Configurer une règle d'autorisation sur un système Cisco Firepower

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Configuration](#)
[Créer une règle d'accès](#)
[Activer une règle d'accès](#)
[Vérification](#)
[Dépannage](#)

Introduction

Ce document décrit une règle de passe, comment la créer et comment l'activer dans une stratégie d'intrusion.

Vous pouvez créer des règles de passage afin d'empêcher les paquets qui répondent aux critères définis dans la règle de passage de déclencher la règle d'alerte dans des situations spécifiques, plutôt que de désactiver la règle d'alerte. Par défaut, les règles d'émission remplacent les règles d'alerte. Un système Firepower compare les paquets aux conditions spécifiées dans chaque règle et, si les données de paquet correspondent à toutes les conditions spécifiées dans une règle, la règle se déclenche. Si une règle est une règle d'alerte, elle génère un événement d'intrusion. S'il s'agit d'une règle de passe, elle ignore le trafic.

Par exemple, vous pouvez souhaiter qu'une règle recherche les tentatives de connexion à un serveur FTP lorsque l'utilisateur “ anonyme ” rester actif. Cependant, si votre réseau dispose d'un ou plusieurs serveurs FTP anonymes légitimes, vous pouvez écrire et activer une règle de passe qui spécifie que, pour ces serveurs spécifiques, les utilisateurs anonymes ne déclenchent pas la règle d'origine.

> **Attention** : Lorsqu'une règle d'origine sur laquelle la règle d'passe est basée reçoit une révision, la règle d'passe n'est pas automatiquement mise à jour. Par conséquent, les règles de passage peuvent être difficiles à maintenir.

> **Note**: Si vous activez la fonction Suppression pour une règle, elle supprime les notifications d'événements pour cette règle. Cependant, la règle est toujours évaluée. Par exemple, si vous supprimez une règle de rejet, les paquets qui correspondent à la règle sont supprimés en silence.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

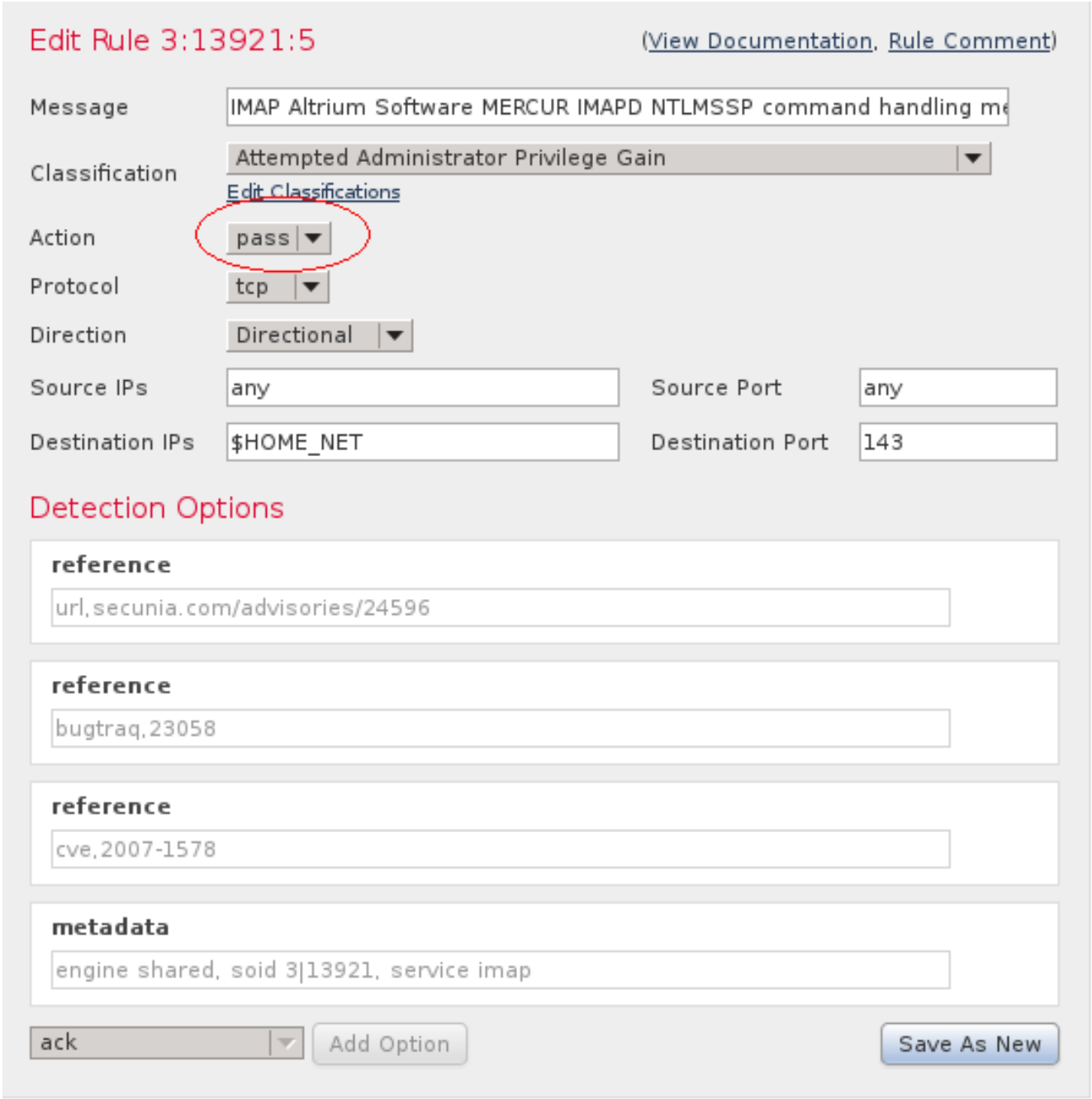
Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

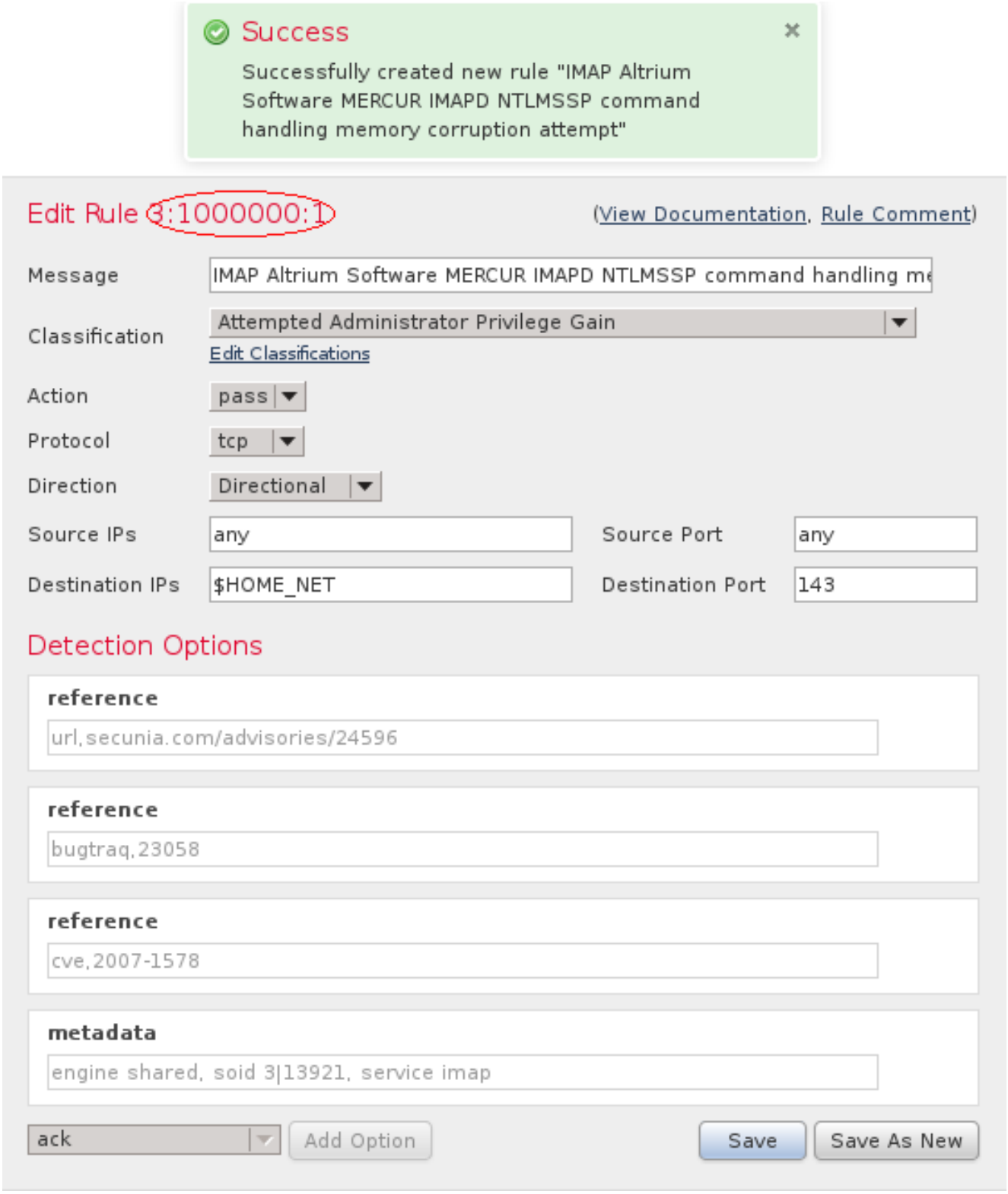
Configuration

Créer une règle d'accès

1. Accédez à **Objets > Règles d'intrusion**. La liste des catégories de règles s'affiche.
2. Recherchez la catégorie de règle associée à la règle à filtrer. Utilisez l'icône fléchée pour développer la catégorie de règle à partir des listes de catégories et trouver la règle pour laquelle vous voulez créer une règle d'acceptation. Vous pouvez également utiliser la zone de recherche des règles.
3. Une fois que vous avez trouvé la règle souhaitée, cliquez sur l'icône représentant un crayon en regard de celle-ci afin de modifier la règle.
4. Lorsque vous modifiez une règle, procédez comme suit : Cliquez sur le bouton **Modifier** correspondant à la règle.Dans la liste déroulante Action, sélectionnez **passer**.Modifiez le champ IP source et le champ IP de destination pour les hôtes ou les réseaux sur lesquels la règle ne doit pas être signalée.Cliquez sur **Enregistrer comme nouveau**.



5. Notez le numéro d'ID de la nouvelle règle. Par exemple, 1000000.



Activer une règle d'accès

Vous devez activer votre nouvelle règle dans la stratégie d'intrusion appropriée afin de transmettre le trafic sur les adresses source ou de destination que vous avez spécifiées. Suivez ces étapes afin d'activer une règle d'autorisation :

1. Modifiez la stratégie d'intrusion active : Accédez à **Politiques > Contrôle d'accès > Intrusion**.Cliquez sur **Modifier** en regard de la stratégie d'intrusion active.
2. Ajouter la nouvelle règle à la liste des règles : Cliquez sur **Règles** dans le volet de gauche.Saisissez l'ID de règle que vous avez noté précédemment dans la zone de

filtre.Cochez la case Règles et modifiez l'état de la règle pour **générer des événements**.Cliquez sur **Informations de stratégie** dans le volet de gauche. Cliquez sur **Valider les modifications**.

3. Cliquez sur **Déployer** afin de déployer les modifications sur le périphérique.

Vérification

Vous devez surveiller les nouveaux événements pendant un certain temps afin de vous assurer qu'aucun événement n'est généré pour cette règle spécifique pour l'adresse IP source ou de destination définie.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.