CSM 3.x : Configurer les autorisations et rôles utilisateur

Contenu

Introduction

Ce document décrit comment installer les autorisations et les rôles aux utilisateurs dans le Cisco Security Manager (CSM).

Conditions préalables

Conditions requises

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

Composants utilisés

Les informations dans ce document sont basées sur le CSM 3.1.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Autorisations utilisateur d'installation

Le Cisco Security Manager authentifie votre nom d'utilisateur et mot de passe avant que vous puissiez ouvrir une session. Après qu'ils soient authentifiés, le directeur de la sécurité établit votre rôle dans l'application. Ce rôle définit vos autorisations (privilèges également appelés), qui sont l'ensemble de tâches ou des exécutions que vous êtes autorisé à exécuter. Si vous n'êtes pas autorisé pour de certains tâches ou périphériques, les commandes de menu relatives, des éléments TOC, et les boutons sont masqués ou désactivés. En outre, un message t'indique que vous n'avez pas l'autorisation de visualiser les informations sélectionnées ou d'exécuter l'exécution sélectionnée.

L'authentification et l'autorisation pour le directeur de la sécurité est gérée par le serveur de CiscoWorks ou le Cisco Secure Access Control Server (ACS). Par défaut, les CiscoWorks gèrent l'authentification et l'autorisation, mais vous pouvez changer en le Cisco Secure ACS à l'aide de la page d'installation de mode d'AAA dans des services de terrain communal de CiscoWorks.

Les principaux avantages d'utiliser le Cisco Secure ACS sont la capacité de créer des rôles de l'utilisateur fortement granulaires avec les positionnements spécialisés d'autorisations (par exemple, permettant à l'utilisateur pour configurer certaine stratégie tape mais pas d'autres) et la capacité de limiter des utilisateurs à certains périphériques en configurant des groupes de périphériques réseau (NDGs).

Les thèmes suivants décrivent des autorisations utilisateur :

- Autorisations de directeur de la sécurité
- Compréhension des rôles de CiscoWorks
- Compréhension des rôles de Cisco Secure ACS
- Associations par défaut entre les autorisations et les rôles dans le directeur de la sécurité

Autorisations de directeur de la sécurité

Le directeur de la sécurité classifie des autorisations dans les catégories comme affichées :

1. **Vue** — Te permet pour visualiser les configurations actuelles. Le pour en savoir plus, voient des autorisations de vue.
2. **Modifiez** — Te permet pour changer les configurations actuelles. Le pour en savoir plus, voient pour modifier des autorisations.
3. **Assignez** — Te permet pour assigner des stratégies aux périphériques et aux topologies VPN. Le pour en savoir plus, voient pour assigner des autorisations
4. **Approuvez** — Te permet pour approuver des changements de politique et des travaux de

déploiement. Le pour en savoir plus, voient pour approuver des autorisations.
5. **Importation** — Te permet pour importer les configurations qui sont déjà déployées sur des périphériques dans le directeur de la sécurité.
6. **Déployez-vous** — Te permet pour déployer des changements de configuration aux périphériques de votre réseau et pour exécuter le repositionnement pour retourner à une configuration précédemment déployée.
7. **Contrôle** — Te permet pour fournir des commandes aux périphériques, tels que le ping.
8. **Soumettez** — Te permet pour soumettre vos modifications de configuration pour approbation.

- Quand vous sélectionnez modifiez, assignez, approuvez, importez, contrôlez ou déployez les autorisations, vous doit également sélectionner les autorisations correspondantes de vue ; autrement, le directeur de la sécurité ne fonctionnera pas correctement.
- Quand vous sélectionnez modifiez les autorisations de stratégie, vous devez également sélectionner la correspondance assignez et visualisez des autorisations de stratégie.
- Quand vous permettez une stratégie qui utilise des objets de stratégie en tant qu'élément de sa définition, vous devez également accorder des autorisations de vue à ces types d'objet. Par exemple, si vous sélectionnez l'autorisation pour modifier des stratégies de routage, vous devez également sélectionner les autorisations pour les objets de réseau et les rôles de visionnement d'interface, qui sont les types d'objet exigés en conduisant des stratégies.
- Le même juge vrai en permettant un objet qui utilise d'autres objets en tant qu'élément de sa définition. Par exemple, si vous sélectionnez l'autorisation pour modifier des groupes d'utilisateurs, vous devez également sélectionner les autorisations pour les objets de réseau, les objets d'ACL, et les Groupes de serveurs AAA de visionnement.

Autorisations de vue

Des autorisations (en lecture seule) de vue dans le directeur de la sécurité sont divisées en catégories comme affichées :

- Autorisations de stratégies de vue
- Autorisations de vues standard
- Autorisations supplémentaires de vue

Autorisations de stratégies de vue

Le directeur de la sécurité inclut les autorisations suivantes de vue pour des stratégies :

1. **Vue > stratégies > Pare-feu.** Te permet pour visualiser des stratégies de service de Pare-feu (situées dans le sélecteur de stratégie sous le Pare-feu) sur des périphériques PIX/ASA/FWSM, des Routeurs IOS, et des périphériques du Catalyst 6500/7600. Les exemples des stratégies de service de Pare-feu incluent des règles d'accès, des règles d'AAA, et des règles d'inspection.
2. **Vue > stratégies > système de prévention des intrusions.** Te permet pour visualiser des stratégies IPS (situées dans le sélecteur de stratégie sous l'IPS), y compris des stratégies pour l'exécution IPS sur des Routeurs IOS.
3. **Vue > stratégies > image.** Te permet pour sélectionner un module de mise à jour de signature dans l'assistant de mises à jour IPS d'application (situé sous des outils > appliquez

la mise à jour IPS), mais ne te permet pas pour assigner le module aux appareils spécifiques, à moins que vous ayez également l'autorisation de modifier > de stratégies > d'image.

4. **Vue > stratégies > NAT**. Vous permet aux stratégies de traduction d'adresses de View Network sur des périphériques PIX/ASA/FWSM et des Routeurs IOS. Les exemples des stratégies NAT incluent des règles statiques et des règles dynamiques.
5. **Vue > stratégies > site à site VPN**. Te permet pour visualiser des règles VPN de site à site sur des périphériques PIX/ASA/FWSM, des Routeurs IOS, et des périphériques du Catalyst 6500/7600. Les exemples des règles VPN de site à site incluent des propositions d'IKE, des propositions d'IPsec, et des clés pré-partagées.
6. **Vue > stratégies > Accès à distance VPN**. Te permet pour visualiser des règles VPN d'Accès à distance sur des périphériques PIX/ASA/FWSM, des Routeurs IOS, et des périphériques du Catalyst 6500/7600. Les exemples des règles VPN d'Accès à distance incluent des propositions d'IKE, des propositions d'IPsec, et des stratégies de PKI.
7. **Vue > stratégies > VPN SSL**. Te permet pour visualiser des stratégies de VPN SSL sur des périphériques PIX/ASA/FWSM et des Routeurs IOS, tels que l'assistant de VPN SSL.
8. **Vue > stratégies > interfaces**. Te permet pour visualiser des stratégies d'interface (situées dans le sélecteur de stratégie sous des interfaces) sur des périphériques PIX/ASA/FWSM, des Routeurs IOS, des capteurs IPS, et des périphériques du Catalyst 6500/7600.Sur des périphériques PIX/ASA/FWSM, cette autorisation couvre des ports et des paramètres d'interface de matériel.Sur des Routeurs IOS, cette autorisation couvre les paramètres d'interface de base et avancés, aussi bien que d'autres stratégies liées à l'interface, telles que le DSL, le PVC, le PPP, et les stratégies de numéroteur.Sur des capteurs IPS, cette autorisation couvre des interfaces physiques et des cartes de résumé.Sur des périphériques du Catalyst 6500/7600, cette autorisation couvre des interfaces et des configurations VLAN.
9. **Vue > stratégies > jetant un pont sur**. Te permet pour visualiser des stratégies de table ARP (situées dans le sélecteur de stratégie sous la plate-forme > jetant un pont sur) sur des périphériques PIX/ASA/FWSM.
10. **Vue > stratégies > gestion de périphérique**. Te permet pour visualiser des stratégies de gestion de périphérique (situées dans le sélecteur de stratégie sous l'admin de plate-forme > de périphérique) sur des périphériques PIX/ASA/FWSM, des Routeurs IOS, et des périphériques du Catalyst 6500/7600 :Sur des périphériques PIX/ASA/FWSM, les exemples incluent l'accès au périphérique maintient l'ordre, des stratégies d'accès de serveur, et des stratégies de Basculement.Sur des Routeurs IOS, les exemples incluent l'accès au périphérique (accès à la ligne y compris) maintient l'ordre, des stratégies d'accès de serveur, AAA, et sécurise le ravitaillement de périphérique.Sur des capteurs IPS, cette autorisation couvre des stratégies d'accès au périphérique et des stratégies d'accès de serveur.Sur des périphériques du Catalyst 6500/7600, cette autorisation couvre des configurations IDSM et des Listes d'accès VLAN.
11. **Vue > stratégies > identité**. Te permet pour visualiser des stratégies d'identité (situées dans le sélecteur de stratégie sous la plate-forme > l'identité) sur des routeurs Cisco IOS, y compris le 802.1x et les stratégies de Contrôle d'admission au réseau (NAC).
12. **Vue > stratégies > se connectant**. Te permet pour visualiser se connecter des stratégies (situées dans le sélecteur de stratégie sous la plate-forme > se connectant) sur des périphériques PIX/ASA/FWSM, des Routeurs IOS, et des capteurs IPS. Les exemples de se connecter des stratégies incluent se connecter l'installation, la configuration du serveur, et les stratégies de serveur de Syslog.
13. **Vue > stratégies > Multidiffusion**. Te permet pour visualiser des stratégies de Multidiffusion

(situées dans le sélecteur de stratégie sous la plate-forme > la Multidiffusion) sur des périphériques PIX/ASA/FWSM. Les exemples des stratégies de Multidiffusion incluent le routage de Multidiffusion et les stratégies IGMP.

14. **Vue > stratégies > QoS**. Te permet pour visualiser des stratégies QoS (situées dans le sélecteur de stratégie sous la plate-forme > la qualité de service) sur des routeurs Cisco IOS.
15. **Vue > stratégies > routage**. Te permet pour visualiser des stratégies de routage (situées dans le sélecteur de stratégie sous la plate-forme > le routage) sur des périphériques PIX/ASA/FWSM et des Routeurs IOS. Les exemples des stratégies de routage incluent l'OSPF, le RIP, et les stratégies statiques de routage.
16. **Vue > stratégies > Sécurité**. Te permet pour visualiser des stratégies de sécurité (situées dans le sélecteur de stratégie sous la plate-forme > la Sécurité) sur des périphériques PIX/ASA/FWSM et des capteurs IPS :Sur des périphériques PIX/ASA/FWSM, les stratégies de sécurité incluent l'anti-mystification, le fragment, et les configurations de délai d'attente.Sur des capteurs IPS, les stratégies de sécurité incluent bloquer des configurations.
17. **Règles de vue > de stratégies > de stratégie de service**. Te permet pour visualiser des stratégies de règle de stratégie de service (situées dans le sélecteur de stratégie dans le cadre de la stratégie de plate-forme > de service ordonne) sur des périphériques PIX 7.x/ASA. Les exemples incluent des files d'attente prioritaire et IPS, QoS, et des règles de connexion.
18. **Vue > stratégies > préférences de l'utilisateur**. Te permet pour visualiser la stratégie de déploiement (située dans le sélecteur de stratégie sous la plate-forme > les préférences de l'utilisateur) sur des périphériques PIX/ASA/FWSM. Cette stratégie contient une option pour effacer toutes les traductions NAT sur le déploiement.
19. **Vue > stratégies > périphérique virtuel**. Te permet pour visualiser des stratégies virtuelles de capteur sur des périphériques IPS. Cette stratégie est utilisée pour créer les capteurs virtuels.
20. **Vue > stratégies > FlexConfig**. Te permet pour visualiser FlexConfigs, qui sont des commandes supplémentaires et des instructions CLI qui peuvent être déployées vers des périphériques PIX/ASA/FWSM, des Routeurs IOS, et des périphériques du Catalyst 6500/7600.

Autorisations de vues standard

Le directeur de la sécurité inclut les autorisations suivantes de vue pour des objets :

1. **La vue > objecte > des Groupes de serveurs AAA**. Te permet pour visualiser des objets de Groupe de serveurs AAA. Ces objets sont utilisés dans les stratégies qui exigent des services d'AAA (authentification, autorisation, et comptabilité).
2. **La vue > objecte > des serveurs d'AAA**. Te permet pour visualiser des objets de serveur d'AAA. Ces objets représentent les différents serveurs d'AAA qui sont définis en tant qu'élément d'un Groupe de serveurs AAA.
3. **La vue > objecte > des listes de contrôle d'accès - Standard/a étendu**. Te permet pour visualiser les objets standard et étendus d'ACL. Des objets étendus d'ACL sont utilisés pour un grand choix de stratégies, telles que NAT et le NAC, et pour établir l'accès VPN. Des objets standard d'ACL sont utilisés pour des stratégies telles que l'OSPF et le SNMP, aussi bien que pour établir l'accès VPN.

4. **La vue > objecte > des listes de contrôle d'accès** - Web. Te permet pour visualiser des objets d'ACL de Web. Des objets d'ACL de Web sont utilisés pour exécuter le filtrage selon le contenu dans des stratégies de VPN SSL.
5. **La vue > objecte > des groupes d'utilisateurs ASA**. Te permet pour visualiser des objets de groupe d'utilisateurs ASA. Ces objets sont configurés sur des dispositifs de sécurité ASA dans l'Easy VPN, l'Accès à distance VPN, et les configurations de VPN SSL.
6. **La vue > objecte > des catégories**. Te permet pour visualiser des objets de catégorie. Ces objets vous aident facilement à identifier des règles et des objets dans des tables de règles par l'utilisation de couleur.
7. **La vue > objecte > des qualifications**. Te permet pour visualiser les objets de créance. Ces objets sont utilisés en configuration Easy VPN pendant le Fonction IKE Extended Authentication (Xauth).
8. **La vue > objecte > FlexConfigs**. Te permet pour visualiser des objets de FlexConfig. Ces objets, qui contiennent des commandes de configuration avec des instructions supplémentaires de langage de script, peuvent être utilisés pour configurer les commandes qui ne sont pas prises en charge par l'interface utilisateur de directeur de la sécurité.
9. **La vue > objecte > des propositions d'IKE**. Te permet pour visualiser des objets de proposition d'IKE. Ces objets contiennent les paramètres exigés pour des propositions d'IKE dans des règles VPN d'Accès à distance.
10. **La vue > les objets > examinent - Class map** - DN. Te permet pour visualiser des objets de class map de DN. Ces objets apparient le trafic DNS avec des critères spécifiques de sorte que des actions puissent être exécutées sur ce trafic.
11. **La vue > les objets > examinent - Class map - FTP**. Te permet pour visualiser des objets de class map de FTP. Ces objets apparient le trafic FTP avec des critères spécifiques de sorte que des actions puissent être exécutées sur ce trafic.
12. **La vue > les objets > examinent - Class map - HTTP**. Te permet pour visualiser des objets de class map de HTTP. Ces objets apparient le trafic http avec des critères spécifiques de sorte que des actions puissent être exécutées sur ce trafic.
13. **La vue > les objets > examinent - Class map - IM**. Te permet pour visualiser des objets du class map IM. Le trafic de la correspondance IM de ces objets avec des critères spécifiques de sorte que des actions puissent être exécutées sur ce trafic.
14. **La vue > les objets > examinent - Class map - SIP**. Te permet pour visualiser des objets de class map de SIP. Ces objets apparient le trafic de SIP avec des critères spécifiques de sorte que des actions puissent être exécutées sur ce trafic.
15. **La vue > les objets > examinent - Cartes de stratégie - DN.** Te permet pour visualiser des objets de carte de stratégie de DN. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic DNS.
16. **La vue > les objets > examinent - Cartes de stratégie - FTP.** Te permet pour visualiser des objets de carte de stratégie de FTP. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic FTP.
17. **La vue > les objets > examinent - Cartes de stratégie - GTP**. Te permet pour visualiser des objets de carte de stratégie GTP. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic GTP.
18. **La vue > les objets > examinent - Cartes de stratégie - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Te permet pour visualiser des objets de carte de stratégie de HTTP créés pour des périphériques ASA/PIX 7.1.x et des Routeurs IOS. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic http.
19. **La vue > les objets > examinent - Cartes de stratégie - HTTP (ASA7.2/PIX7.2)**. Te permet

pour visualiser des objets de carte de stratégie de HTTP créés pour des périphériques ASA 7.2/PIX 7.2. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic http.

20. **La vue > les objets > examinent - Cartes de stratégie - IM (ASA7.2/PIX7.2)**. Te permet pour visualiser des objets de carte de la stratégie IM créés pour des périphériques ASA 7.2/PIX 7.2. Ces objets sont utilisés pour créer des cartes d'inspection pour IM le trafic.
21. **La vue > les objets > examinent - Cartes de stratégie - IM (IOS)**. Te permet pour visualiser des objets de carte de la stratégie IM créés pour des périphériques IOS. Ces objets sont utilisés pour créer des cartes d'inspection pour IM le trafic.
22. **La vue > les objets > examinent - Cartes de stratégie - SIP**. Te permet pour visualiser des objets de carte de stratégie de SIP. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic de SIP.
23. **La vue > les objets > examinent - Expressions régulières**. Te permet pour visualiser des objets d'expression régulière. Ces objets représentent les différentes expressions régulières qui sont définies en tant qu'élément d'un groupe d'expression régulière.
24. **La vue > les objets > examinent - Groupes d'expressions régulières**. Te permet pour visualiser des objets de groupe d'expression régulière. Ces objets sont utilisés par certains class map et examinent des cartes pour apparier le texte à l'intérieur d'un paquet.
25. **La vue > les objets > examinent - Cartes de TCP**. Te permet pour visualiser des objets de carte de TCP. Ces objets personnalisent l'inspection sur l'écoulement de TCP dans les deux directions.
26. **La vue > objecte > des rôles d'interface**. Te permet pour visualiser des objets de rôle d'interface. Ces objets définissent nommer les modèles qui peuvent représenter des plusieurs interfaces sur différents types de périphériques. Enable de rôles d'interface vous pour s'appliquer des stratégies aux interfaces spécifiques sur de plusieurs périphériques sans devoir manuellement définir le nom de chaque interface.
27. **La vue > objecte > des jeux de transformations d'IPsec**. Te permet pour visualiser des objets de jeu de transformations d'IPsec. Ces objets comportent une combinaison des protocoles de Sécurité, des algorithmes et d'autres configurations qui spécifient exactement comment les données dans le tunnel d'IPsec seront chiffrées et authentifiées.
28. **La vue > objecte > des cartes d'attribut de LDAP**. Te permet pour visualiser des objets de carte d'attribut de LDAP. Ces objets sont utilisés pour tracer des noms (définis par l'utilisateur) faits sur commande d'attribut aux noms d'attribut de LDAP de Cisco.
29. **La vue > objecte > des réseaux/hôtes**. Vous permet aux objets de View Network/hôte. Ces objets sont les collections logiques d'adresses IP qui représentent des réseaux, des hôtes, ou chacun des deux. Les objets de réseau/hôte te permettent de définir des stratégies sans spécifier chaque réseau ou de les héberger individuellement.
30. **La vue > objecte > des inscriptions de PKI**. Te permet pour visualiser des objets d'inscription de PKI. Ces objets définissent les serveurs de l'autorité de certification (CA) qui fonctionnent dans une infrastructure de clé publique.
31. **La vue > objecte > des listes de transmission du port**. Te permet pour visualiser des objets de liste de transmission du port. Ces objets définissent les mappages des numéros de port sur un client distant à l'adresse IP de l'application et mettent en communication derrière une passerelle de VPN SSL.
32. **La vue > objecte > des configurations de Secure Desktop**. Te permet pour visualiser des objets de configuration de Secure Desktop. Ces objets sont des composants réutilisables et Désignés qui peuvent être mis en référence par des stratégies de VPN SSL pour fournir le moyen fiable d'éliminer tous les suivis des données sensibles qui sont partagées pour la durée d'une session de VPN SSL.

33. **La vue > objecte > des services - Listes des ports**. Te permet pour visualiser des objets de liste des ports. Ces objets, qui contiennent un ou plusieurs nombres de plages de port, sont utilisés pour rationaliser le processus de créer des objets de service.
34. **La vue > objecte > des services/groupes de service** te permet pour visualiser des objets de service et de groupe de service. Ces objets sont les mappages définis du protocole et mettent en communication les définitions qui décrivent des services réseau utilisés par des stratégies, telles que le Kerberos, le SSH, et le POP3.
35. **La vue > objecte > simple se connectent des serveurs**. Te permet pour visualiser simple se connectent des objets de serveur. L'ouverture de session simple (SSO) permet des utilisateurs de VPN SSL d'écrire un nom d'utilisateur et mot de passe une fois et de pouvoir accéder à des services et des web server protégés par multiple.
36. **La vue > objecte > des moniteurs de SLA**. Te permet pour visualiser des objets de moniteur de SLA. Ces objets sont utilisés par des appliances de Sécurité PIX/ASA exécutant la version 7.2 ou ultérieures pour exécuter le cheminement d'artère. Cette caractéristique fournit une méthode pour dépister la Disponibilité d'une route primaire et pour installer une route de secours si la route primaire échoue.
37. **La vue > objecte > des personnalisations de VPN SSL**. Te permet pour visualiser des objets de personnalisation de VPN SSL. Ces objets définissent comment changer l'apparence des pages de VPN SSL qui sont affichées aux utilisateurs, tels que la procédure de connexion/déconnexion et les pages d'accueil.
38. **La vue > objecte > des passerelles de VPN SSL**. Te permet pour visualiser des objets de passerelle de VPN SSL. Ces objets définissent les paramètres qui permettent à la passerelle d'être utilisée comme proxy pour des connexions aux ressources protégées dans votre VPN SSL.
39. **La vue > objecte > des objets de style**. Te permet pour visualiser des objets de style. Ces objets vous permettent de configurer des éléments de style, tels que des caractéristiques de la police et des couleurs, pour personnaliser l'apparence de la page de VPN SSL qui paraît aux utilisateurs de VPN SSL quand ils se connectent aux dispositifs de sécurité.
40. **La vue > objecte > des objets des textes**. Te permet pour visualiser des objets des textes de libre-forme. Ces objets comportent une paire de nom et de valeur, où la valeur peut être une chaîne simple, une liste de chaînes, ou une table des chaînes.
41. **La vue > objecte > des plages de temps.** Te permet pour visualiser des objets de plage de temps. Ces objets sont utilisés en créant des règles basées sur temps d'ACLs et d'inspection. Ils sont également utilisés en définissant des groupes d'utilisateurs ASA pour limiter l'accès VPN aux heures précises pendant la semaine.
42. **La vue > objecte > la circulation**. Te permet pour visualiser des objets de la circulation. Ces objets définissent la circulation spécifique à l'usage des périphériques PIX 7.x/ASA 7.x.
43. **La vue > objecte > des listes URL**. Te permet pour visualiser des objets de liste URL. Ces objets définissent l'URLs qui sont affichés sur la page du portail après une procédure de connexion réussie. Ceci permet à des utilisateurs d'accéder aux ressources disponibles sur des sites Web de VPN SSL en fonctionnant dans le mode d'accès sans client.
44. **La vue > objecte > des groupes d'utilisateurs**. Te permet pour visualiser des objets de groupe d'utilisateurs. Ces objets définissent des groupes de clients distants qui sont utilisés dans des topologies d'Easy VPN, l'Accès à distance VPN, et des VPN SSL.
45. **La vue > objecte > des listes de serveur WINS**. Te permet pour visualiser des objets de liste de serveur WINS. Ces objets représentent les serveurs WINS, qui sont utilisés par VPN SSL pour accéder à ou fichiers partagés sur des systèmes distants.
46. **La vue > objecte > interne - Règles de DN**. Te permet pour visualiser les règles de DN

utilisées par des stratégies de DN. C'est un objet interne utilisé par le directeur de la sécurité qui n'apparaît pas dans le gestionnaire d'objet de stratégie.

47. **La vue > objecte > des mises à jour de client interne**. C'est un objet interne exigé par des objets de groupe d'utilisateurs qui n'apparaît pas dans le gestionnaire d'objet de stratégie.
48. **La vue > objecte > interne - As standard**. C'est un objet interne pour les entrées de contrôle d'accès standard, qui sont utilisées par des objets d'ACL.
49. **La vue > objecte > interne - As étendus.** C'est un objet interne pour les entrées de contrôle d'accès étendues, qui sont utilisées par des objets d'ACL.

Autorisations supplémentaires de vue

Le directeur de la sécurité inclut les autorisations supplémentaires suivantes de vue :

1. **Vue > admin**. Te permet pour visualiser des paramètres administratifs de directeur de la sécurité.
2. **Vue > CLI**. Te permet pour visualiser les commandes CLI configurées sur un périphérique et pour visionner les commandes préalablement qui sont sur le point d'être déployées.
3. **Vue > Config Archive**. Te permet pour visualiser la liste de configurations contenues dans les archives de configuration. Vous ne pouvez visualiser la configuration de périphérique ou aucune commandes CLI.
4. **Vue > périphériques**. Te permet pour visualiser des périphériques en vue l'affichage périphériques et toutes les informations relatives, y compris leurs paramètres de périphérique, des propriétés, des affectations, et ainsi de suite.
5. **Vue > gestionnaires de périphériques**. Te permet pour lancer des versions en lecture seule des gestionnaires de périphériques pour différents périphériques, tels que le Cisco Router and Security Device Manager (SDM) pour des routeurs Cisco IOS.
6. **Vue > topologie**. Te permet pour visualiser des cartes configurées dans la vue de carte.

Modifiez les autorisations

Modifiez les autorisations (lecture/écriture) dans le directeur de la sécurité sont divisés en catégories comme affichées :

- Modifiez les autorisations de stratégies
- Modifiez les autorisations d'objets
- Supplémentaire modifiez les autorisations

Modifiez les autorisations de stratégies

Remarque: Quand vous spécifiez modifiez les autorisations de stratégie, s'assurent que vous avez sélectionné la correspondance assignez et visualisent des autorisations de stratégie aussi bien.

Le directeur de la sécurité inclut le suivant modifient des autorisations pour des stratégies :

1. **Modifiez > des stratégies > Pare-feu**. Te permet pour modifier des stratégies de service de Pare-feu (situées dans le sélecteur de stratégie sous le Pare-feu) sur des périphériques PIX/ASA/FWSM, des Routeurs IOS, et des périphériques du Catalyst 6500/7600. Les exemples des stratégies de service de Pare-feu incluent des règles d'accès, des règles

d'AAA, et des règles d'inspection.

2. **Modifiez > les stratégies > le système de prévention des intrusions**. Te permet pour modifier des stratégies IPS (situées dans le sélecteur de stratégie sous l'IPS), y compris des stratégies pour l'exécution IPS sur des Routeurs IOS. Cette autorisation te permet également pour accorder des signatures dans l'assistant de mise à jour de signature (situé sous des outils > appliquez la mise à jour IPS).
3. **Modifiez > des stratégies > image**. Te permet pour assigner un module de mise à jour de signature aux périphériques dans l'assistant de mises à jour IPS d'application (situé sous des outils > appliquez la mise à jour IPS). Cette autorisation te permet également pour assigner les configurations automatiques de mise à jour aux appareils spécifiques (situés sous les outils > la gestion de directeur de la sécurité > les mises à jour IPS).
4. **Modifiez > des stratégies > NAT**. Te permet pour modifier des stratégies de traduction d'adresses réseau sur des périphériques PIX/ASA/FWSM et des Routeurs IOS. Les exemples des stratégies NAT incluent des règles statiques et des règles dynamiques.
5. **Modifiez > les stratégies > le site à site VPN**. Te permet pour modifier des règles VPN de site à site sur des périphériques PIX/ASA/FWSM, des Routeurs IOS, et des périphériques du Catalyst 6500/7600. Les exemples des règles VPN de site à site incluent des propositions d'IKE, des propositions d'IPsec, et des clés pré-partagées.
6. **Modifiez > des stratégies > l'Accès à distance VPN**. Te permet pour modifier des règles VPN d'Accès à distance sur des périphériques PIX/ASA/FWSM, des Routeurs IOS, et des périphériques du Catalyst 6500/7600. Les exemples des règles VPN d'Accès à distance incluent des propositions d'IKE, des propositions d'IPsec, et des stratégies de PKI.
7. **Modifiez > des stratégies > VPN SSL**. Te permet pour modifier des stratégies de VPN SSL sur des périphériques PIX/ASA/FWSM et des Routeurs IOS, tels que l'assistant de VPN SSL.
8. **Modifiez > des stratégies > des interfaces**. Te permet pour modifier des stratégies d'interface (situées dans le sélecteur de stratégie sous des interfaces) sur des périphériques PIX/ASA/FWSM, des Routeurs IOS, des capteurs IPS, et des périphériques du Catalyst 6500/7600 :Sur des périphériques PIX/ASA/FWSM, cette autorisation couvre des ports et des paramètres d'interface de matériel.Sur des Routeurs IOS, cette autorisation couvre les paramètres d'interface de base et avancés, aussi bien que d'autres stratégies liées à l'interface, telles que le DSL, le PVC, le PPP, et les stratégies de numéroteur.Sur des capteurs IPS, cette autorisation couvre des interfaces physiques et des cartes de résumé.Sur des périphériques du Catalyst 6500/7600, cette autorisation couvre des interfaces et des configurations VLAN.
9. **Modifiez > des stratégies > en jetant un pont sur**. Te permet pour modifier des stratégies de table ARP (situées dans le sélecteur de stratégie sous la plate-forme > jetant un pont sur) sur des périphériques PIX/ASA/FWSM.
10. **Modifiez > les stratégies > la gestion de périphérique**. Te permet pour modifier des stratégies de gestion de périphérique (situées dans le sélecteur de stratégie sous l'admin de plate-forme > de périphérique) sur des périphériques PIX/ASA/FWSM, des Routeurs IOS, et des périphériques du Catalyst 6500/7600 :Sur des périphériques PIX/ASA/FWSM, les exemples incluent l'accès au périphérique maintient l'ordre, des stratégies d'accès de serveur, et des stratégies de Basculement.Sur des Routeurs IOS, les exemples incluent l'accès au périphérique (accès à la ligne y compris) maintient l'ordre, des stratégies d'accès de serveur, AAA, et sécurise le ravitaillement de périphérique.Sur des capteurs IPS, cette autorisation couvre des stratégies d'accès au périphérique et des stratégies d'accès de serveur.Sur des périphériques du Catalyst 6500/7600, cette autorisation couvre les

configurations IDSM et la liste d'accès VLAN.

11. **Modifiez > des stratégies > identité**. Te permet pour modifier des stratégies d'identité (situées dans le sélecteur de stratégie sous la plate-forme > l'identité) sur des routeurs Cisco IOS, y compris le 802.1x et les stratégies de Contrôle d'admission au réseau (NAC).
12. **Modifiez > des stratégies > en se connectant**. Te permet pour modifier se connecter des stratégies (situées dans le sélecteur de stratégie sous la plate-forme > se connectant) sur des périphériques PIX/ASA/FWSM, des Routeurs IOS, et des capteurs IPS. Les exemples de se connecter des stratégies incluent se connecter l'installation, la configuration du serveur, et les stratégies de serveur de Syslog.
13. **Modifiez > des stratégies > Multidiffusion**. Te permet pour modifier des stratégies de Multidiffusion (situées dans le sélecteur de stratégie sous la plate-forme > la Multidiffusion) sur des périphériques PIX/ASA/FWSM. Les exemples des stratégies de Multidiffusion incluent le routage de Multidiffusion et les stratégies IGMP.
14. **Modifiez > des stratégies > QoS**. Te permet pour modifier des stratégies QoS (situées dans le sélecteur de stratégie sous la plate-forme > la qualité de service) sur des routeurs Cisco IOS.
15. **Modifiez > des stratégies > routage**. Te permet pour modifier des stratégies de routage (situées dans le sélecteur de stratégie sous la plate-forme > le routage) sur des périphériques PIX/ASA/FWSM et des Routeurs IOS. Les exemples des stratégies de routage incluent l'OSPF, le RIP, et les stratégies statiques de routage.
16. **Modifiez > des stratégies > Sécurité**. Te permet pour modifier des stratégies de sécurité (situées dans le sélecteur de stratégie sous la plate-forme > la Sécurité) sur des périphériques PIX/ASA/FWSM et des capteurs IPS :Sur des périphériques PIX/ASA/FWSM, les stratégies de sécurité incluent l'anti-mystification, le fragment, et les configurations de délai d'attente.Sur des capteurs IPS, les stratégies de sécurité incluent bloquer des configurations.
17. **Modifiez > des règles de stratégies > de stratégie de service**. Te permet pour modifier des stratégies de règle de stratégie de service (situées dans le sélecteur de stratégie dans le cadre de la stratégie de plate-forme > de service ordonne) sur des périphériques PIX 7.x/ASA. Les exemples incluent des files d'attente prioritaire et IPS, QoS, et des règles de connexion.
18. **Modifiez > des stratégies > des préférences de l'utilisateur**. Te permet pour modifier la stratégie de déploiement (située dans le sélecteur de stratégie sous la plate-forme > les préférences de l'utilisateur) sur des périphériques PIX/ASA/FWSM. Cette stratégie contient une option pour effacer toutes les traductions NAT sur le déploiement.
19. **Modifiez > les stratégies > le périphérique virtuel**. Te permet pour modifier des stratégies virtuelles de capteur sur des périphériques IPS. Employez cette stratégie pour créer les capteurs virtuels.
20. **Modifiez > des stratégies > FlexConfig**. Te permet pour modifier FlexConfigs, qui sont des commandes supplémentaires et des instructions CLI qui peuvent être déployées vers des périphériques PIX/ASA/FWSM, des Routeurs IOS, et des périphériques du Catalyst 6500/7600.

Modifiez les autorisations d'objets

Le directeur de la sécurité inclut les autorisations suivantes de vue pour des objets :

1. **Modifiez > objectez > des Groupes de serveurs AAA**. Te permet pour visualiser des objets

de Groupe de serveurs AAA. Ces objets sont utilisés dans les stratégies qui exigent des services d'AAA (authentification, autorisation, et comptabilité).

2. **Modifiez > objectez > des serveurs d'AAA**. Te permet pour visualiser des objets de serveur d'AAA. Ces objets représentent les différents serveurs d'AAA qui sont définis en tant qu'élément d'un Groupe de serveurs AAA.
3. **Modifiez > objectez > des listes de contrôle d'accès - Standard/a étendu**. Te permet pour visualiser les objets standard et étendus d'ACL. Des objets étendus d'ACL sont utilisés pour un grand choix de stratégies, telles que NAT et le NAC, et pour établir l'accès VPN. Des objets standard d'ACL sont utilisés pour des stratégies telles que l'OSPF et le SNMP, aussi bien que pour établir l'accès VPN.
4. **Modifiez > objectez > des listes de contrôle d'accès - Web**. Te permet pour visualiser des objets d'ACL de Web. Des objets d'ACL de Web sont utilisés pour exécuter le filtrage selon le contenu dans des stratégies de VPN SSL.
5. **Modifiez > objectez > des** groupes d'utilisateurs **ASA**. Te permet pour visualiser des objets de groupe d'utilisateurs ASA. Ces objets sont configurés sur des dispositifs de sécurité ASA dans l'Easy VPN, l'Accès à distance VPN, et les configurations de VPN SSL.
6. **Modifiez > objectez > des catégories**. Te permet pour visualiser des objets de catégorie. Ces objets vous aident facilement à identifier des règles et des objets dans des tables de règles par l'utilisation de couleur.
7. **Modifiez > objectez > des qualifications**. Te permet pour visualiser les objets de créance. Ces objets sont utilisés en configuration Easy VPN pendant le Fonction IKE Extended Authentication (Xauth).
8. **Modifiez > objectez > FlexConfigs**. Te permet pour visualiser des objets de FlexConfig. Ces objets, qui contiennent des commandes de configuration avec des instructions supplémentaires de langage de script, peuvent être utilisés pour configurer les commandes qui ne sont pas prises en charge par l'interface utilisateur de directeur de la sécurité.
9. **Modifiez > objectez > des propositions d'IKE**. Te permet pour visualiser des objets de proposition d'IKE. Ces objets contiennent les paramètres exigés pour des propositions d'IKE dans des règles VPN d'Accès à distance.
10. **Modifiez > des objets > examinent - Class map - DN**. Te permet pour visualiser des objets de class map de DN. Ces objets apparient le trafic DNS avec des critères spécifiques de sorte que des actions puissent être exécutées sur ce trafic.
11. **Modifiez > des objets > examinent - Class map - FTP**. Te permet pour visualiser des objets de class map de FTP. Ces objets apparient le trafic FTP avec des critères spécifiques de sorte que des actions puissent être exécutées sur ce trafic.
12. **Modifiez > des objets > examinent - Class map - HTTP**. Te permet pour visualiser des objets de class map de HTTP. Ces objets apparient le trafic http avec des critères spécifiques de sorte que des actions puissent être exécutées sur ce trafic.
13. **Modifiez > des objets > examinent - Class map - IM**. Te permet pour visualiser des objets du class map IM. Le trafic de la correspondance IM de ces objets avec des critères spécifiques de sorte que des actions puissent être exécutées sur ce trafic.
14. **Modifiez > des objets > examinent - Class map - SIP**. Te permet pour visualiser des objets de class map de SIP. Ces objets apparient le trafic de SIP avec des critères spécifiques de sorte que des actions puissent être exécutées sur ce trafic.
15. **Modifiez > des objets > examinent - Cartes de stratégie - DN**. Te permet pour visualiser des objets de carte de stratégie de DN. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic DNS.
16. **Modifiez > des objets > examinent - Cartes de stratégie - FTP**. Te permet pour visualiser

des objets de carte de stratégie de FTP. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic FTP.

17. **Modifiez > des objets > examinent - Cartes de stratégie - HTTP (ASA7.1.x/PIX7.1.x/IOS)**. Te permet pour visualiser des objets de carte de stratégie de HTTP créés pour des périphériques ASA/PIX 7.x et des Routeurs IOS. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic http.
18. **Modifiez > des objets > examinent - Cartes de stratégie - HTTP (ASA7.2/PIX7.2)**. Te permet pour visualiser des objets de carte de stratégie de HTTP créés pour des périphériques ASA 7.2/PIX 7.2. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic http.
19. **Modifiez > des objets > examinent - Cartes de stratégie - IM (ASA7.2/PIX7.2)**. Te permet pour visualiser des objets de carte de la stratégie IM créés pour des périphériques ASA 7.2/PIX 7.2. Ces objets sont utilisés pour créer des cartes d'inspection pour IM le trafic.
20. **Modifiez > des objets > examinent - Cartes de stratégie - IM (IOS)**. Te permet pour visualiser des objets de carte de la stratégie IM créés pour des périphériques IOS. Ces objets sont utilisés pour créer des cartes d'inspection pour IM le trafic.
21. **Modifiez > des objets > examinent - Cartes de stratégie - SIP**. Te permet pour visualiser des objets de carte de stratégie de SIP. Ces objets sont utilisés pour créer des cartes d'inspection pour le trafic de SIP.
22. **Modifiez > des objets > examinent - Expressions régulières**. Te permet pour visualiser des objets d'expression régulière. Ces objets représentent les différentes expressions régulières qui sont définies en tant qu'élément d'un groupe d'expression régulière.
23. **Modifiez > des objets > examinent - Groupes d'expressions régulières**. Te permet pour visualiser des objets de groupe d'expression régulière. Ces objets sont utilisés par certains class map et examinent des cartes pour apparier le texte à l'intérieur d'un paquet.
24. **Modifiez > des objets > examinent - Cartes de TCP**. Te permet pour visualiser des objets de carte de TCP. Ces objets personnalisent l'inspection sur l'écoulement de TCP dans les deux directions.
25. **Modifiez > objectez > des rôles d'interface**. Te permet pour visualiser des objets de rôle d'interface. Ces objets définissent nommer les modèles qui peuvent représenter des plusieurs interfaces sur différents types de périphériques. Enable de rôles d'interface vous pour s'appliquer des stratégies aux interfaces spécifiques sur de plusieurs périphériques sans devoir manuellement définir le nom de chaque interface.
26. **Modifiez > objectez > des jeux de transformations d'IPsec**. Te permet pour visualiser des objets de jeu de transformations d'IPsec. Ces objets comportent une combinaison des protocoles de Sécurité, des algorithmes et d'autres configurations qui spécifient exactement comment les données dans le tunnel d'IPsec seront chiffrées et authentifiées.
27. **Modifiez > objectez > des cartes d'attribut de LDAP**. Te permet pour visualiser des objets de carte d'attribut de LDAP. Ces objets sont utilisés pour tracer des noms (définis par l'utilisateur) faits sur commande d'attribut aux noms d'attribut de LDAP de Cisco.
28. **Modifiez > objectez > des réseaux/hôtes**. Vous permet aux objets de View Network/hôte. Ces objets sont les collections logiques d'adresses IP qui représentent des réseaux, des hôtes, ou chacun des deux. Les objets de réseau/hôte te permettent de définir des stratégies sans spécifier chaque réseau ou de les héberger individuellement.
29. **Modifiez > objectez > des inscriptions de PKI**. Te permet pour visualiser des objets d'inscription de PKI. Ces objets définissent les serveurs de l'autorité de certification (CA) qui fonctionnent dans une infrastructure de clé publique.
30. **Modifiez > objectez > des listes de transmission du port**. Te permet pour visualiser des

objets de liste de transmission du port. Ces objets définissent les mappages des numéros de port sur un client distant à l'adresse IP de l'application et mettent en communication derrière une passerelle de VPN SSL.

31. **Modifiez > objectez > des configurations de Secure Desktop**. Te permet pour visualiser des objets de configuration de Secure Desktop. Ces objets sont des composants réutilisables et Désignés qui peuvent être mis en référence par des stratégies de VPN SSL pour fournir le moyen fiable d'éliminer tous les suivis des données sensibles qui sont partagées pour la durée d'une session de VPN SSL.
32. **Modifiez > objectez > des services - Listes des ports**. Te permet pour visualiser des objets de liste des ports. Ces objets, qui contiennent un ou plusieurs nombres de plages de port, sont utilisés pour rationaliser le processus de créer des objets de service.
33. **Modifiez > objectez > des services/groupes de service.** Te permet pour visualiser le service et le groupe de service objecte. Ces objets sont les mappages définis du protocole et mettent en communication les définitions qui décrivent des services réseau utilisés par des stratégies, telles que le Kerberos, le SSH, et le POP3.
34. **Modifiez > objectez > simple se connectent des serveurs.** Te permet pour visualiser simple se connectent des objets de serveur. L'ouverture de session simple (SSO) permet des utilisateurs de VPN SSL d'écrire un nom d'utilisateur et mot de passe une fois et de pouvoir accéder à des services et des web server protégés par multiple.
35. **Modifiez > objectez > des moniteurs de SLA**. Te permet pour visualiser des objets de moniteur de SLA. Ces objets sont utilisés par des appliances de Sécurité PIX/ASA exécutant la version 7.2 ou ultérieures pour exécuter le cheminement d'artère. Cette caractéristique fournit une méthode pour dépister la Disponibilité d'une route primaire et pour installer une route de secours si la route primaire échoue.
36. **Modifiez > objectez > des personnalisations de VPN SSL**. Te permet pour visualiser des objets de personnalisation de VPN SSL. Ces objets définissent comment changer l'apparence des pages de VPN SSL qui sont affichées aux utilisateurs, tels que la procédure de connexion/déconnexion et les pages d'accueil.
37. **Modifiez > objectez > des passerelles de VPN SSL**. Te permet pour visualiser des objets de passerelle de VPN SSL. Ces objets définissent les paramètres qui permettent à la passerelle d'être utilisée comme proxy pour des connexions aux ressources protégées dans votre VPN SSL.
38. **Modifiez > objectez > des objets de style**. Te permet pour visualiser des objets de style. Ces objets vous permettent de configurer des éléments de style, tels que des caractéristiques de la police et des couleurs, pour personnaliser l'apparence de la page de VPN SSL qui paraît aux utilisateurs de VPN SSL quand ils se connectent aux dispositifs de sécurité.
39. **Modifiez > objectez > des objets des textes**. Te permet pour visualiser des objets des textes de libre-forme. Ces objets comportent une paire de nom et de valeur, où la valeur peut être une chaîne simple, une liste de chaînes, ou une table des chaînes.
40. **Modifiez > objectez > des plages de temps.** Te permet pour visualiser des objets de plage de temps. Ces objets sont utilisés en créant des règles basées sur temps d'ACLs et d'inspection. Ils sont également utilisés en définissant des groupes d'utilisateurs ASA pour limiter l'accès VPN aux heures précises pendant la semaine.
41. **Modifiez > objectez > la circulation**. Te permet pour visualiser des objets de la circulation. Ces objets définissent la circulation spécifique à l'usage des périphériques PIX 7.x/ASA 7.x.
42. **Modifiez > objectez > des listes URL**. Te permet pour visualiser des objets de liste URL. Ces objets définissent l'URLs qui sont affichés sur la page du portail après une procédure

de connexion réussie. Ceci permet à des utilisateurs d'accéder aux ressources disponibles sur des sites Web de VPN SSL en fonctionnant dans le mode d'accès sans client.

43. **Modifiez > objectez > des groupes d'utilisateurs**. Te permet pour visualiser des objets de groupe d'utilisateurs. Ces objets définissent des groupes de clients distants qui sont utilisés dans des topologies d'Easy VPN, l'Accès à distance VPN, et le VPN SSL
44. **Modifiez > objectez > des listes de serveur WINS**. Te permet pour visualiser des objets de liste de serveur WINS. Ces objets représentent les serveurs WINS, qui sont utilisés par VPN SSL pour accéder à ou fichiers partagés sur des systèmes distants.
45. **Modifiez > objectez > interne - Règles de DN.** Te permet pour visualiser les règles de DN utilisées par des stratégies de DN. C'est un objet interne utilisé par le directeur de la sécurité qui n'apparaît pas dans le gestionnaire d'objet de stratégie.
46. **Modifiez > objectez > des mises à jour de client interne**. C'est un objet interne exigé par des objets de groupe d'utilisateurs qui n'apparaît pas dans le gestionnaire d'objet de stratégie.
47. **Modifiez > objectez > interne - ACE standard**. C'est un objet interne pour les entrées de contrôle d'accès standard, qui sont utilisées par des objets d'ACL.
48. **Modifiez > objectez > interne - ACE étendu**. C'est un objet interne pour les entrées de contrôle d'accès étendues, qui sont utilisées par des objets d'ACL.

Supplémentaire modifiez les autorisations

Le directeur de la sécurité inclut le supplémentaire modifient des autorisations comme affichées :

1. **Modifiez > admin**. Te permet pour modifier des paramètres administratifs de directeur de la sécurité.
2. **Modifiez > Config Archive**. Te permet pour modifier la configuration de périphérique dans les archives de configuration. En outre, il te permet pour ajouter des configurations aux archives et pour personnaliser l'outil d'archives de configuration.
3. **Modifiez > des périphériques**. Te permet pour ajouter et supprimer des périphériques, aussi bien que modifie des propriétés et des attributs de périphérique. Pour découvrir les stratégies sur le périphérique étant ajouté, vous devez également activer l'autorisation d'importation. En outre, si vous activez l'autorisation de modifier > de périphériques, assurez-vous que vous activez également l'autorisation d'assigner > de stratégies > d'interfaces.
4. **Modifiez > hiérarchie**. Te permet pour modifier des groupes de périphériques.
5. **Modifiez > topologie**. Te permet pour modifier des cartes dans la vue de carte.

Assignez les autorisations

Le directeur de la sécurité inclut les autorisations d'affectation de stratégie comme affichées :

1. **Assignez > des stratégies > Pare-feu**. Te permet pour assigner des stratégies de service de Pare-feu (situées dans le sélecteur de stratégie sous le Pare-feu) aux périphériques PIX/ASA/FWSM, aux Routeurs IOS, et aux périphériques du Catalyst 6500/7600. Les exemples des stratégies de service de Pare-feu incluent des règles d'accès, des règles d'AAA, et des règles d'inspection.
2. **Assignez > les stratégies > le système de prévention des intrusions**. Te permet pour assigner des stratégies IPS (situées dans le sélecteur de stratégie sous l'IPS), y compris des stratégies pour l'exécution IPS sur des Routeurs IOS.
3. **Assignez > des stratégies > image**. Cette autorisation n'est pas actuellement utilisée par le

directeur de la sécurité.

4. **Assignez > des stratégies > NAT**. Te permet pour assigner des stratégies de traduction d'adresses réseau aux périphériques PIX/ASA/FWSM et aux Routeurs IOS. Les exemples des stratégies NAT incluent des règles statiques et des règles dynamiques.
5. **Assignez > les stratégies > le site à site VPN**. Te permet pour assigner des règles VPN de site à site aux périphériques PIX/ASA/FWSM, aux Routeurs IOS, et aux périphériques du Catalyst 6500/7600. Les exemples des règles VPN de site à site incluent des propositions d'IKE, des propositions d'IPsec, et des clés pré-partagées.
6. **Assignez > des stratégies > l'Accès à distance VPN**. Te permet pour assigner des règles VPN d'Accès à distance aux périphériques PIX/ASA/FWSM, aux Routeurs IOS, et aux périphériques du Catalyst 6500/7600. Les exemples des règles VPN d'Accès à distance incluent des propositions d'IKE, des propositions d'IPsec, et des stratégies de PKI.
7. **Assignez > des stratégies > VPN SSL**. Te permet pour assigner des stratégies de VPN SSL aux périphériques PIX/ASA/FWSM et aux Routeurs IOS, tels que l'assistant de VPN SSL.
8. **Assignez > des stratégies > des interfaces**. Te permet pour assigner des stratégies d'interface (situées dans le sélecteur de stratégie sous des interfaces) aux périphériques PIX/ASA/FWSM, aux Routeurs IOS, et aux périphériques du Catalyst 6500/7600 :Sur des périphériques PIX/ASA/FWSM, cette autorisation couvre des ports et des paramètres d'interface de matériel.Sur des Routeurs IOS, cette autorisation couvre les paramètres d'interface de base et avancés, aussi bien que d'autres stratégies liées à l'interface, telles que le DSL, le PVC, le PPP, et les stratégies de numéroteur.Sur des périphériques du Catalyst 6500/7600, cette autorisation couvre des interfaces et des configurations VLAN.
9. **Assignez > des stratégies > en jetant un pont sur**. Te permet pour assigner des stratégies de table ARP (situées dans le sélecteur de stratégie sous la plate-forme > jetant un pont sur) aux périphériques PIX/ASA/FWSM.
10. **Assignez > les stratégies > la gestion de périphérique**. Te permet pour assigner des stratégies de gestion de périphérique (situées dans le sélecteur de stratégie sous l'admin de plate-forme > de périphérique) aux périphériques PIX/ASA/FWSM, aux Routeurs IOS, et aux périphériques du Catalyst 6500/7600 :Sur des périphériques PIX/ASA/FWSM, les exemples incluent l'accès au périphérique maintient l'ordre, des stratégies d'accès de serveur, et des stratégies de Basculement.Sur des Routeurs IOS, les exemples incluent l'accès au périphérique (accès à la ligne y compris) maintient l'ordre, des stratégies d'accès de serveur, AAA, et sécurise le ravitaillement de périphérique.Sur des capteurs IPS, cette autorisation couvre des stratégies d'accès au périphérique et des stratégies d'accès de serveur.Sur des périphériques du Catalyst 6500/7600, cette autorisation couvre des configurations IDSM et des Listes d'accès VLAN.
11. **Assignez > des stratégies > identité**. Te permet pour assigner des stratégies d'identité (situées dans le sélecteur de stratégie sous la plate-forme > l'identité) aux routeurs Cisco IOS, y compris le 802.1x et les stratégies de Contrôle d'admission au réseau (NAC).
12. **Assignez > des stratégies > en se connectant**. Te permet pour assigner se connecter des stratégies (situées dans le sélecteur de stratégie sous la plate-forme > se connectant) aux périphériques PIX/ASA/FWSM et aux Routeurs IOS. Les exemples de se connecter des stratégies incluent se connecter l'installation, la configuration du serveur, et les stratégies de serveur de Syslog.
13. **Assignez > des stratégies > Multidiffusion**. Te permet pour assigner des stratégies de Multidiffusion (situées dans le sélecteur de stratégie sous la plate-forme > la Multidiffusion) aux périphériques PIX/ASA/FWSM. Les exemples des stratégies de Multidiffusion incluent le routage de Multidiffusion et les stratégies IGMP.

14. **Assignez > des stratégies > QoS**. Te permet pour assigner des stratégies QoS (situées dans le sélecteur de stratégie sous la plate-forme > la qualité de service) aux routeurs Cisco IOS.
15. **Assignez > des stratégies > routage**. Te permet pour assigner des stratégies de routage (situées dans le sélecteur de stratégie sous la plate-forme > le routage) aux périphériques PIX/ASA/FWSM et aux Routeurs IOS. Les exemples des stratégies de routage incluent l'OSPF, le RIP, et les stratégies statiques de routage.
16. **Assignez > des stratégies > Sécurité**. Te permet pour assigner des stratégies de sécurité (situées dans le sélecteur de stratégie sous la plate-forme > la Sécurité) aux périphériques PIX/ASA/FWSM. Les stratégies de sécurité incluent l'anti-mystification, le fragment, et les configurations de délai d'attente.
17. **Assignez > des règles de stratégies > de stratégie de service**. Te permet pour assigner des stratégies de règle de stratégie de service (situées dans le sélecteur de stratégie dans le cadre de la stratégie de plate-forme > de service ordonne) aux périphériques PIX 7.x/ASA. Les exemples incluent des files d'attente prioritaire et IPS, QoS, et des règles de connexion.
18. **Assignez > des stratégies > des préférences de l'utilisateur**. Te permet pour assigner la stratégie de déploiement (située dans le sélecteur de stratégie sous la plate-forme > les préférences de l'utilisateur) aux périphériques PIX/ASA/FWSM. Cette stratégie contient une option pour effacer toutes les traductions NAT sur le déploiement.
19. **Assignez > les stratégies > le périphérique virtuel**. Te permet pour assigner des stratégies virtuelles de capteur aux périphériques IPS. Employez cette stratégie pour créer les capteurs virtuels.
20. **Assignez > des stratégies > FlexConfig**. Te permet pour assigner FlexConfigs, qui sont des commandes supplémentaires et des instructions CLI qui peuvent être déployées vers des périphériques PIX/ASA/FWSM, des Routeurs IOS, et des périphériques du Catalyst 6500/7600.

Remarque: Quand vous spécifiez assignez les autorisations, s'assurent que vous avez sélectionné les autorisations correspondantes de vue aussi bien.

Approuvez les autorisations

Le directeur de la sécurité fournit les autorisations d'approbation comme affichées :

1. **Approuvez > CLI**. Te permet pour approuver les modifications de commande CLI contenues dans un travail de déploiement.
2. **Approuvez > stratégie**. Te permet pour approuver les modifications de configuration contenues dans les stratégies qui ont été configurées dans une activité de processus.

Compréhension des rôles de CiscoWorks

Quand des utilisateurs sont créés dans des services communs de CiscoWorks, ils sont assignés un ou plusieurs rôles. Les autorisations associées avec chaque rôle déterminent les exécutions que chaque utilisateur est autorisé à exécuter dans le directeur de la sécurité.

Les thèmes suivants décrivent des rôles de CiscoWorks :

- Rôles communs de par défaut de services de CiscoWorks

- Assigner des rôles aux utilisateurs dans des services de terrain communal de CiscoWorks

Rôles communs de par défaut de services de CiscoWorks

Les services communs de CiscoWorks contiennent les rôles par défaut suivants :

1. **Centre d'assistance** — Les utilisateurs de centre d'assistance peuvent visualiser (mais ne pas modifier) des périphériques, des stratégies, des objets, et des cartes de topologie.
2. **Opérateur réseau** — En plus des autorisations de vue, les opérateurs réseau peuvent visualiser des commandes CLI et des paramètres administratifs de directeur de la sécurité. Les opérateurs réseau peuvent également modifier les commandes d'archives et de question de configuration (telles que le ping) aux périphériques.
3. **Approbateur** — En plus des autorisations de vue, les approbateurs peuvent approuver ou rejeter les travaux de déploiement. Ils ne peuvent pas exécuter le déploiement.
4. **Administrateur réseau** — Les administrateurs réseau ont le point de vue complet et modifient des autorisations, excepté modifier des paramètres administratifs. Ils peuvent découvrir des périphériques et les stratégies configurées sur ces périphériques, assigner des stratégies aux périphériques, et des commandes de question aux périphériques. Les administrateurs réseau ne peuvent pas approuver des activités ou des travaux de déploiement ; cependant, ils peuvent déployer les travaux qui ont été approuvés par d'autres.
5. **Administrateur système** — Les administrateurs système ont accès complet à toutes les autorisations de directeur de la sécurité, y compris la modification, l'affectation de stratégie, l'approbation d'activité et de travail, la détection, le déploiement, et fourniture des commandes aux périphériques.

Remarque: Les rôles supplémentaires, tels que des données d'exportation, pourraient être en commun des services affichés si des applications supplémentaires sont installées sur le serveur. Le rôle de données d'exportation est pour des développeurs tiers et n'est pas utilisé par le directeur de la sécurité.

Conseil : Bien que vous ne puissiez pas changer la définition des rôles de CiscoWorks, vous pouvez définir quels rôles sont assignés à chaque utilisateur. Le pour en savoir plus, voient assigner des rôles aux utilisateurs dans des services de terrain communal de CiscoWorks.

Assigner des rôles aux utilisateurs dans des services de terrain communal de CiscoWorks

Les services communs de CiscoWorks te permettent de définir quels rôles sont assignés à chaque utilisateur. En changeant la définition de rôle pour un utilisateur, vous changez les types d'exécutions que cet utilisateur est autorisé exécutent dans le directeur de la sécurité. Par exemple, si vous assignez le rôle de centre d'assistance, l'utilisateur est limité pour visualiser des exécutions et ne peut modifier aucune données. Cependant, si vous assignez le rôle d'opérateur réseau, l'utilisateur peut également modifier les archives de configuration. Vous pouvez assigner de plusieurs rôles à chaque utilisateur.

Remarque: Vous devez redémarrer le directeur de la sécurité après avoir apporté des modifications aux autorisations utilisateur.

Procédure :

1. En commun les services, **serveur** choisi **> Sécurité**, sélectionnent alors la **Gestion > l'utilisateur local de confiance de serveur unique installés du** TOC.**Conseil :** Pour atteindre la page d'installation d'utilisateur local du directeur de la sécurité, les outils choisis > la gestion de directeur de la sécurité > le degré de sécurité de serveur, cliquent sur alors l'installation d'utilisateur local.
2. Sélectionnez la case à côté d'un utilisateur existant, puis cliquez sur Edit.
3. Àla page des informations utilisateur, sélectionnez les rôles pour assigner à cet utilisateur en cliquant sur les cases.Pour plus d'informations sur chaque rôle, voir les rôles communs de par défaut de services de CiscoWorks.
4. Cliquez sur OK pour sauvegarder vos modifications.
5. Directeur de la sécurité de reprise.

Compréhension des rôles de Cisco Secure ACS

Le Cisco Secure ACS fournit la meilleure flexibilité pour gérer des autorisations de directeur de la sécurité que font les CiscoWorks parce qu'elle prend en charge les rôles spécifiques à l'application que vous pouvez configurer. Chaque rôle se compose d'un ensemble d'autorisations qui déterminent le niveau de l'autorisation aux tâches de directeur de la sécurité. Dans le Cisco Secure ACS, vous assignez un rôle à chaque groupe d'utilisateurs (et sur option, aux utilisateurs individuels aussi bien), qui permet à chaque utilisateur dans ce groupe d'exécuter les exécutions a autorisé par les autorisations définies pour ce rôle.

En outre, vous pouvez assigner ces rôles aux groupes de périphériques de Cisco Secure ACS, permettant des autorisations d'être différencié sur différents ensembles de périphériques.

Remarque: Les groupes de périphériques de Cisco Secure ACS sont indépendant des groupes de périphériques de directeur de la sécurité.

Les thèmes suivants décrivent des rôles de Cisco Secure ACS :

- Rôles par défaut de Cisco Secure ACS
- Personnaliser des rôles de Cisco Secure ACS

Rôles par défaut de Cisco Secure ACS

Le Cisco Secure ACS inclut les mêmes rôles que des CiscoWorks (voir compréhension des rôles de CiscoWorks), plus ces rôles supplémentaires :

1. **Approbateur de Sécurité** — Les approbateurs de Sécurité peuvent visualiser (mais ne pas modifier) des périphériques, des stratégies, des objets, des cartes, des commandes CLI, et des paramètres administratifs. 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 le travail de déploiement, ni peuvent ils exécuter le déploiement.
2. **Administrateur de Sécurité** — En plus de avoir des autorisations de vue, les administrateurs de Sécurité peuvent modifier des périphériques, des groupes de périphériques, des stratégies, des objets, et des cartes de topologie. Ils peuvent également assigner des stratégies aux périphériques et aux topologies VPN, et exécutent la détection pour importer de nouveaux périphériques dans le système.
3. **Administrateur réseau** — En plus des autorisations de vue, les administrateurs réseau

peuvent modifier les archives de configuration, exécuter le déploiement, et les commandes de question aux périphériques.

Remarque: Les autorisations contenues dans le rôle de l'administrateur réseau de Cisco Secure ACS sont différentes de ceux contenues dans le rôle de l'administrateur réseau de CiscoWorks. Le pour en savoir plus, voient compréhension des rôles de CiscoWorks.

Àla différence des CiscoWorks, le Cisco Secure ACS te permet de personnaliser les autorisations associées avec chaque rôle de directeur de la sécurité. Pour plus d'informations sur modifier les rôles par défaut, voyez personnaliser des rôles de Cisco Secure ACS.

Remarque: Le Cisco Secure ACS 3.3 ou plus tard doit être installé pour l'autorisation de directeur de la sécurité.

Personnaliser des rôles de Cisco Secure ACS

Le Cisco Secure ACS te permet de modifier les autorisations associées avec chaque rôle de directeur de la sécurité. Vous pouvez également personnaliser le Cisco Secure ACS en créant des rôles de l'utilisateur spécialisés avec les autorisations qui sont visées aux tâches particulières de directeur de la sécurité.

Remarque: Vous devez redémarrer le directeur de la sécurité après avoir apporté des modifications aux autorisations utilisateur.

Procédure :

1. Dans le Cisco Secure ACS, le clic **a partagé des composants de profil** sur la barre de navigation.
2. **Cisco Security Manager de** clic à la page partagée de composants. Les rôles qui sont configurés pour le directeur de la sécurité sont affichés.
3. Faites un de ce qui suit :Pour créer un rôle, cliquez sur Add. Passez à l'étape 4.Pour modifier un rôle existant, cliquez sur le rôle. Passez à l'étape 5.
4. Écrivez un nom pour le rôle et, sur option, une description.
5. Sélectionnez et désélectionnez les cases dans l'arborescence d'autorisations pour définir les autorisations pour ce rôleSélectionner la case pour un branchement de l'arborescence sélectionne toutes les autorisations dans ce branchement. Par exemple, sélectionner **assignent** sélectionne toutes les autorisations d'assigner.Pour une liste complète d'autorisations de directeur de la sécurité, voir les autorisations de directeur de la sécurité.**Remarque:** Quand vous sélectionnez modifiez, approuvez, assignez, importez, contrôlez ou déployez les autorisations, vous doit également sélectionner les autorisations correspondantes de vue ; autrement, le directeur de la sécurité ne fonctionnera pas correctement.
6. Cliquez sur **Submit** pour enregistrer les modifications.
7. Directeur de la sécurité de reprise.

Associations par défaut entre les autorisations et les rôles dans le directeur de la sécurité

Cette table affiche comment des autorisations de directeur de la sécurité sont associées avec des rôles de services de terrain communal de CiscoWorks et les rôles par défaut dans le Cisco Secure

ACS.

Autorisations	Rôles							
	Admin de système	Admin de Sécurité (ACS)	Approbateur de Sécurité (ACS)	Admin de réseau (on de entretenue)	Admin de réseau (ACS)	Approbateur	Opérateur réseau	Centre d'assistance
Autorisations de vue								
Périphérique de vue	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Stratégie de vue	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Vues standard	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Topologie de vue	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Vue CLI	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non
Admin de vue	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non
Config Archive de vue	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Oui
Gestionnaires de périphériques de vue	Oui	Oui	Oui	Oui	Oui	Oui	Oui	Non
Modifiez les autorisations								
Modifiez le périphérique	Oui	Oui	Non	Oui	Non	Non	Non	Non
Modifiez la hiérarchie	Oui	Oui	Non	Oui	Non	Non	Non	Non
Modifiez la stratégie	Oui	Oui	Non	Oui	Non	Non	Non	Non
Modifiez l'image	Oui	Oui	Non	Oui	Non	Non	Non	Non
Modifiez les objets	Oui	Oui	Non	Oui	Non	Non	Non	Non
Modifiez la topologie	Oui	Oui	Non	Oui	Non	Non	Non	Non
Modifiez	Oui	No	No	No	No	No	No	Non

l'admin		n	n	n	n	n	n	
Modifiez le Config Archive	Oui	Oui	Non	Oui	Oui	Non	Oui	Non
Autorisations supplémentaires								
Assignez la stratégie	Oui	Oui	Non	Oui	Non	Non	Non	Non
Approuvez la stratégie	Oui	Non	Oui	Non	Non	Non	Non	Non
Approuvez le CLI	Oui	Non	Non	Non	Non	Oui	Non	Non
Le découvrez (importation)	Oui	Oui	Non	Oui	Non	Non	Non	Non
Déployez-vous	Oui	Non	Non	Oui	Oui	Non	Non	Non
Contrôle	Oui	Non	Non	Oui	Oui	Non	Oui	Non
Soumettez	Oui	Oui	Non	Oui	Non	Non	Non	Non

Informations connexes

- Page de support de Cisco Security Manager
- Support et documentation techniques - Cisco Systems