Configurez une règle de passage sur un système de Cisco FirePOWER

Contenu

Introduction

Ce document décrit une règle de passage, 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 à des critères définis dans la règle de passage de déclencher la règle vigilante dans des situations spécifiques, plutôt que désactivant la règle vigilante. Par défaut, passez les règles d'alerte de priorité de règles. Un système de FirePOWER compare des paquets contre les conditions spécifiées dans chaque règle et, si les données de paquets apparient toutes les conditions spécifiées dans une règle, les déclencheurs de règle. Si une règle est une règle vigilante, elle génère un événement d'intrusion. Si c'est une règle de passage, il ignore le trafic.

Par exemple, vous pourriez vouloir une règle qui recherche des tentatives de se connecter dans un ftp server en tant qu'utilisateur « anonyme » pour rester active. Cependant, si votre réseau a un ou plusieurs serveurs légitimes de FTP anonyme, vous pourriez écrire et lancer une règle de passage qui spécifie que, pour ces serveurs spécifiques, les utilisateurs anonymes ne déclenchent pas la règle d'origine.

> **Attention** : Quand une règle d'origine que la règle de passage est basé en fonction reçoit une révision, la règle de passage n'est pas automatiquement mise à jour. Par conséquent, il pourrait être difficiles mettre à jour des règles de passage.

> **Note**: Si vous activez la caractéristique de suppression pour une règle, elle supprime les notifications d'événement pour cette règle. Cependant la règle est est évaluée toujours. Par exemple, si vous supprimez une règle de baisse, des paquets qui apparient la règle sont silencieusement lâchés.

Conditions préalables

Exigences

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

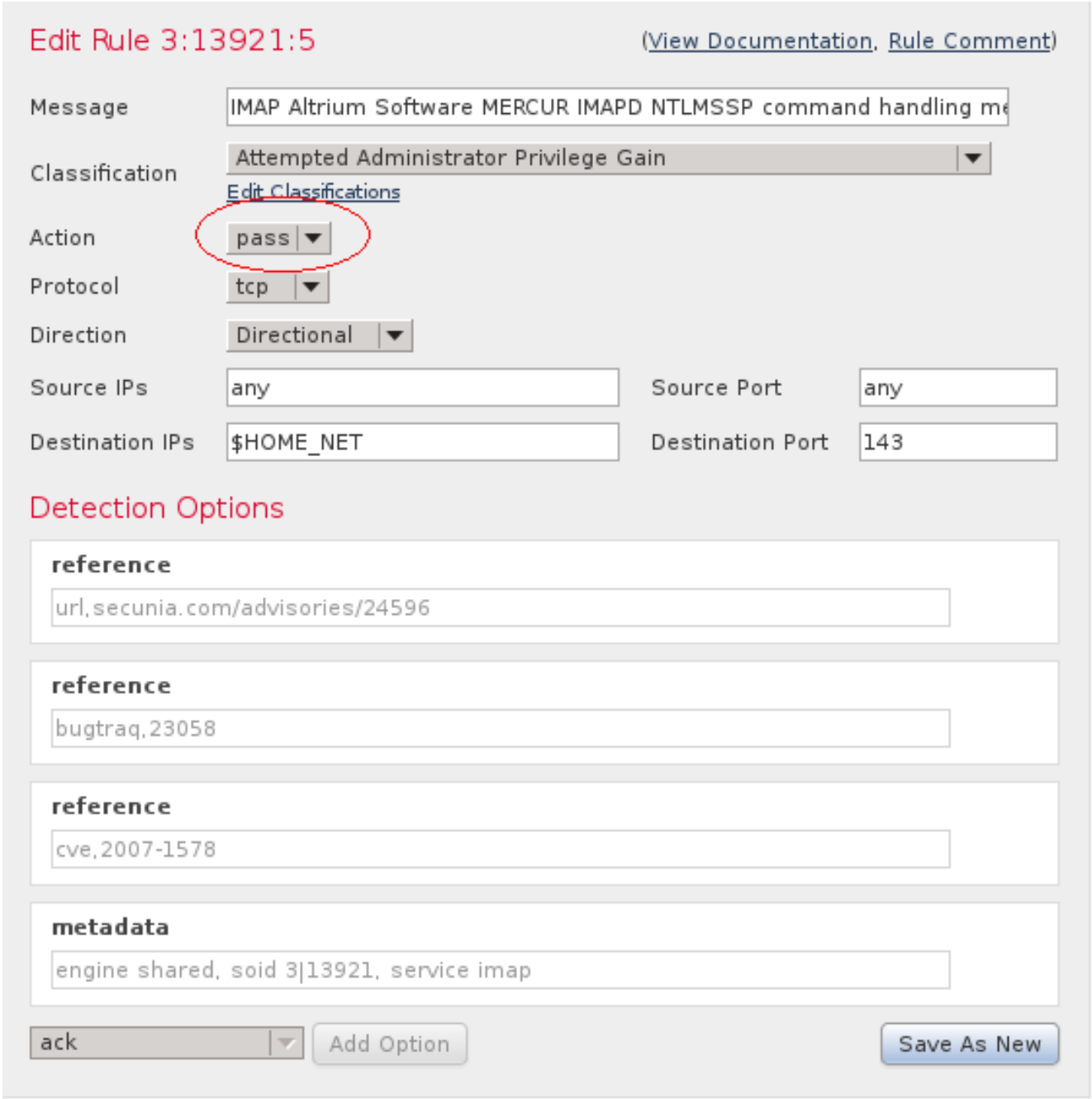
Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

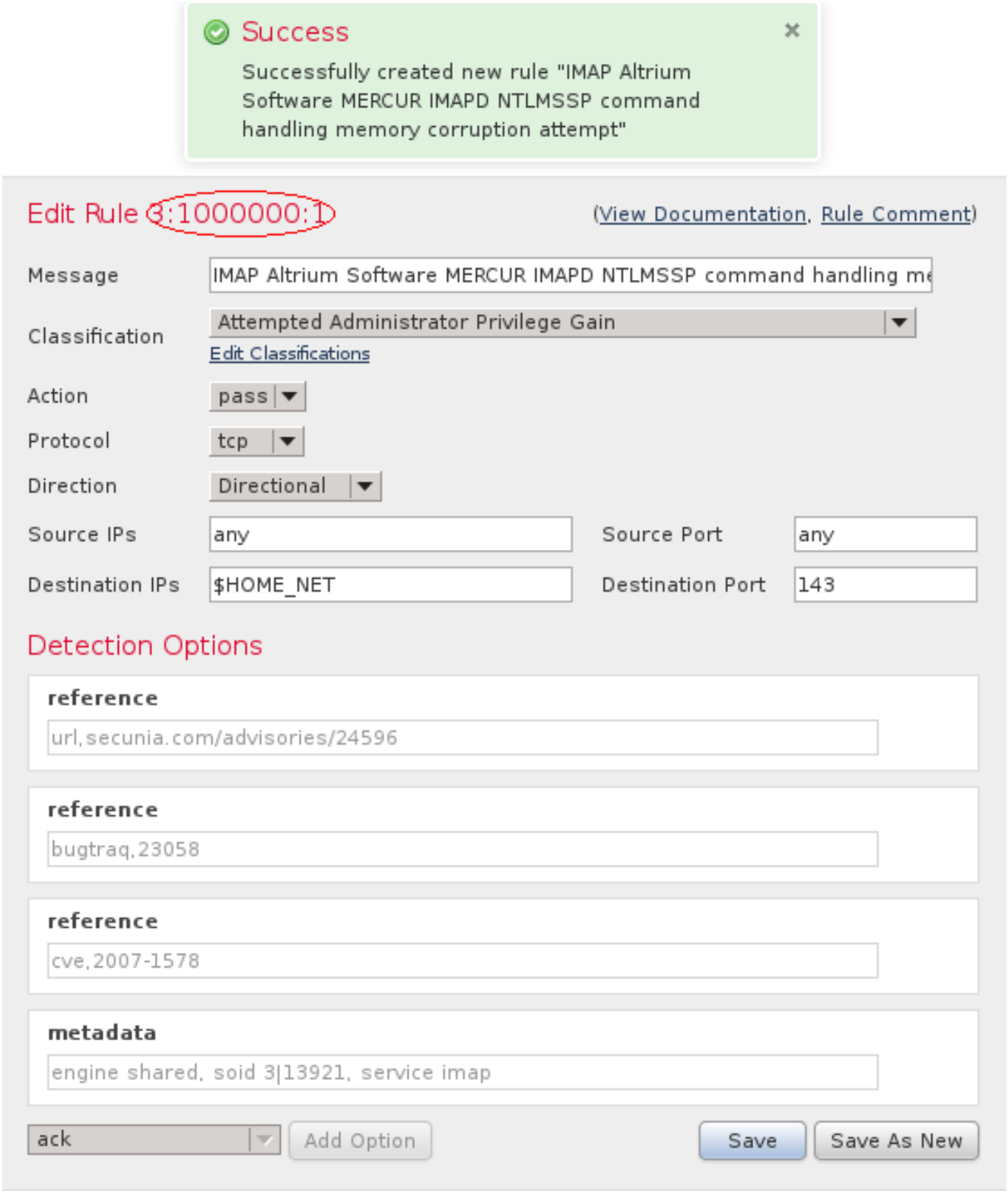
Configurer

Créez une règle de passage

1. Naviguez vers des **objets > des règles d'intrusion**. La liste de catégories de règle apparaît.
2. Trouvez la catégorie de règle qui est associée avec la règle que vous voulez filtrer. Employez l'icône de flèche pour développer la catégorie de règle des listes de catégorie et pour trouver la règle pour laquelle vous voulez faire un passage ordonner. Alternativement, vous pouvez utiliser la fenêtre de recherche de règle.
3. Une fois que vous trouvez la règle désirée, cliquez sur l'icône de crayon à côté de elle afin d'éditer la règle.
4. Quand vous éditez une règle, terminez-vous ces étapes : Cliquez sur le bouton d'**éditer** qui correspond à la règle.Dans la liste déroulante d'action, choisissez le **passage**.Changez le champ de champ IPS de source et IPS de destination aux hôtes ou aux réseaux que vous ne voulez pas la règle d'alerter en fonction.**Sauvegarde de** clic **comme nouvelle**.



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



Activez une règle de passage

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

1. Modifiez la stratégie active d'intrusion : Naviguez vers les **stratégies > le contrôle d'accès > l'intrusion**.Cliquez sur Edit à côté de la stratégie active d'intrusion.
2. Ajoutez la nouvelle règle à la liste de règle : **Règles de** clic sur du côté gauche le volet.Écrivez l'ID de règle que vous avez noté plus tôt dans la case de filtre.Cochez la case

de règles, et changez l'état de règle **pour générer des événements**.**Les informations de stratégie de** clic sur du côté gauche le volet. **Modifications de validation de** clic.
3. Le clic **se déploient** afin de déployer les modifications sur le périphérique.

Vérifiez

Vous devriez surveiller les nouveaux événements pendant quelque temps afin de s'assurer qu'aucun événement n'est généré pour cette règle spécifique pour la source ou l'adresse IP définie de destination.

Dépanner

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