individuellement.
30. **Affichage > Objets > Inscriptions PKI**. Permet d'afficher les objets d'inscription PKI. Ces objets définissent les serveurs de l'autorité de certification qui fonctionnent au sein d'une infrastructure à clé publique.
31. **Affichage > Objets > Listes de transfert de port**. Permet d'afficher les objets de liste de transfert de port. Ces objets définissent les mappages de numéros de port sur un client distant à l'adresse IP de l'application et au port derrière une passerelle VPN SSL.
32. **Affichage > Objets > Configurations sécurisées des postes de travail**. Permet d'afficher des objets de configuration de bureau sécurisés. Ces objets sont des composants nommés réutilisables qui peuvent être référencés par des stratégies VPN SSL pour fournir un moyen fiable d'éliminer toutes les traces de données sensibles partagées pendant la durée d'une session VPN SSL.
33. **Affichage > Objets > Services - Listes de ports**. Permet d'afficher des objets de liste de ports. Ces objets, qui contiennent une ou plusieurs plages de numéros de port, sont utilisés pour rationaliser le processus de création d'objets de service.
34. **Affichage > Objets > Services/Groupes de services** Permet d'afficher les objets de service et de groupe de services. Ces objets sont des mappages définis de définitions de protocole et de port qui décrivent les services réseau utilisés par les politiques, telles que Kerberos, SSH et POP3.
35. **Affichage > Objets > Serveurs à connexion unique**. Permet d'afficher une seule signature

sur les objets serveur. L'authentification unique (SSO) permet aux utilisateurs VPN SSL de saisir un nom d'utilisateur et un mot de passe une fois et d'accéder à plusieurs services protégés et serveurs Web.

36. **Affichage > Objets > Moniteurs SLA**. Permet d'afficher les objets de surveillance SLA. Ces objets sont utilisés par les appliances de sécurité PIX/ASA exécutant la version 7.2 ou ultérieure pour effectuer le suivi de route. Cette fonctionnalité fournit une méthode pour suivre la disponibilité d'une route principale et installer une route de secours en cas d'échec de la route principale.
37. **Affichage > Objets > Personnalisations VPN SSL**. Permet d'afficher les objets de personnalisation VPN SSL. Ces objets définissent comment modifier l'apparence des pages VPN SSL affichées aux utilisateurs, telles que les pages de connexion/déconnexion et d'accueil.
38. **Affichage > Objets > Passerelles VPN SSL**. Permet d'afficher les objets de passerelle VPN SSL. Ces objets définissent des paramètres qui permettent à la passerelle d'être utilisée comme proxy pour les connexions aux ressources protégées de votre VPN SSL.
39. **Affichage > Objets > Objets de style**. Permet d'afficher des objets de style. Ces objets vous permettent de configurer des éléments de style, tels que les caractéristiques et les couleurs des polices, pour personnaliser l'apparence de la page VPN SSL qui apparaît aux utilisateurs VPN SSL lorsqu'ils se connectent à l'appliance de sécurité.
40. **Affichage > Objets > Objets texte**. Permet d'afficher des objets texte de forme libre. Ces objets comprennent une paire nom/valeur, où la valeur peut être une chaîne unique, une liste de chaînes ou une table de chaînes.
41. **Affichage > Objets > Plages de temps.** Permet d'afficher des objets de plage de temps. Ces objets sont utilisés lors de la création de listes de contrôle d'accès basées sur le temps et de règles d'inspection. Ils sont également utilisés lors de la définition de groupes d'utilisateurs ASA pour restreindre l'accès VPN à des heures spécifiques de la semaine.
42. **Affichage > Objets > Flux de trafic**. Permet d'afficher les objets de flux de trafic. Ces objets définissent des flux de trafic spécifiques à utiliser par les périphériques PIX 7.x/ASA 7.x.
43. **Affichage > Objets > Listes d'URL**. Permet d'afficher les objets de liste d'URL. Ces objets définissent les URL affichées sur la page du portail après une connexion réussie. Cela permet aux utilisateurs d'accéder aux ressources disponibles sur les sites Web VPN SSL lorsqu'ils fonctionnent en mode d'accès sans client.
44. **Affichage > Objets > Groupes d'utilisateurs**. Permet d'afficher les objets de groupe d'utilisateurs. Ces objets définissent des groupes de clients distants qui sont utilisés dans les topologies Easy VPN, les VPN d'accès distant et les VPN SSL.
45. **Affichage > Objets > Listes de serveurs WINS**. Permet d'afficher les objets de liste de serveurs WINS. Ces objets représentent des serveurs WINS, qui sont utilisés par le VPN SSL pour accéder aux fichiers ou les partager sur des systèmes distants.
46. **Affichage > Objets > Interne - Règles DN**. Permet d'afficher les règles DN utilisées par les stratégies DN. Il s'agit d'un objet interne utilisé par Security Manager qui n'apparaît pas dans Policy Object Manager.
47. **Affichage > Objets > Interne - Mises à jour du client**. Il s'agit d'un objet interne requis par les objets de groupe d'utilisateurs qui n'apparaît pas dans le Gestionnaire d'objets de stratégie.
48. **Affichage > Objets > Interne - ACE standard**. Il s'agit d'un objet interne pour les entrées de contrôle d'accès standard, qui sont utilisées par les objets ACL.
49. **Affichage > Objets > Interne - ACE étendues.** Il s'agit d'un objet interne pour les entrées de contrôle d'accès étendu, qui sont utilisées par les objets ACL.

Autorisations d'affichage supplémentaires

Security Manager inclut les autorisations d'affichage supplémentaires suivantes :

1. **Affichage > Admin**. Permet d'afficher les paramètres d'administration de Security Manager.
2. **Affichage > CLI**. Permet d'afficher les commandes CLI configurées sur un périphérique et d'afficher un aperçu des commandes qui sont sur le point d'être déployées.
3. **Affichage > Archivage de configuration**. Permet d'afficher la liste des configurations contenues dans l'archive de configuration. Vous ne pouvez pas afficher la configuration du périphérique ou les commandes CLI.
4. **Affichage > Périphériques**. Permet d'afficher les périphériques en mode Périphérique et toutes les informations associées, notamment leurs paramètres, propriétés, affectations, etc.
5. **Affichage > Gestionnaires de périphériques**. Permet de lancer des versions en lecture seule des gestionnaires de périphériques pour des périphériques individuels, tels que le gestionnaire de routeur et de périphérique de sécurité (SDM) Cisco pour les routeurs Cisco IOS.
6. **Affichage > Topologie**. Permet d'afficher les cartes configurées en mode Plan.

Modifier les autorisations

Les autorisations de modification (lecture-écriture) dans Security Manager sont divisées en catégories, comme illustré :

- Modifier les autorisations de stratégies
- Modifier les autorisations d'objets
- Autorisations de modification supplémentaires

Modifier les autorisations de stratégies

Remarque : lorsque vous spécifiez les autorisations de modification de stratégie, assurez-vous que vous avez sélectionné les autorisations d'affectation et d'affichage de stratégie correspondantes.

Security Manager inclut les autorisations de modification suivantes pour les stratégies :

1. **Modifier > Stratégies > Pare-feu**. Permet de modifier les stratégies de service de pare-feu (situées dans le sélecteur de stratégie sous Pare-feu) sur les périphériques PIX/ASA/FWSM, les routeurs IOS et les périphériques Catalyst 6500/7600. Les règles d'accès, les règles AAA et les règles d'inspection sont des exemples de stratégies de service de pare-feu.
2. **Modifier > Politiques > Système de prévention des intrusions**. Permet de modifier les stratégies IPS (situées dans le sélecteur de stratégies sous IPS), y compris les stratégies IPS s'exécutant sur les routeurs IOS. Cette autorisation vous permet également de régler les signatures dans l'Assistant Mise à jour des signatures (situé sous Outils > Appliquer la mise à jour IPS).
3. **Modifier > Stratégies > Image**. Vous permet d'affecter un package de mise à jour de signature aux périphériques dans l'Assistant Appliquer les mises à jour IPS (situé sous Outils > Appliquer la mise à jour IPS). Cette autorisation vous permet également d'affecter des paramètres de mise à jour automatique à des périphériques spécifiques (situés sous Outils >

Administration de Security Manager > Mises à jour IPS).

4. **Modifier > Stratégies > NAT**. Permet de modifier les stratégies de traduction d'adresses réseau sur les périphériques PIX/ASA/FWSM et les routeurs IOS. Les règles statiques et les règles dynamiques sont des exemples de politiques NAT.
5. **Modifier > Stratégies > VPN site à site**. Permet de modifier les stratégies VPN de site à site sur les périphériques PIX/ASA/FWSM, les routeurs IOS et les périphériques Catalyst 6500/7600. Les propositions IKE, les propositions IPsec et les clés pré-partagées sont des exemples de politiques VPN de site à site.
6. **Modifier > Stratégies > VPN d'accès à distance**. Permet de modifier les stratégies VPN d'accès à distance sur les périphériques PIX/ASA/FWSM, les routeurs IOS et les périphériques Catalyst 6500/7600. Les propositions IKE, les propositions IPsec et les politiques PKI sont des exemples de politiques VPN d'accès à distance.
7. **Modifier > Stratégies > VPN SSL**. Permet de modifier les stratégies VPN SSL sur les périphériques PIX/ASA/FWSM et les routeurs IOS, comme l'assistant VPN SSL.
8. **Modifier > Stratégies > Interfaces**. Permet de modifier les stratégies d'interface (situées dans le sélecteur de stratégies sous Interfaces) sur les périphériques PIX/ASA/FWSM, les routeurs IOS, les capteurs IPS et les périphériques Catalyst 6500/7600 :Sur les périphériques PIX/ASA/FWSM, cette autorisation couvre les ports matériels et les paramètres d'interface.Sur les routeurs IOS, cette autorisation couvre les paramètres d'interface de base et avancés, ainsi que d'autres stratégies d'interface, telles que les stratégies DSL, PVC, PPP et de numérotation.Sur les capteurs IPS, cette autorisation couvre les interfaces physiques et les cartes récapitulatives.Sur les périphériques Catalyst 6500/7600, cette autorisation couvre les interfaces et les paramètres VLAN.
9. **Modifier > Stratégies > Pontage**. Permet de modifier les stratégies de table ARP (situées dans le sélecteur de stratégies sous Plateforme > Pontage) sur les périphériques PIX/ASA/FWSM.
10. **Modifier > Stratégies > Administration des périphériques**. Permet de modifier les stratégies d'administration des périphériques (situées dans le sélecteur de stratégies sous Platform > Device Admin) sur les périphériques PIX/ASA/FWSM, les routeurs IOS et les périphériques Catalyst 6500/7600 :Sur les périphériques PIX/ASA/FWSM, les exemples incluent les politiques d'accès aux périphériques, les politiques d'accès aux serveurs et les politiques de basculement.Sur les routeurs IOS, les exemples incluent les politiques d'accès aux périphériques (y compris l'accès aux lignes), les politiques d'accès aux serveurs, AAA et Secure Device Provisioning.Sur les capteurs IPS, cette autorisation couvre les stratégies d'accès aux périphériques et aux serveurs.Sur les périphériques Catalyst 6500/7600, cette autorisation couvre les paramètres IDSM et la liste d'accès VLAN.
11. **Modifier > Stratégies > Identité**. Permet de modifier les stratégies d'identité (situées dans le sélecteur de stratégies sous Plateforme > Identité) sur les routeurs Cisco IOS, y compris les stratégies 802.1x et NAC (Network Admission Control).
12. **Modifier > Stratégies > Journalisation**. Permet de modifier les stratégies de journalisation (situées dans le sélecteur de stratégies sous Plateforme > Journalisation) sur les périphériques PIX/ASA/FWSM, les routeurs IOS et les capteurs IPS. Les stratégies de journalisation incluent la configuration de la journalisation, la configuration du serveur et les stratégies de serveur syslog.
13. **Modifier > Stratégies > Multidiffusion**. Permet de modifier les stratégies de multidiffusion (situées dans le sélecteur de stratégies sous Plateforme > Multidiffusion) sur les périphériques PIX/ASA/FWSM. Parmi les exemples de politiques de multidiffusion figurent le routage de multidiffusion et les politiques IGMP.

14. **Modifier > Stratégies > QoS**. Permet de modifier les stratégies QoS (situées dans le sélecteur de stratégies sous Plateforme > Qualité de service) sur les routeurs Cisco IOS.
15. **Modifier > Stratégies > Routage**. Permet de modifier les stratégies de routage (situées dans le sélecteur de stratégies sous Plateforme > Routage) sur les périphériques PIX/ASA/FWSM et les routeurs IOS. Les politiques de routage OSPF, RIP et statique sont des exemples de politiques de routage.
16. **Modifier > Stratégies > Sécurité**. Permet de modifier les stratégies de sécurité (situées dans le sélecteur de stratégies sous Plateforme > Sécurité) sur les périphériques PIX/ASA/FWSM et les capteurs IPS :Sur les périphériques PIX/ASA/FWSM, les stratégies de sécurité incluent des paramètres d'anti-spoofing, de fragment et de délai d'attente.Sur les capteurs IPS, les stratégies de sécurité incluent les paramètres de blocage.
17. **Modifier > Stratégies > Règles de stratégie de service**. Permet de modifier les stratégies de règles de stratégie de service (situées dans le sélecteur de stratégie sous Plateforme > Règles de stratégie de service) sur les périphériques PIX 7.x/ASA. Exemples : files d'attente prioritaires et règles IPS, QoS et de connexion.
18. **Modifier > Stratégies > Préférences utilisateur**. Permet de modifier la stratégie de déploiement (située dans le sélecteur de stratégie sous Plateforme > Préférences utilisateur) sur les périphériques PIX/ASA/FWSM. Cette stratégie contient une option permettant de supprimer toutes les traductions NAT lors du déploiement.
19. **Modifier > Stratégies > Périphérique virtuel**. Permet de modifier les stratégies de capteur virtuel sur les périphériques IPS. Utilisez cette stratégie pour créer des capteurs virtuels.
20. **Modifier > Stratégies > FlexConfig**. Permet de modifier les configurations FlexConfigs, qui sont des commandes et des instructions CLI supplémentaires qui peuvent être déployées sur des périphériques PIX/ASA/FWSM, des routeurs IOS et des périphériques Catalyst 6500/7600.

Modifier les autorisations d'objets

Security Manager inclut les autorisations d'affichage suivantes pour les objets :

1. **Modifier > Objets > Groupes de serveurs AAA**. Permet d'afficher les objets de groupe de serveurs AAA. Ces objets sont utilisés dans les stratégies qui nécessitent des services AAA (authentification, autorisation et comptabilité).
2. **Modifier > Objets > Serveurs AAA**. Permet d'afficher les objets serveur AAA. Ces objets représentent des serveurs AAA individuels qui sont définis comme faisant partie d'un groupe de serveurs AAA.
3. **Modifier > Objets > Listes de contrôle d'accès - Standard/Étendu**. Permet d'afficher les objets de liste de contrôle d'accès standard et étendue. Les objets ACL étendus sont utilisés pour diverses politiques, telles que NAT et NAC, et pour établir l'accès VPN. Les objets ACL standard sont utilisés pour des politiques telles que OSPF et SNMP, ainsi que pour établir un accès VPN.
4. **Modifier > Objets > Listes de contrôle d'accès - Web**. Permet d'afficher les objets de liste de contrôle d'accès Web. Les objets ACL Web sont utilisés pour effectuer le filtrage de contenu dans les stratégies VPN SSL.
5. **Modifier > Objets >** Groupes d'utilisateurs **ASA** Permet d'afficher les objets de groupe d'utilisateurs ASA. Ces objets sont configurés sur des appliances de sécurité ASA dans des configurations Easy VPN, VPN d'accès à distance et VPN SSL.
6. **Modifier > Objets > Catégories**. Permet d'afficher des objets de catégorie. Ces objets vous

aident à identifier facilement les règles et les objets dans les tables de règles à l'aide de couleurs.

7. **Modifier > Objets > Informations d'identification**. Permet d'afficher les objets d'informations d'identification. Ces objets sont utilisés dans la configuration Easy VPN lors de l'authentification étendue IKE (Xauth).
8. **Modifier > Objets > Configurations flexibles**. Permet d'afficher les objets FlexConfig. Ces objets, qui contiennent des commandes de configuration avec des instructions de langage de script supplémentaires, peuvent être utilisés pour configurer des commandes qui ne sont pas prises en charge par l'interface utilisateur de Security Manager.
9. **Modifier > Objets > Propositions IKE**. Permet d'afficher les objets de proposition IKE. Ces objets contiennent les paramètres requis pour les propositions IKE dans les stratégies VPN d'accès à distance.
10. **Modify > Objects > Inspect - Class Maps - DNS**. Permet d'afficher les objets de mappage de classe DNS. Ces objets correspondent au trafic DNS avec des critères spécifiques afin que des actions puissent être effectuées sur ce trafic.
11. **Modify > Objects > Inspect - Class Maps - FTP**. Permet d'afficher les objets de mappage de classe FTP. Ces objets correspondent au trafic FTP avec des critères spécifiques afin que des actions puissent être effectuées sur ce trafic.
12. **Modify > Objects > Inspect - Class Maps - HTTP**. Permet d'afficher les objets de mappage de classe HTTP. Ces objets correspondent au trafic HTTP avec des critères spécifiques afin que des actions puissent être effectuées sur ce trafic.
13. **Modifier > Objets > Inspect - Class Maps - IM**. Permet d'afficher les objets de mappage de classe de messagerie instantanée. Ces objets correspondent au trafic de messagerie instantanée avec des critères spécifiques afin que des actions puissent être effectuées sur ce trafic.
14. **Modify > Objects > Inspect - Class Maps - SIP**. Permet d'afficher les objets de mappage de classe SIP. Ces objets correspondent au trafic SIP avec des critères spécifiques afin que des actions puissent être effectuées sur ce trafic.
15. **Modify > Objects > Inspect - Policy Maps - DNS**. Permet d'afficher les objets de mappage de stratégie DNS. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic DNS.
16. **Modify > Objects > Inspect - Policy Maps - FTP**. Permet d'afficher les objets de mappage de stratégie FTP. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic FTP.
17. **Modify > Objects > Inspect - Policy Maps - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Permet d'afficher les objets de mappage de stratégie HTTP créés pour les périphériques ASA/PIX 7.x et les routeurs IOS. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic HTTP.
18. **Modify > Objects > Inspect - Policy Maps - HTTP (ASA7.2/PIX7.2)**. Permet d'afficher les objets de mappage de stratégie HTTP créés pour les périphériques ASA 7.2/PIX 7.2. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic HTTP.
19. **Modify > Objects > Inspect - Policy Maps - IM (ASA7.2/PIX7.2)**. Permet d'afficher les objets de mappage de stratégie de messagerie instantanée créés pour les périphériques ASA 7.2/PIX 7.2. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic de messagerie instantanée.
20. **Modify > Objects > Inspect - Policy Maps - IM (IOS)**. Permet d'afficher les objets de mappage de stratégie de messagerie instantanée créés pour les périphériques IOS. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic de messagerie

instantanée.

21. **Modify > Objects > Inspect - Policy Maps - SIP**. Permet d'afficher les objets de mappage de stratégie SIP. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic SIP.
22. **Modifier > Objets > Inspecter - Expressions régulières**. Permet d'afficher des objets d'expression régulière. Ces objets représentent des expressions régulières individuelles définies comme faisant partie d'un groupe d'expressions régulières.
23. **Modifier > Objets > Inspecter - Groupes d'expressions régulières**. Permet d'afficher les objets de groupe d'expressions régulières. Ces objets sont utilisés par certaines cartes de classe et inspectent les cartes pour faire correspondre du texte à l'intérieur d'un paquet.
24. **Modify > Objects > Inspect - TCP Maps**. Permet d'afficher des objets de mappage TCP. Ces objets personnalisent l'inspection sur le flux TCP dans les deux directions.
25. **Modifier > Objets > Rôles d'interface**. Permet d'afficher les objets de rôle d'interface. Ces objets définissent des modèles de noms qui peuvent représenter plusieurs interfaces sur différents types de périphériques. Les rôles d'interface vous permettent d'appliquer des stratégies à des interfaces spécifiques sur plusieurs périphériques sans avoir à définir manuellement le nom de chaque interface.
26. **Modifier > Objets > Jeux de transformations IPsec**. Permet d'afficher les objets de jeu de transformation IPsec. Ces objets comprennent une combinaison de protocoles de sécurité, d'algorithmes et d'autres paramètres qui spécifient exactement comment les données du tunnel IPsec seront cryptées et authentifiées.
27. **Modifier > Objets > Cartes d'attributs LDAP**. Permet d'afficher les objets de mappage d'attribut LDAP. Ces objets sont utilisés pour mapper des noms d'attribut personnalisés (définis par l'utilisateur) à des noms d'attribut LDAP Cisco.
28. **Modifier > Objets > Réseaux/Hôtes**. Permet d'afficher les objets réseau/hôte. Ces objets sont des ensembles logiques d'adresses IP qui représentent des réseaux, des hôtes ou les deux. Les objets réseau/hôte vous permettent de définir des stratégies sans spécifier chaque réseau ou hôte individuellement.
29. **Modifier > Objets > Inscriptions PKI**. Permet d'afficher les objets d'inscription PKI. Ces objets définissent les serveurs de l'autorité de certification qui fonctionnent au sein d'une infrastructure à clé publique.
30. **Modifier > Objets > Listes de transfert de port**. Permet d'afficher les objets de liste de transfert de port. Ces objets définissent les mappages de numéros de port sur un client distant à l'adresse IP de l'application et au port derrière une passerelle VPN SSL.
31. **Modifier > Objets > Configurations sécurisées du bureau**. Permet d'afficher des objets de configuration de bureau sécurisés. Ces objets sont des composants nommés réutilisables qui peuvent être référencés par des stratégies VPN SSL pour fournir un moyen fiable d'éliminer toutes les traces de données sensibles partagées pendant la durée d'une session VPN SSL.
32. **Modifier > Objets > Services - Listes de ports**. Permet d'afficher des objets de liste de ports. Ces objets, qui contiennent une ou plusieurs plages de numéros de port, sont utilisés pour rationaliser le processus de création d'objets de service.
33. **Modifier > Objets > Services/Groupes de services.** Permet d'afficher les objets de service et de groupe de services. Ces objets sont des mappages définis de définitions de protocole et de port qui décrivent les services réseau utilisés par les politiques, telles que Kerberos, SSH et POP3.
34. **Modifier > Objets > Serveurs à connexion unique.** Permet d'afficher une seule signature sur les objets serveur. L'authentification unique (SSO) permet aux utilisateurs VPN SSL de saisir un nom d'utilisateur et un mot de passe une fois et d'accéder à plusieurs services

protégés et serveurs Web.

35. **Modifier > Objets > Moniteurs SLA**. Permet d'afficher les objets de surveillance SLA. Ces objets sont utilisés par les appliances de sécurité PIX/ASA exécutant la version 7.2 ou ultérieure pour effectuer le suivi de route. Cette fonctionnalité fournit une méthode pour suivre la disponibilité d'une route principale et installer une route de secours en cas d'échec de la route principale.
36. **Modifier > Objets > Personnalisations VPN SSL**. Permet d'afficher les objets de personnalisation VPN SSL. Ces objets définissent comment modifier l'apparence des pages VPN SSL affichées aux utilisateurs, telles que les pages de connexion/déconnexion et d'accueil.
37. **Modifier > Objets > Passerelles VPN SSL**. Permet d'afficher les objets de passerelle VPN SSL. Ces objets définissent des paramètres qui permettent à la passerelle d'être utilisée comme proxy pour les connexions aux ressources protégées de votre VPN SSL.
38. **Modifier > Objets > Objets de style**. Permet d'afficher des objets de style. Ces objets vous permettent de configurer des éléments de style, tels que les caractéristiques et les couleurs des polices, pour personnaliser l'apparence de la page VPN SSL qui apparaît aux utilisateurs VPN SSL lorsqu'ils se connectent à l'appliance de sécurité.
39. **Modifier > Objets > Objets texte**. Permet d'afficher des objets texte de forme libre. Ces objets comprennent une paire nom/valeur, où la valeur peut être une chaîne unique, une liste de chaînes ou une table de chaînes.
40. **Modifier > Objets > Plages de temps.** Permet d'afficher des objets de plage de temps. Ces objets sont utilisés lors de la création de listes de contrôle d'accès basées sur le temps et de règles d'inspection. Ils sont également utilisés lors de la définition de groupes d'utilisateurs ASA pour restreindre l'accès VPN à des heures spécifiques de la semaine.
41. **Modifier > Objets > Flux de trafic**. Permet d'afficher les objets de flux de trafic. Ces objets définissent des flux de trafic spécifiques à utiliser par les périphériques PIX 7.x/ASA 7.x.
42. **Modifier > Objets > Listes d'URL**. Permet d'afficher les objets de liste d'URL. Ces objets définissent les URL affichées sur la page du portail après une connexion réussie. Cela permet aux utilisateurs d'accéder aux ressources disponibles sur les sites Web VPN SSL lorsqu'ils fonctionnent en mode d'accès sans client.
43. **Modifier > Objets > Groupes d'utilisateurs**. Permet d'afficher les objets de groupe d'utilisateurs. Ces objets définissent des groupes de clients distants qui sont utilisés dans les topologies Easy VPN, les VPN d'accès distant et les VPN SSL
44. **Modifier > Objets > Listes de serveurs WINS**. Permet d'afficher les objets de liste de serveurs WINS. Ces objets représentent des serveurs WINS, qui sont utilisés par le VPN SSL pour accéder aux fichiers ou les partager sur des systèmes distants.
45. **Modifier > Objets > Interne - Règles DN.** Permet d'afficher les règles DN utilisées par les stratégies DN. Il s'agit d'un objet interne utilisé par Security Manager qui n'apparaît pas dans Policy Object Manager.
46. **Modifier > Objets > Interne - Mises à jour du client**. Il s'agit d'un objet interne requis par les objets de groupe d'utilisateurs qui n'apparaît pas dans le Gestionnaire d'objets de stratégie.
47. **Modifier > Objets > Interne - ACE standard**. Il s'agit d'un objet interne pour les entrées de contrôle d'accès standard, qui sont utilisées par les objets ACL.
48. **Modifier > Objets > Interne - ACE étendue**. Il s'agit d'un objet interne pour les entrées de contrôle d'accès étendu, qui sont utilisées par les objets ACL.

Autorisations de modification supplémentaires

Security Manager inclut les autorisations de modification supplémentaires comme indiqué :

1. **Modifier > Admin**. Permet de modifier les paramètres d'administration de Security Manager.
2. **Modifier > Archivage de configuration**. Permet de modifier la configuration du périphérique dans l'archive de configuration. En outre, il vous permet d'ajouter des configurations à l'archive et de personnaliser l'outil d'archivage de la configuration.
3. **Modifier > Périphériques**. Permet d'ajouter et de supprimer des périphériques, ainsi que de modifier les propriétés et les attributs des périphériques. Pour découvrir les stratégies sur le périphérique ajouté, vous devez également activer l'autorisation d'importation. En outre, si vous activez l'autorisation Modifier > Périphériques, assurez-vous que vous activez également l'autorisation Affecter > Stratégies > Interfaces.
4. **Modifier > Hiérarchie**. Permet de modifier les groupes de périphériques.
5. **Modifier > Topologie**. Permet de modifier les cartes en mode Plan.

Affecter des autorisations

Security Manager inclut les autorisations d'affectation de stratégie comme indiqué :

1. **Affecter > Stratégies > Pare-feu**. Permet d'affecter des stratégies de service de pare-feu (situées dans le sélecteur de stratégie sous Pare-feu) aux périphériques PIX/ASA/FWSM, aux routeurs IOS et aux périphériques Catalyst 6500/7600. Les règles d'accès, les règles AAA et les règles d'inspection sont des exemples de stratégies de service de pare-feu.
2. **Affecter > Stratégies > Système de prévention des intrusions**. Vous permet d'affecter des stratégies IPS (situées dans le sélecteur de stratégies sous IPS), y compris des stratégies IPS s'exécutant sur des routeurs IOS.
3. **Affecter > Stratégies > Image**. Cette autorisation n'est actuellement pas utilisée par le Gestionnaire de sécurité.
4. **Affecter > Stratégies > NAT**. Permet d'attribuer des stratégies de traduction d'adresses réseau aux périphériques PIX/ASA/FWSM et aux routeurs IOS. Les règles statiques et les règles dynamiques sont des exemples de politiques NAT.
5. **Affecter > Stratégies > VPN site à site**. Permet d'affecter des stratégies VPN de site à site aux périphériques PIX/ASA/FWSM, aux routeurs IOS et aux périphériques Catalyst 6500/7600. Les propositions IKE, les propositions IPsec et les clés pré-partagées sont des exemples de politiques VPN de site à site.
6. **Affecter > Stratégies > VPN d'accès à distance**. Permet d'attribuer des stratégies VPN d'accès à distance aux périphériques PIX/ASA/FWSM, aux routeurs IOS et aux périphériques Catalyst 6500/7600. Les propositions IKE, les propositions IPsec et les politiques PKI sont des exemples de politiques VPN d'accès à distance.
7. **Affecter > Stratégies > VPN SSL**. Vous permet d'attribuer des stratégies VPN SSL aux périphériques PIX/ASA/FWSM et aux routeurs IOS, tels que l'assistant VPN SSL.
8. **Affecter > Stratégies > Interfaces**. Permet d'affecter des stratégies d'interface (situées dans le sélecteur de stratégies sous Interfaces) aux périphériques PIX/ASA/FWSM, aux routeurs IOS et aux périphériques Catalyst 6500/7600 :Sur les périphériques PIX/ASA/FWSM, cette autorisation couvre les ports matériels et les paramètres d'interface.Sur les routeurs IOS, cette autorisation couvre les paramètres d'interface de base et avancés, ainsi que d'autres stratégies d'interface, telles que les stratégies DSL, PVC, PPP et de numérotation.Sur les périphériques Catalyst 6500/7600, cette autorisation couvre les interfaces et les paramètres VLAN.

9. **Affecter > Stratégies > Pontage**. Permet d'affecter des stratégies de table ARP (situées dans le sélecteur de stratégies sous Plateforme > Pontage) aux périphériques PIX/ASA/FWSM.
10. **Affecter > Stratégies > Administration des périphériques**. Permet d'affecter des stratégies d'administration de périphériques (situées dans le sélecteur de stratégies sous Platform > Device Admin) aux périphériques PIX/ASA/FWSM, aux routeurs IOS et aux périphériques Catalyst 6500/7600 :Sur les périphériques PIX/ASA/FWSM, les exemples incluent les politiques d'accès aux périphériques, les politiques d'accès aux serveurs et les politiques de basculement.Sur les routeurs IOS, les exemples incluent les politiques d'accès aux périphériques (y compris l'accès aux lignes), les politiques d'accès aux serveurs, AAA et Secure Device Provisioning.Sur les capteurs IPS, cette autorisation couvre les stratégies d'accès aux périphériques et aux serveurs.Sur les périphériques Catalyst 6500/7600, cette autorisation couvre les paramètres IDSM et les listes d'accès VLAN.
11. **Affecter > Stratégies > Identité**. Permet d'affecter des stratégies d'identité (situées dans le sélecteur de stratégies sous Plateforme > Identité) aux routeurs Cisco IOS, y compris les stratégies 802.1x et NAC (Network Admission Control).
12. **Affecter > Stratégies > Journalisation**. Permet d'affecter des stratégies de journalisation (situées dans le sélecteur de stratégies sous Plateforme > Journalisation) aux périphériques PIX/ASA/FWSM et aux routeurs IOS. Les stratégies de journalisation incluent la configuration de la journalisation, la configuration du serveur et les stratégies de serveur syslog.
13. **Affecter > Stratégies > Multidiffusion**. Permet d'affecter des stratégies de multidiffusion (situées dans le sélecteur de stratégies sous Plateforme > Multidiffusion) aux périphériques PIX/ASA/FWSM. Parmi les exemples de politiques de multidiffusion figurent le routage de multidiffusion et les politiques IGMP.
14. **Affecter > Stratégies > QoS**. Permet d'affecter des stratégies QoS (situées dans le sélecteur de stratégies sous Plateforme > Qualité de service) aux routeurs Cisco IOS.
15. **Affecter > Stratégies > Routage**. Permet d'affecter des stratégies de routage (situées dans le sélecteur de stratégies sous Plateforme > Routage) aux périphériques PIX/ASA/FWSM et aux routeurs IOS. Les politiques de routage OSPF, RIP et statique sont des exemples de politiques de routage.
16. **Affecter > Stratégies > Sécurité**. Permet d'affecter des stratégies de sécurité (situées dans le sélecteur de stratégies sous Plateforme > Sécurité) aux périphériques PIX/ASA/FWSM. Les stratégies de sécurité incluent les paramètres d'anti-usurpation, de fragment et de délai d'attente.
17. **Affecter > Stratégies > Règles de stratégie de service**. Permet d'affecter des stratégies de règles de stratégie de service (situées dans le sélecteur de stratégies sous Plateforme > Règles de stratégie de service) aux périphériques PIX 7.x/ASA. Exemples : files d'attente prioritaires et règles IPS, QoS et de connexion.
18. **Affecter > Stratégies > Préférences utilisateur**. Permet d'affecter la stratégie de déploiement (située dans le sélecteur de stratégie sous Plateforme > Préférences utilisateur) aux périphériques PIX/ASA/FWSM. Cette stratégie contient une option permettant de supprimer toutes les traductions NAT lors du déploiement.
19. **Affecter > Stratégies > Périphérique virtuel**. Permet d'affecter des stratégies de capteur virtuel aux périphériques IPS. Utilisez cette stratégie pour créer des capteurs virtuels.
20. **Affecter > Stratégies > FlexConfig**. Vous permet d'attribuer des configurations FlexConfigs, qui sont des commandes et des instructions CLI supplémentaires qui peuvent être déployées sur des périphériques PIX/ASA/FWSM, des routeurs IOS et des périphériques Catalyst 6500/7600.

Remarque : lorsque vous spécifiez des autorisations d'affectation, assurez-vous que vous avez également sélectionné les autorisations d'affichage correspondantes.

Approuver les autorisations

Security Manager fournit les autorisations d'approbation comme indiqué :

1. **Approuver > CLI**. Permet d'approuver les modifications de commande CLI contenues dans une tâche de déploiement.
2. **Approuver > Stratégie**. Permet d'approuver les modifications de configuration contenues dans les stratégies configurées dans une activité de workflow.

Présentation des rôles CiscoWorks

Lorsque des utilisateurs sont créés dans CiscoWorks Common Services, ils se voient attribuer un ou plusieurs rôles. Les autorisations associées à chaque rôle déterminent les opérations que chaque utilisateur est autorisé à effectuer dans Security Manager.

Les rubriques suivantes décrivent les rôles CiscoWorks :

- Rôles par défaut de CiscoWorks Common Services
- Attribution de rôles aux utilisateurs dans CiscoWorks Common Services

Rôles par défaut de CiscoWorks Common Services

CiscoWorks Common Services contient les rôles par défaut suivants :

1. **Help Desk** : les utilisateurs du centre d'assistance peuvent afficher (mais pas modifier) les périphériques, les stratégies, les objets et les cartes topologiques.
2. **Opérateur réseau** - En plus d'afficher les autorisations, les opérateurs réseau peuvent afficher les commandes CLI et les paramètres d'administration de Security Manager. Les opérateurs réseau peuvent également modifier l'archive de configuration et émettre des commandes (telles que ping) sur les périphériques.
3. **Approbateur** - Outre les autorisations d'affichage, les approbateurs peuvent approuver ou rejeter des tâches de déploiement. Ils ne peuvent pas effectuer de déploiement.
4. **Administrateur réseau** : les administrateurs réseau disposent d'autorisations complètes d'affichage et de modification, à l'exception de la modification des paramètres d'administration. Ils peuvent détecter les périphériques et les stratégies configurées sur ces périphériques, attribuer des stratégies aux périphériques et émettre des commandes aux périphériques. Les administrateurs réseau ne peuvent pas approuver les activités ou les tâches de déploiement ; cependant, ils peuvent déployer des emplois qui ont été approuvés par d'autres.
5. **Administrateur système** - Les administrateurs système ont un accès complet à toutes les autorisations du Gestionnaire de sécurité, y compris la modification, l'affectation des stratégies, l'approbation des activités et des tâches, la découverte, le déploiement et l'émission de commandes aux périphériques.

Remarque : Des rôles supplémentaires, tels que les données d'exportation, peuvent être affichés dans Common Services si des applications supplémentaires sont installées sur le serveur. Le rôle

d'exportation des données est destiné aux développeurs tiers et n'est pas utilisé par Security Manager.

Conseil : Bien que vous ne puissiez pas modifier la définition des rôles CiscoWorks, vous pouvez définir quels rôles sont attribués à chaque utilisateur. Pour plus d'informations, consultez Affectation de rôles aux utilisateurs dans CiscoWorks Common Services.

Attribution de rôles aux utilisateurs dans CiscoWorks Common Services

CiscoWorks Common Services vous permet de définir les rôles attribués à chaque utilisateur. En modifiant la définition de rôle d'un utilisateur, vous modifiez les types d'opérations que cet utilisateur est autorisé à effectuer dans Security Manager. Par exemple, si vous affectez le rôle Centre d'assistance, l'utilisateur est limité à afficher les opérations et ne peut modifier aucune donnée. Cependant, si vous attribuez le rôle Network Operator, l'utilisateur peut également modifier l'archive de configuration. Vous pouvez attribuer plusieurs rôles à chaque utilisateur.

Remarque : Vous devez redémarrer Security Manager après avoir modifié les autorisations utilisateur.

Procédure:

1. Dans Common Services, sélectionnez **Server > Security**, puis sélectionnez **Single-Server Trust Management > Local User Setup** dans la table des matières.**Conseil :** Pour accéder à la page Configuration de l'utilisateur local à partir du Gestionnaire de sécurité, sélectionnez Outils > Administration du Gestionnaire de sécurité > Sécurité du serveur, puis cliquez sur Configuration de l'utilisateur local.
2. Cochez la case en regard d'un utilisateur existant, puis cliquez sur **Modifier**.
3. Sur la page Informations sur l'utilisateur, activez les cases à cocher des rôles à attribuer à cet utilisateur.Pour plus d'informations sur chaque rôle, consultez Rôles par défaut de CiscoWorks Common Services.
4. Cliquez sur **OK** pour enregistrer vos modifications.
5. Redémarrez Security Manager.

Comprendre les rôles Cisco Secure ACS

Cisco Secure ACS offre une plus grande souplesse de gestion des autorisations Security Manager que CiscoWorks, car il prend en charge les rôles spécifiques aux applications que vous pouvez configurer. Chaque rôle est constitué d'un ensemble d'autorisations qui déterminent le niveau d'autorisation des tâches du Gestionnaire de sécurité. Dans Cisco Secure ACS, vous affectez un rôle à chaque groupe d'utilisateurs (et éventuellement à chaque utilisateur), ce qui permet à chaque utilisateur de ce groupe d'effectuer les opérations autorisées par les autorisations définies pour ce rôle.

En outre, vous pouvez attribuer ces rôles aux groupes de périphériques Cisco Secure ACS, ce qui permet de différencier les autorisations sur différents ensembles de périphériques.

Remarque : les groupes de périphériques Cisco Secure ACS sont indépendants des groupes de périphériques Security Manager.

Les rubriques suivantes décrivent les rôles Cisco Secure ACS :

Rôles par défaut Cisco Secure ACS

Cisco Secure ACS inclut les mêmes rôles que CiscoWorks (voir Comprendre les rôles CiscoWorks), ainsi que les rôles supplémentaires suivants :

1. **Approbateur de sécurité** : les approbateurs de sécurité peuvent afficher (mais pas modifier) les périphériques, les stratégies, les objets, les cartes, les commandes CLI et les paramètres d'administration. En outre, les approbateurs de sécurité peuvent approuver ou rejeter les modifications de configuration contenues dans une activité. Ils ne peuvent pas approuver ou rejeter la tâche de déploiement, ni effectuer de déploiement.
2. **Administrateur de la sécurité** - En plus d'avoir des autorisations d'affichage, les administrateurs de la sécurité peuvent modifier les périphériques, les groupes de périphériques, les stratégies, les objets et les cartes topologiques. Ils peuvent également affecter des politiques aux périphériques et aux topologies VPN, et effectuer une détection pour importer de nouveaux périphériques dans le système.
3. **Administrateur réseau** - Outre les autorisations d'affichage, les administrateurs réseau peuvent modifier l'archive de configuration, effectuer le déploiement et émettre des commandes sur les périphériques.

Remarque : Les autorisations contenues dans le rôle d'administrateur réseau Cisco Secure ACS sont différentes de celles contenues dans le rôle d'administrateur réseau CiscoWorks. Pour plus d'informations, consultez Présentation des rôles CiscoWorks.

Contrairement à CiscoWorks, Cisco Secure ACS vous permet de personnaliser les autorisations associées à chaque rôle Security Manager. Pour plus d'informations sur la modification des rôles par défaut, consultez Personnalisation des rôles Cisco Secure ACS.

Remarque : Cisco Secure ACS 3.3 ou version ultérieure doit être installé pour l'autorisation de Security Manager.

Personnalisation des rôles Cisco Secure ACS

Cisco Secure ACS vous permet de modifier les autorisations associées à chaque rôle Security Manager. Vous pouvez également personnaliser Cisco Secure ACS en créant des rôles d'utilisateurs spécialisés avec des autorisations ciblées sur des tâches spécifiques du Gestionnaire de sécurité.

Remarque : Vous devez redémarrer Security Manager après avoir modifié les autorisations utilisateur.

Procédure:

1. Dans Cisco Secure ACS, cliquez sur **Composants de profil partagé** dans la barre de navigation.
2. Cliquez sur **Cisco Security Manager** sur la page Shared Components. Les rôles configurés pour Security Manager s'affichent.
3. Effectuez l'une des opérations suivantes :Pour créer un rôle, cliquez sur **Ajouter**. Passez à

l'étape 4.Pour modifier un rôle existant, cliquez sur le rôle. Passez à l'étape 5.

4. Entrez un nom pour le rôle et éventuellement une description.
5. Activez et désélectionnez les cases à cocher de l'arborescence des autorisations pour définir les autorisations de ce rôleLa case à cocher d'une branche de l'arborescence sélectionne toutes les autorisations de cette branche. Par exemple, la sélection **Affecter** sélectionne toutes les autorisations d'affectation.Pour obtenir une liste complète des autorisations du Gestionnaire de sécurité, consultez Autorisations du Gestionnaire de sécurité.**Remarque :** Lorsque vous sélectionnez les autorisations de modification, d'approbation, d'affectation, d'importation, de contrôle ou de déploiement, vous devez également sélectionner les autorisations d'affichage correspondantes ; sinon, Security Manager ne fonctionnera pas correctement.
6. Cliquez sur **Submit pour enregistrer les modifications.**
7. Redémarrez Security Manager.

Associations par défaut entre les autorisations et les rôles dans Security Manager

Ce tableau montre comment les autorisations Security Manager sont associées aux rôles CiscoWorks Common Services et aux rôles par défaut dans Cisco Secure ACS.

Autorisations	Rôles							
	Administrateur système	Security Admin (ACS)	Approbateur de sécurité (ACS)	Admin réseau (CW)	Administration réseau (ACS)	Approbateur	Opérateur réseau	Centre d'assistance
Afficher les autorisations								
Afficher le périphérique	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Afficher la stratégie	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Afficher les objets	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Afficher la topologie	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Afficher CLI	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non
Afficher Admin	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non
Afficher l'archive de configuratio	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui

n								
Afficher les gestionnaires de périphériques	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non
Modifier les autorisations								
Modifier le périphérique	Oui	Oui	Non	Oui	Non	Non	Non	Non
Modifier la hiérarchie	Oui	Oui	Non	Oui	Non	Non	Non	Non
Modifier la stratégie	Oui	Oui	Non	Oui	Non	Non	Non	Non
Modifier l'image	Oui	Oui	Non	Oui	Non	Non	Non	Non
Modifier des objets	Oui	Oui	Non	Oui	Non	Non	Non	Non
Modifier la topologie	Oui	Oui	Non	Oui	Non	Non	Non	Non
Modifier Admin	Oui	Non	Non	Non	Non	Non	Non	Non
Modifier l'archive de configuration	Oui	Oui	Non	Oui	Oui	Non	Oui	Non
Autorisations supplémentaires								
Affecter une stratégie	Oui	Oui	Non	Oui	Non	Non	Non	Non
Approuver la stratégie	Oui	Non	Oui	Non	Non	Non	Non	Non
Approuver CLI	Oui	Non	Non	Non	Non	Oui	Non	Non
Découvrir (Importer)	Oui	Oui	Non	Oui	Non	Non	Non	Non
Déployer	Oui	Non	Non	Oui	Oui	Non	Non	Non
Contrôle	Oui	Non	Non	Oui	Oui	Non	Oui	Non
Envoyer	Oui	Oui	Non	Oui	Non	Non	Non	Non

Informations connexes

- Page d'assistance de Cisco Security Manager
- Support et documentation techniques - Cisco Systems