Configuration du système

Ce chapitre explique comment configurer les paramètres de configuration du système sur le Cisco Secure Firewall Management Center.

Exigences et conditions préalables pour la configuration du système

Prise en charge des modèles

Centre de gestion

Domaines pris en charge

Global

Rôles utilisateur

Admin

Gérer la configuration du système Cisco Secure Firewall Management Center

La configuration du système identifie les paramètres de base pour centre de gestion.

Procédure

Étape 1 Choisissez **System** (⚙) > **Configuration**.

Étape 2 Utilisez le panneau de navigation pour choisir les configurations à modifier.

Préférences liées au contrôle d'accès

Configurer les préférence de contrôle d'accès sur **System** (⚙) > **Configuration** > **Préférences de contrôle d'accès**.

Exiger des commentaires sur les modifications de règles

Vous pouvez suivre les modifications apportées aux règles de contrôle d'accès en autorisant (ou en demandant) aux utilisateurs de les commenter lorsqu'ils les enregistrent. Cela vous permet d'évaluer rapidement pourquoi les politiques essentielles d'un déploiement ont été modifiées. Par défaut, cette fonction est désactivée.

Rapprochement des changements

Pour surveiller les modifications apportées par les utilisateurs et vous assurer qu'elles respectent la norme préconisée par votre organisation, vous pouvez configurer le système pour envoyer, par courriel, un rapport détaillé des modifications effectuées au cours des dernières 24 heures. Chaque fois qu'un utilisateur enregistre des modifications à la configuration du système, un instantané des modifications est pris. Le rapport de rapprochement des modifications combine les informations de ces instantanés pour présenter un résumé clair des récentes modifications apportées au système.

L'exemple de graphique suivant présente la section Utilisateur d'un exemple de rapport de rapprochement des modifications et répertorie la valeur précédente pour chaque configuration et la valeur après les modifications. Lorsque les utilisateurs apportent plusieurs modifications à la même configuration, le rapport répertorie des résumés de chaque modification par ordre chronologique, en commençant par la plus récente.

Vous pouvez afficher les modifications apportées au cours des 24 heures précédentes.

Configuration du rapprochement des changements

Procédure

Étape 1 Choisissez **System** (⚙) > **Configuration**.

Étape 2 Cliquez sur **Change Reconciliations** (Rapprochements des changements)

Étape 3 Cochez la case **Enable** (activer).

Étape 4 Dans les listes déroulantes **Time to run**, choisissez l'heure à laquelle vous souhaitez que le système envoie le rapport de rapprochement des modifications.

Étape 5 Saisissez les adresses courriel dans le champ **Email to**.

Astuces Une fois que vous avez ajouté les adresses courriel, cliquez sur **Renvoyer le dernier rapport** pour envoyer aux destinataires une copie du plus récent rapport de rapprochement des modifications.

Étape 6 Si vous souhaitez inclure les modifications de politique, cochez la case **Inclure la configuration de politique**.

Étape 7 Si vous souhaitez inclure toutes les modifications effectuées au cours des dernières 24 heures, cochez la case **Show Full Change Historique** (afficher l'historique des modifications complet).

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

Sujets connexes

Utilisation du journal d'audit pour examiner les modifications

Options de rapprochement des changements

L'option **Inclure la configuration de politique** contrôle si le système inclut les enregistrements des modifications de politique dans le rapport de rapprochement des modifications. Cela comprend les modifications apportées aux politiques de contrôle d'accès, de prévention des intrusions, du système, d'intégrité et de découverte du réseau. Si vous ne sélectionnez pas cette option, le rapport n'affichera pas les modifications apportées aux politiques. Cette option est disponible sur les centre de gestion uniquement.

L'option **Afficher l'historique complet des modifications** contrôle si le système inclut les enregistrements de tous les changements effectués au cours des dernières 24 heures dans le rapport de rapprochement des modifications. Si vous ne sélectionnez pas cette option, le rapport comprend uniquement une vue consolidée des changements pour chaque catégorie.

Remarque Le rapport de rapprochement des modifications n'inclut pas les modifications apportées aux interfaces défense contre les menaces et aux paramètres de routage.

Avis courriel

Vous ne pouvez pas configurer un hôte de messagerie. L'hôte de relais de messagerie est codé en dur pour être utilisé à partir d'un hôte statique. Il est défini sur email-smtp.us-west-2.amazonaws.com avec autorisation. Pour les notifications, l'expéditeur du courriel est cdo-alert@cisco.com

Préférences pour les politiques d'intrusion

Vous pouvez configurer le système pour suivre les modifications liées aux politiques à l'aide de la fonctionnalité de commentaires lorsque les utilisateurs modifient les politiques de prévention des intrusions. Une fois les commentaires de modification de politique activés, les administrateurs peuvent évaluer rapidement la raison de la modification des politiques essentielles d'un déploiement.

Si vous activez les commentaires sur les modifications de politique, vous pouvez rendre le commentaire facultatif ou obligatoire. Le système invite l'utilisateur à ajouter un commentaire lorsque chaque nouvelle modification de politique est enregistrée.

Vous pouvez également faire consigner les modifications apportées aux politiques de prévention des intrusions dans le journal d'audit.

Pour recevoir des notifications des modifications apportées à des règles définies par le système *remplacées* lors des mises à jour des LSP, assurez-vous que la case **Retain user overrides for deleted Snort 3 rules** (Conserver les remplacements de l'utilisateur pour les règles du Snort 3 supprimées) est cochée. Par défaut système, cette case est cochée. Lorsque cette case est cochée, le système conserve les remplacements de règles dans les nouvelles règles de remplacement qui sont ajoutées lors de la mise à jour du LSP. Les notifications s'affichent sous l'onglet **Tasks** (Tâches), sous l'icône **Notifications** située à côté de **Cog** (Rouage) ( ).

Préférences pour les politiques d'analyse de réseau

Vous pouvez configurer le système pour suivre les modifications liées aux politiques à l'aide de la fonctionnalité de commentaires lorsque les utilisateurs modifient les politiques d'analyse de réseau. Une fois les commentaires de modification de politique activés, les administrateurs peuvent évaluer rapidement la raison de la modification des politiques essentielles d'un déploiement.

Si vous activez les commentaires sur les modifications de politique, vous pouvez rendre le commentaire facultatif ou obligatoire. Le système invite l'utilisateur à ajouter un commentaire lorsque chaque nouvelle modification de politique est enregistrée.

Si vous le souhaitez, vous pouvez écrire les modifications apportées aux politiques d'analyse de réseau dans le journal d'audit.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.