

Configuration d'une règle de passage sur un système de FireSIGHT

Contenu

[Introduction](#)

[Configuration](#)

[Créez une règle de passage](#)

[Activez une règle de passage](#)

[Vérification](#)

Introduction

Vous pouvez créer des règles de passage 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 FireSIGHT compare des paquets contre les conditions spécifiées dans chaque règle et, si les données de paquets appartiennent 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.

Ce document décrit ce qui est une règle de passage, comment la créer et comment l'activer dans une stratégie d'intrusion.

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 peut être difficiles mettre à jour des règles de passage.

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

Configuration

Créez une règle de passage

1. Naviguez vers les **stratégies > l'éditeur d'intrusion > de règle**, pour ouvrir l'éditeur de règle utilisant l'interface web

2. Trouvez la règle que vous voulez filtrer. Employez la fenêtre de recherche ou les listes de catégorie pour trouver la règle pour laquelle vous voulez faire un **passage** ordonner.

3. Éditez la règle d'apparier vos critères :

- Cliquez sur le bouton d'**éditer** correspondant à la règle.
- Changez l'**IP de source ip** et de **destination aux** hôtes ou aux réseaux que vous ne voulez pas la règle d'alerter en fonction.
- Changez l'**action de l'alerte de passer**.

Edit Rule 3:13921:5

[\(View Documentation, Rule Comment\)](#)

Message	IMAP Altrium Software MERCUR IMAPD NTLMSSP command handling me		
Classification	Attempted Administrator Privilege Gain ▼		
	Edit Classifications		
Action	pass ▼		
Protocol	tcp ▼		
Direction	Directional ▼		
Source IPs	any	Source Port	any
Destination IPs	\$HOME_NET	Destination Port	143

Detection Options

reference

url,secunia.com/advisories/24596

reference

bugtraq,23058

reference

cve,2007-1578

metadata

engine shared, soid 3|13921, service imap

ack ▼

Add Option

Save As New

4. **Sauvegarde de clic comme nouvelle.** Notez le numéro d'ID de la nouvelle règle. Par exemple, 1000000.



Success



Successfully created new rule "IMAP Altrium Software MERCUR IMAPD NTLMSSP command handling memory corruption attempt"

Edit Rule 3:1000000:1

[\(View Documentation, Rule Comment\)](#)

Message	IMAP Altrium Software MERCUR IMAPD NTLMSSP command handling me		
Classification	Attempted Administrator Privilege Gain		
	Edit Classifications		
Action	pass		
Protocol	tcp		
Direction	Directional		
Source IPs	any	Source Port	any
Destination IPs	\$HOME_NET	Destination Port	143

Detection Options

reference

url,secunia.com/advisories/24596

reference

bugtraq,23058

reference

cve,2007-1578

metadata

engine shared, soid 3|13921, service imap

ack

Add Option

Save

Save As New

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 les étapes ci-dessous pour activer une règle de passage :

1. Modifiez la stratégie active d'intrusion.

- Naviguez vers des **stratégies > l'intrusion > la stratégie d'intrusion**.
- Cliquez sur Edit à côté de votre stratégie fonctionnante.

2. Ajoutez la nouvelle règle à la liste de règle.

- **Règles de clic** sur le volet de côté gauche.
- Écrivez l'ID de règle que vous avez noté plus tôt dans la case de filtre.
- Sélectionnez la case de règles, et changez l'état de règle **pour générer des événements**.
- **Les informations de stratégie de clic** sur le volet de côté gauche. **La validation de clic change le bouton**.

3. Cliquez sur le bouton de **stratégie d'application** à côté de la stratégie d'intrusion. Sélectionnez vos périphériques et le clic **réappliquent**.

Vérification

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