Configure a Pass Rule on a Cisco Firepower System

Contents

Introduction

This document describes a pass rule, how to create it, and how to enable it in an intrusion policy.

You can create pass rules in order to prevent packets that meet criteria defined in the pass rule from triggering the alert rule in specific situations, rather than disabling the alert rule. By default, pass rules override alert rules. A Firepower System compares packets against the conditions specified in each rule and, if the packet data matches all of the conditions specified in a rule, the rule triggers. If a rule is an alert rule, it generates an intrusion event. If it is a pass rule, it ignores the traffic.

For example, you might want a rule that looks for attempts to log into an FTP server as the user “anonymous” to remain active. However, if your network has one or more legitimate anonymous FTP servers, you could write and activate a pass rule that specifies that, for those specific servers, anonymous users do not trigger the original rule.

> **Caution**: When an original rule that the pass rule is based on receives a revision, the pass rule is not automatically updated. Therefore, pass rules might be difficult to maintain.

> **Note**: If you enable the Suppression feature for a rule, it suppresses the event notifications for that rule. However the rule is still is evaluated. For example, if you supress a drop rule, packets that match the rule are silently dropped.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

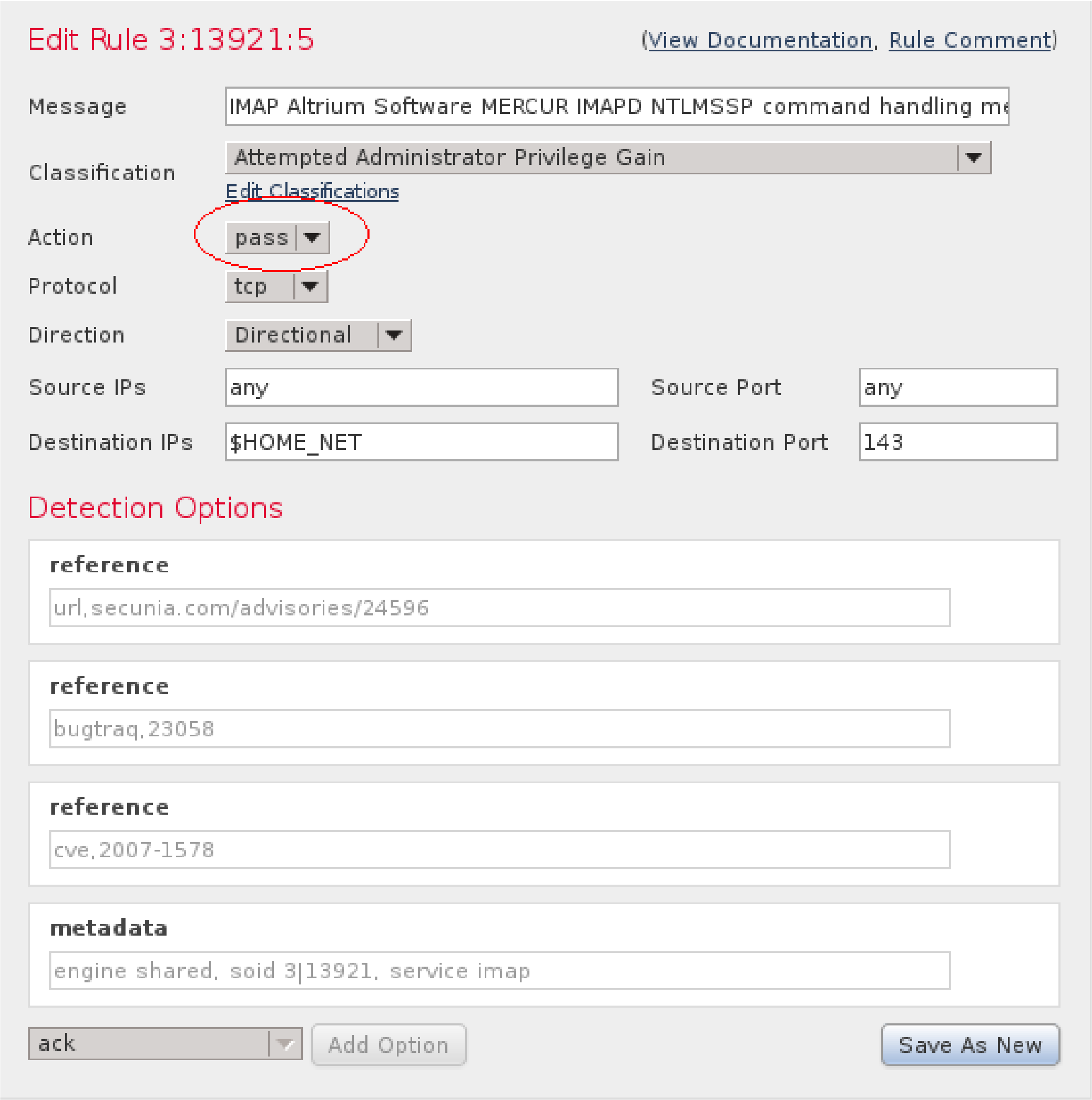
This document is not restricted to specific software and hardware versions.

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.

Configure

Create a Pass Rule

1. Navigate to **Objects > Intrusion Rules**. The list of rule categories appears.
2. Find the rule category that is associated with the rule you want to filter. Use the arrow icon to expand the rule category from the category listings and find the rule that you want to make a pass rule for. Alternatively, you can use the rule search box.
3. Once you find the desired rule, click the pencil icon next to it in order to edit the rule.
4. When you edit a rule, complete these steps: Click the **Edit** button that corresponds to the rule.In the Action drop-down list, choose **pass**.Change the Source IPs field and Destination IPs field to the hosts or networks that you do not want the rule to alert on.Click **Save As New**.



Edit Rule 3:13921:5

Message: IMAP Altrium Software MERCUR IMAPD NTLMSSP command handling me

Classification: Attempted Administrator Privilege Gain

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

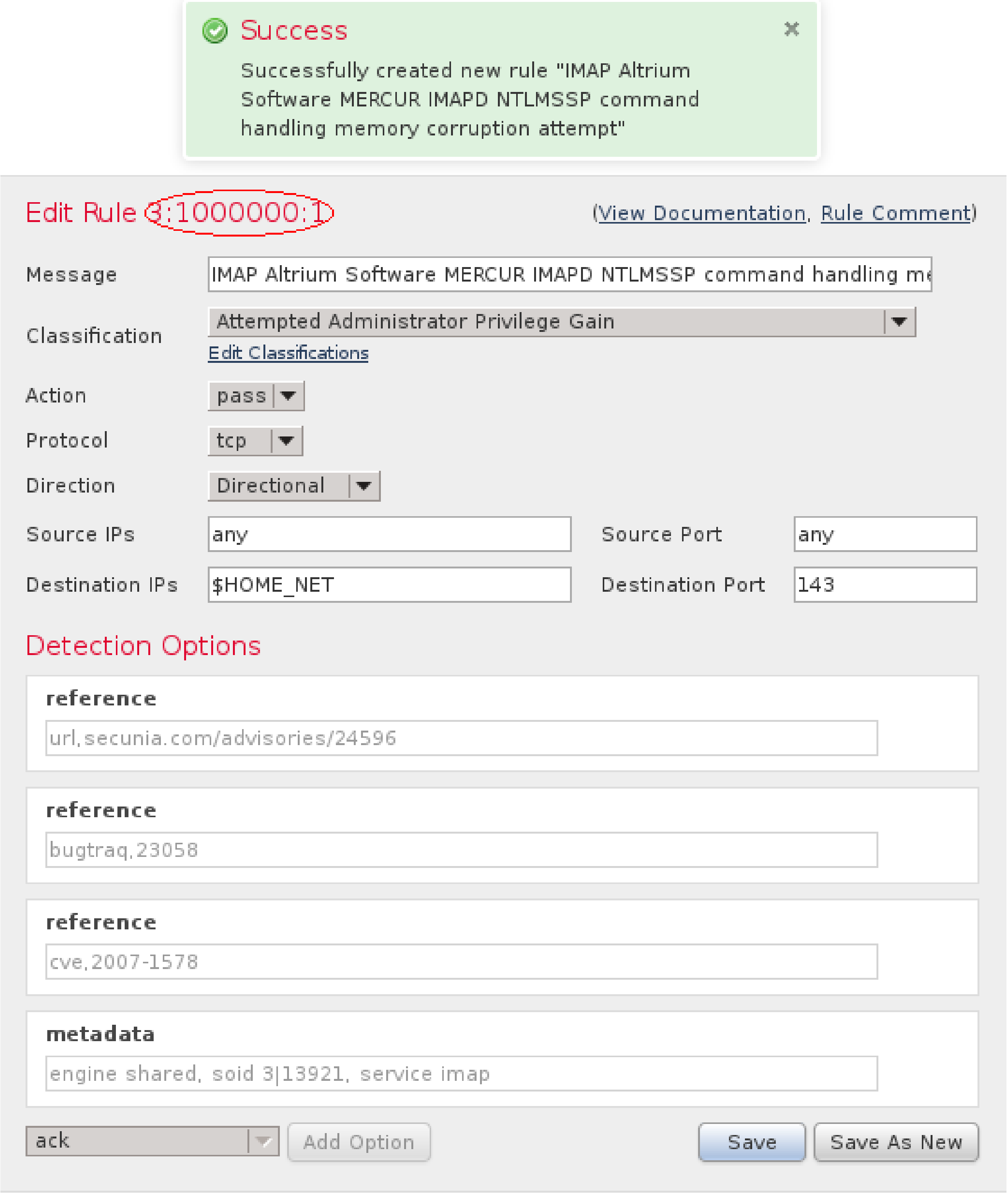
reference: bugtraq,23058

reference: cve,2007-1578

metadata: engine shared, soid 3|13921, service imap

ack

5. Note the ID number of the new rule. For example, 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

Enable a Pass Rule

You need to enable your new rule in the appropriate intrusion policy in order to pass traffic on the source or destination addresses that you specified. Follow these steps in order to enable a pass rule:

1. Modify the active intrusion policy: Navigate to **Policies > Access Control > Intrusion**.Click **Edit** next to the active intrusion policy.
2. Add the new rule to the rule list: Click **Rules** on the left-side pane.Enter the Rule ID you noted earlier in the filter box.Check the Rules check box, and change the Rule State to

Generate Events.Click **Policy Information** on the left-side pane. Click **Commit Changes**.

3. Click **Deploy** in order to deploy the changes on the device.

Verify

You should monitor the new events for some time in order to make sure no events are generated for this specific rule for the defined source or destination IP address.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.