Konfigurieren einer Passregel für ein Cisco FirePOWER-System

Inhalt

Einführung

In diesem Dokument wird eine Pass-Regel beschrieben, wie Sie sie erstellen und in einer Intrusion-Richtlinie aktivieren.

Sie können Pass-Regeln erstellen, um zu verhindern, dass Pakete, die die in der Pass-Regel definierten Kriterien erfüllen, die Warnregel in bestimmten Situationen auslösen, anstatt die Warnregel zu deaktivieren. In der Standardeinstellung überschreiben Regeln Warnungsregeln. Ein FirePOWER-System vergleicht Pakete mit den in jeder Regel angegebenen Bedingungen. Wenn die Paketdaten mit allen in einer Regel angegebenen Bedingungen übereinstimmen, wird die Regel ausgelöst. Wenn eine Regel eine Warnregel ist, wird ein Intrusion-Ereignis generiert. Wenn es sich um eine Pass-Regel handelt, wird der Datenverkehr ignoriert.

Sie können z. B. eine Regel wünschen, die nach Versuchen sucht, sich bei einem FTP-Server anzumelden, da der Benutzer "anonym" aktiv bleiben soll. Wenn Ihr Netzwerk jedoch über einen oder mehrere legitime anonyme FTP-Server verfügt, können Sie eine Pass-Regel schreiben und aktivieren, die angibt, dass für diese speziellen Server anonyme Benutzer die ursprüngliche Regel nicht auslösen.

> **Vorsicht**: Wenn eine ursprüngliche Regel, die besagt, dass die Pass-Regel auf einer Revision beruht, wird die Pass-Regel nicht automatisch aktualisiert. Aus diesem Grund ist die Beibehaltung von Pass-Regeln möglicherweise schwierig.

> **Hinweis**: Wenn Sie die Unterdrückungsfunktion für eine Regel aktivieren, werden die Ereignisbenachrichtigungen für diese Regel unterdrückt. Die Regel wird jedoch noch ausgewertet. Wenn Sie z. B. eine Drop-Regel unterdrücken, werden Pakete, die der Regel entsprechen, im Hintergrund verworfen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

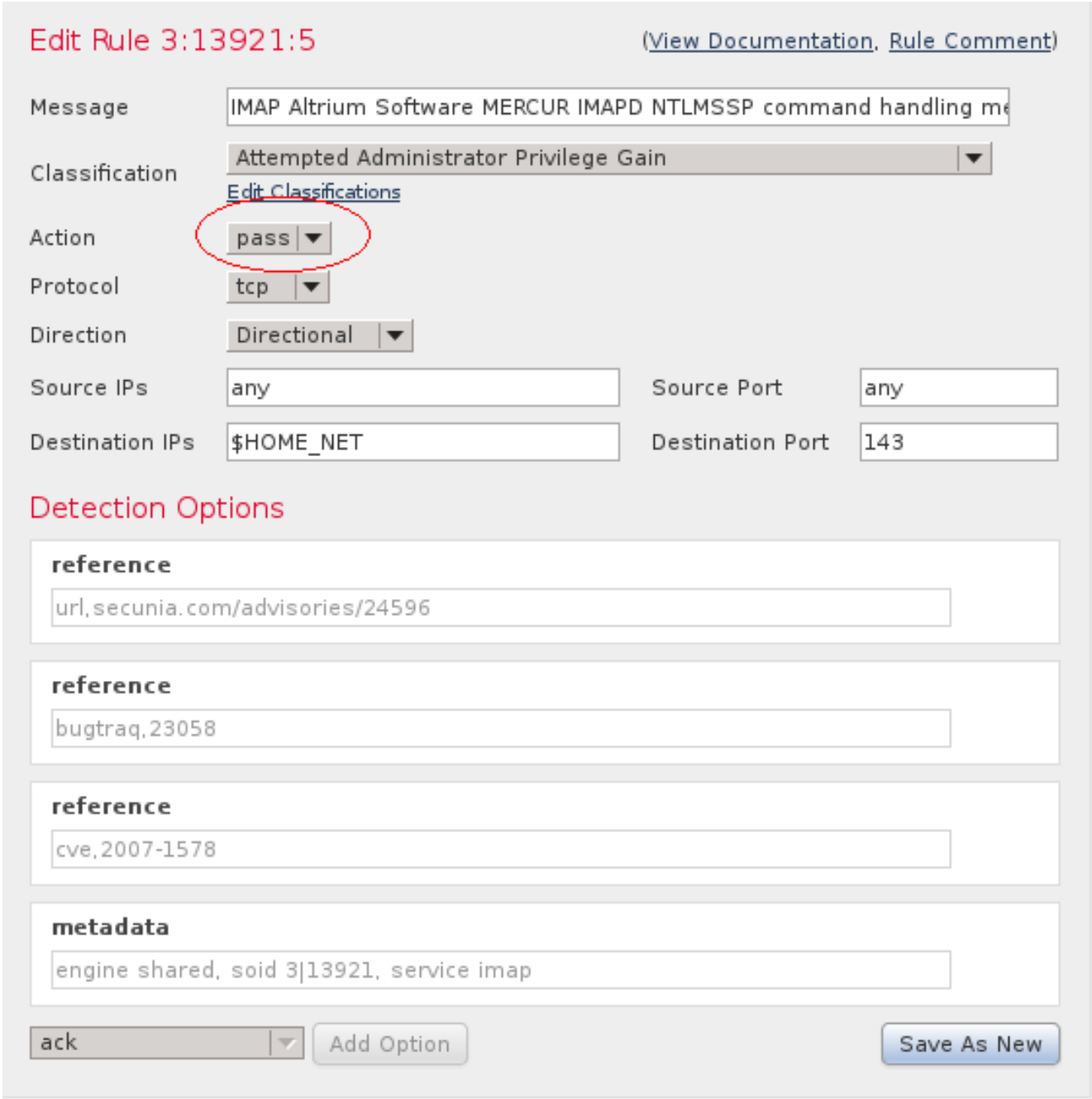
Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

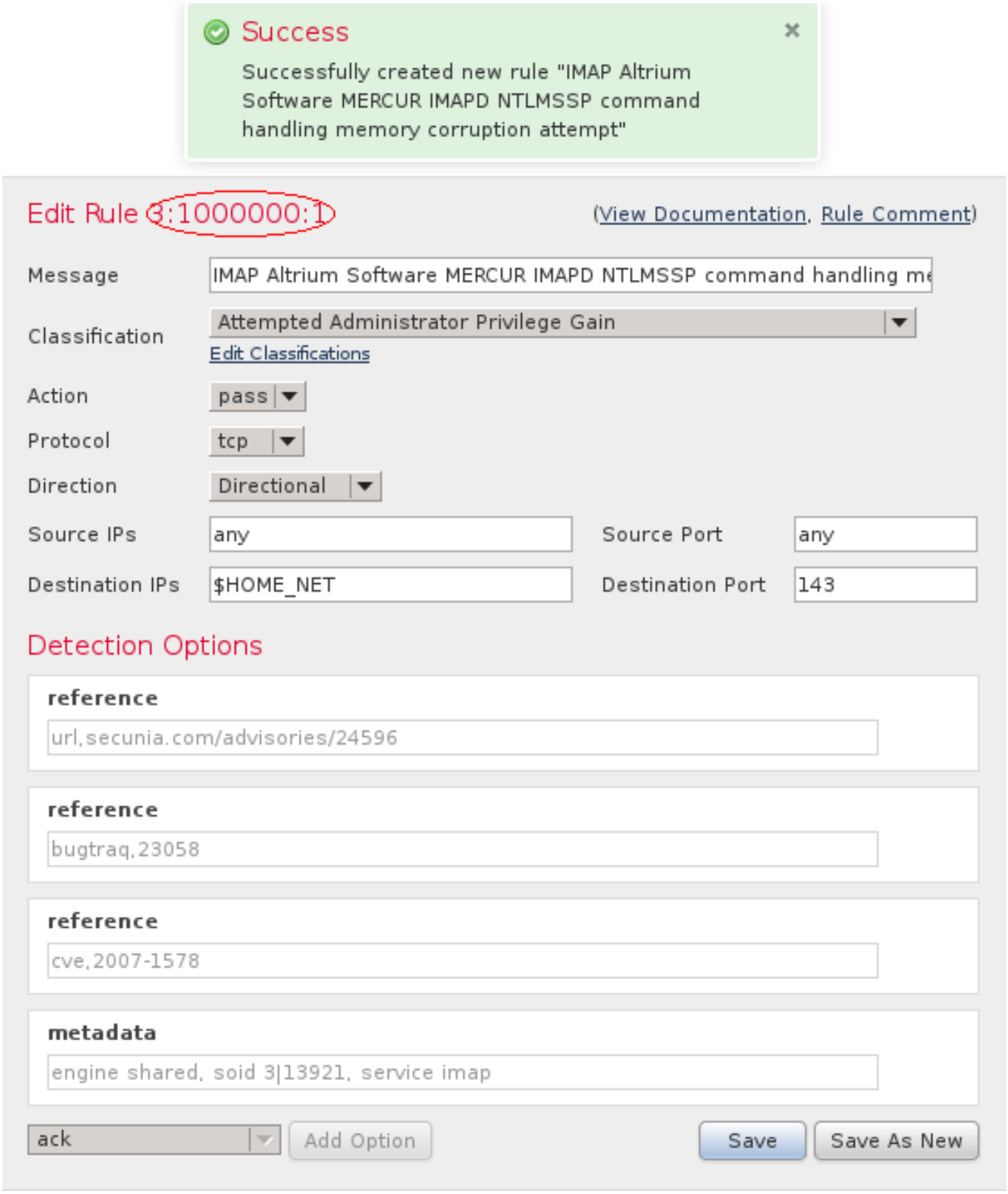
Konfigurieren

Erstellen einer Pass-Regel

1. Navigieren Sie zu **Objekte > Angriffsregeln**. Die Liste der Regelkategorien wird angezeigt.
2. Suchen Sie die Regelkategorie, die der Regel zugeordnet ist, die Sie filtern möchten. Verwenden Sie das Pfeilsymbol, um die Regelkategorie aus den Kategorienauflistungen zu erweitern und die Regel zu finden, für die Sie eine Pass-Regel erstellen möchten. Sie können auch das Regelsuchfeld verwenden.
3. Wenn Sie die gewünschte Regel gefunden haben, klicken Sie auf das Bleistiftsymbol neben der Regel, um sie zu bearbeiten.
4. Gehen Sie wie folgt vor, wenn Sie eine Regel bearbeiten: Klicken Sie auf die Schaltfläche **Bearbeiten**, die der Regel entspricht.Wählen Sie in der Dropdown-Liste Aktion die Option **Übergeben aus**.Ändern Sie das Feld Quell-IPs und das Feld Ziel-IPs in die Hosts oder Netzwerke, bei denen die Regel nicht benachrichtigt werden soll.Klicken Sie auf **Als neu speichern**.



5. Notieren Sie sich die ID-Nummer der neuen Regel. Beispiel: 1000000.



Aktivieren einer Pass-Regel

Sie müssen Ihre neue Regel in der entsprechenden Zugriffsrichtlinie aktivieren, um Datenverkehr an die von Ihnen angegebenen Quell- oder Zieladressen weiterzuleiten. Führen Sie die folgenden Schritte aus, um eine Regel für die erfolgreiche Ausführung zu aktivieren:

1. Ändern Sie die aktive Intrusion Policy: Navigieren Sie zu **Richtlinien > Zugriffskontrolle > Zugriffskontrolle**.Klicken Sie neben der aktiven Intrusion-Policy **auf Edit**.
2. Fügen Sie die neue Regel der Regelliste hinzu: Klicken Sie im linken Bereich auf **Regeln**.Geben Sie die zuvor erwähnte Regel-ID in das Filterfeld ein.Aktivieren Sie das

Kontrollkästchen Regeln, und ändern Sie den Regelstatus in **Generieren von Ereignissen**.Klicken Sie im linken Bereich auf **Policy Information** (Richtlinieninformationen). Klicken Sie auf **Änderungen bestätigen**.

3. Klicken Sie auf **Bereitstellen**, um die Änderungen auf dem Gerät bereitzustellen.

Überprüfen

Sie sollten die neuen Ereignisse für einige Zeit überwachen, um sicherzustellen, dass für diese bestimmte Regel für die definierte Quell- oder Ziel-IP-Adresse keine Ereignisse generiert werden.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.