

FireSIGHT システムでのパス ルールの設定

目次

[概要](#)

[設定](#)

[パス ルールを作成して下さい](#)

[パス ルールを有効に して下さい](#)

[確認](#)

概要

ルールをある特定の状況では引き起こすことからのルールで定義される条件を満たすルールを作成できま ルールをディセーブルにしますよりもむしろパケットを防ぐ。デフォルトで、ルール上書きする ルール。SireSIGHT システムは各ルールおよび、ルールトリガーで規定される条件に対してパケットデータがルールで規定される条件すべてと一致すればパケットを比較します。ルールが ルールである場合、不正侵入 イベントを生成します。ルールである場合、トラフィックを無視します。

たとえば、アクティブのままになるために「匿名ユーザ」として FTP サーバにログイン する 試みを探すルールがほしいと思うかもしれません。ただし、ネットワークに1つ以上の正当な匿名FTP サーバがあれば、それらの特定のサーバのために、匿名ユーザーはオリジナル ルールを引き起こさないこと規定 する ルールを書き、アクティブにする可能性があります。

それをおよび不正侵入 ポリシーでそれを作成する方法を ルールはであるものこの資料に、有効にする方法を記述されています。

注意： ルールが基づいているオリジナル ルールが修正を受け取るとき、ルールは自動的にアップデートされません。従って、ルールは維持しにくくないですかもしれません。

注: ルールのための抑制機能を有効に する場合、そのルールのためのイベント 通知を抑制します。ただしルールはまだ評価されますあります。たとえば、ルールを抑制すれば、ルールを一致するパケットは無言で廃棄されます。

設定

パス ルールを作成して下さい

1. Webインターフェイスを使用しているルール エディタを開くためにポリシー > 不正侵入 > ル

ール エディタに、ナビゲートして下さい

2. フィルタリングしたいと思うルールを調べて下さい。 支配させたいと思うルールを見つけるのに検索ボックスかカテゴリ リストを使用して下さい。

3. 条件を満たすルールを編集して下さい:

- ルールに相当して **Edit ボタン**をクリックして下さい。
- 警告 するルールがほしいと思わないことホストかネットワークに出典 IP および宛先IP を変更して下さい。
- 渡るためにアラートから処理を変更して下さい。

Edit Rule 3:13921:5 [\(View Documentation, Rule Comment\)](#)

Message

Classification [Edit Classifications](#)

Action

Protocol

Direction

Source IPs Source Port

Destination IPs Destination Port

Detection Options

reference

reference

reference

metadata

4. 新しい『Save As』 をクリックして下さい。 新しいルールの ID 番号に注意して下さい。 たとえば、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			
<input type="text" value="url,secunia.com/advisories/24596"/>			
reference			
<input type="text" value="bugtraq,23058"/>			
reference			
<input type="text" value="cve,2007-1578"/>			
metadata			
<input type="text" value="engine shared, soid 3 13921, service imap"/>			
ack ▼	<input type="button" value="Add Option"/>	<input type="button" value="Save"/>	<input type="button" value="Save As New"/>

パス ルールを有効に して下さい

規定した 送信元または宛先アドレスのトラフィックを通過させることを適切な不正侵入 ポリシーの新しいルールが可能にする必要があります。 ルールを有効に するために下記のステップに従って下さい:

1. アクティブな不正侵入 ポリシーを修正して下さい。

- [Policies] > [Intrusion] > [Intrusion Policy] に移動します。
- はたらくポリシーの隣で『Edit』をクリックして下さい。

2. ルール リストに新しいルールを追加して下さい。

- 左側 ペインで『Rules』をクリックして下さい。
- フィルタ ボックスで先に注意したルール ID を入力して下さい。
- Rules チェックボックスを選択し、**イベントを生成するためにルール状態を変更して下さい**。
- 左側 ペインの**ポリシー情報**をクリックして下さい。 **託します変更**ボタンをクリックして下さい。

3. 不正侵入 ポリシーの隣で**適用ポリシー** ボタンをクリックして下さい。 デバイスを選択し、**再適用**をクリックして下さい。

確認

イベントが定義された出典または宛先IP のこの特定のルールのために生成されないことを確かめるために新しいイベントをしばらくの間監視する必要があります。