# Benutzerdefinierte lokale Snort-Regeln in Snort3 auf FTD konfigurieren

## Inhalt



## Einleitung

In diesem Dokument wird das Verfahren zur Konfiguration benutzerdefinierter lokaler Snort-Regeln in Snort3 auf der Firewall-Bedrohungsabwehr (FTD) beschrieben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco FirePOWER Management Center (FMC)
- Schutz vor Bedrohungen durch Firewall (FTD)

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

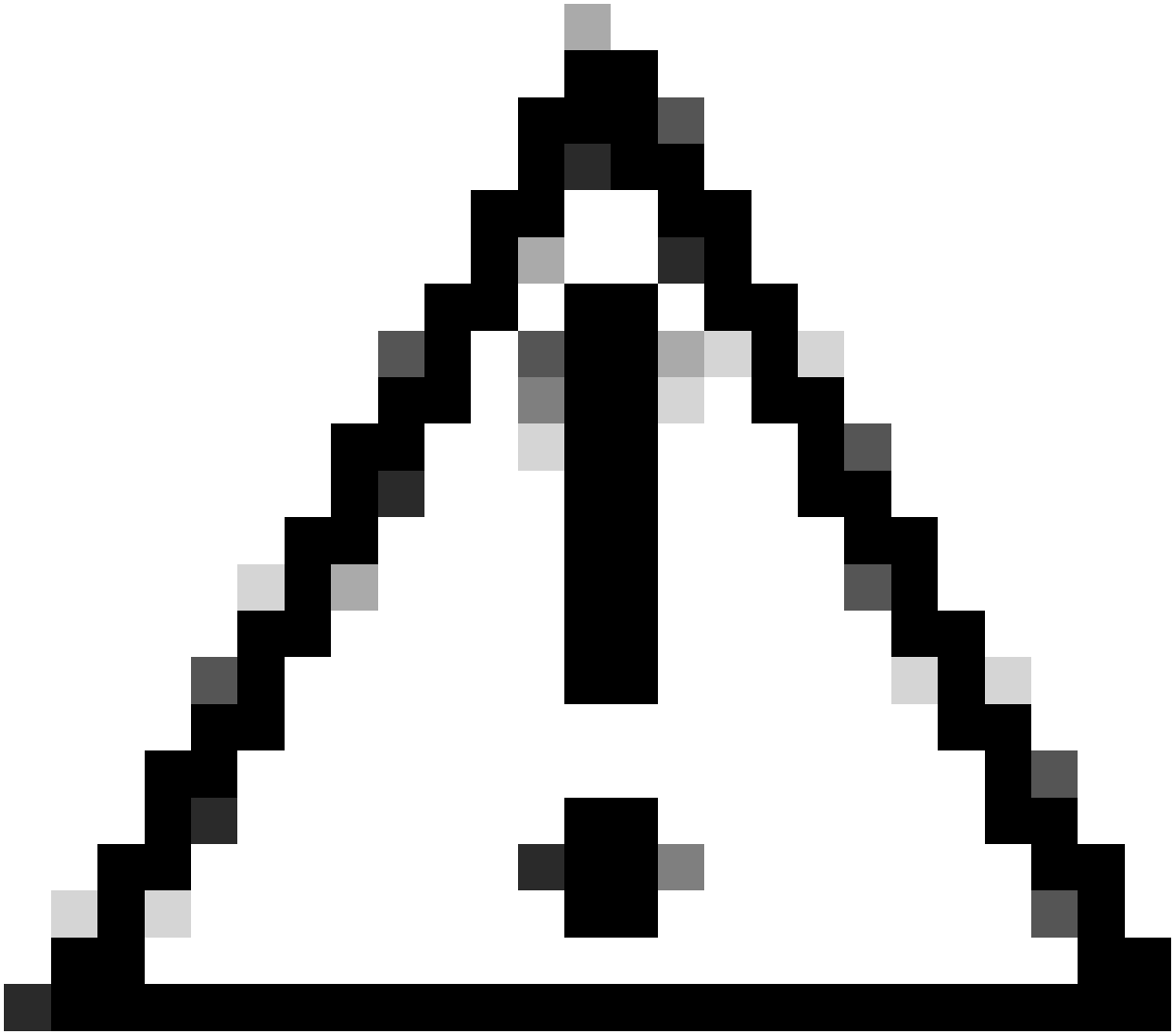
- Cisco FirePOWER Management Center für VMware 7.4.1
- Cisco FirePOWER 2120 7.4.1

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrundinformationen

Die Unterstützung von Snort 3 beim Schutz vor Bedrohungen mit Management Center beginnt in Version 7.0. Für neue und neu erstellte Geräte der Version 7.0 und höher ist Snort 3 die Standard-Prüfungs-Engine.

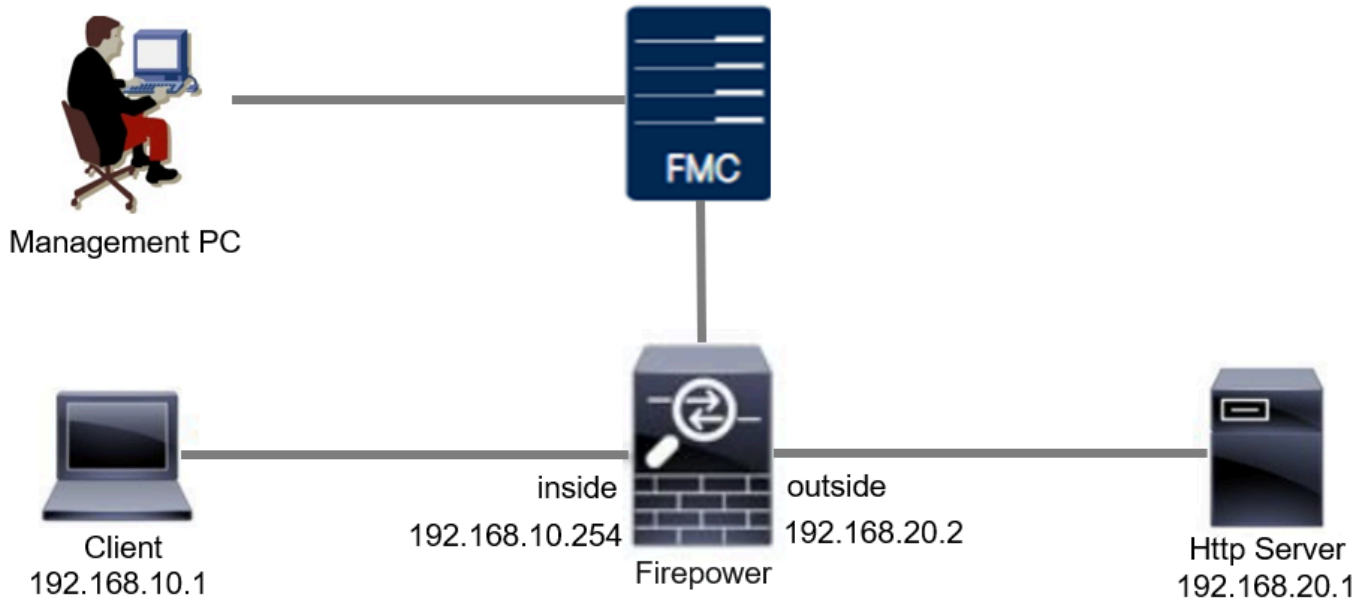
In diesem Dokument finden Sie ein Beispiel zum Anpassen von Snort-Regeln für Snort 3 sowie ein praktisches Verifizierungsbeispiel. Insbesondere wird erläutert, wie Sie eine Angriffsrichtlinie mit einer angepassten Snort-Regel konfigurieren und überprüfen, um HTTP-Pakete zu verwerfen, die eine bestimmte Zeichenfolge (Benutzername) enthalten.



Vorsicht: Das Erstellen benutzerdefinierter lokaler Snort-Regeln und die Bereitstellung von Support hierfür fallen nicht unter den TAC-Support. Daher kann dieses Dokument nur als Referenz verwendet werden und Sie bitten, diese benutzerdefinierten Regeln nach eigenem Ermessen und mit eigener Verantwortung zu erstellen und zu verwalten.

## Netzwerkdiagramm

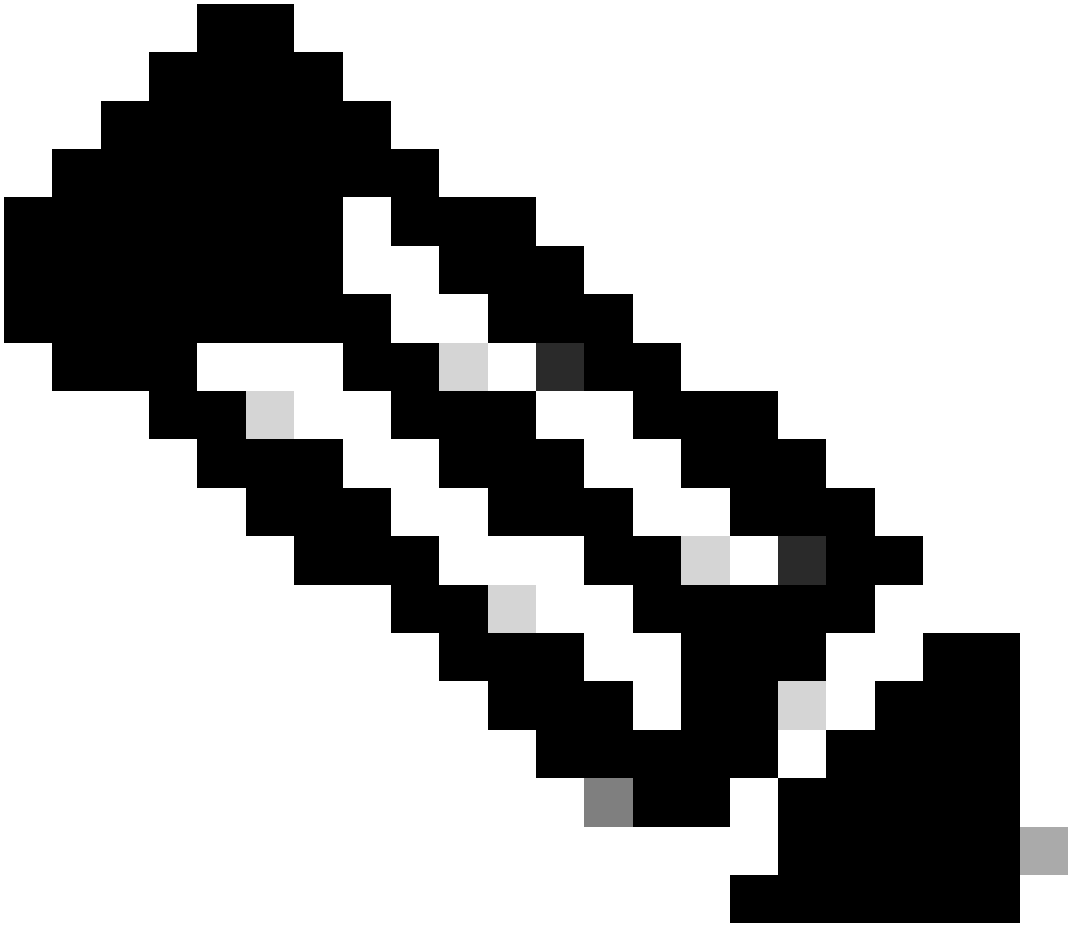
In diesem Dokument wird die Konfiguration und Überprüfung der benutzerdefinierten lokalen Snort-Regel in Snort3 in diesem Diagramm vorgestellt.




Netzwerkdiagramm

## Konfiguration

Dies ist die Konfiguration der benutzerdefinierten lokalen Snort-Regel zum Erkennen und Löschen von HTTP-Antwortpaketen, die eine bestimmte Zeichenfolge (Benutzername) enthalten.

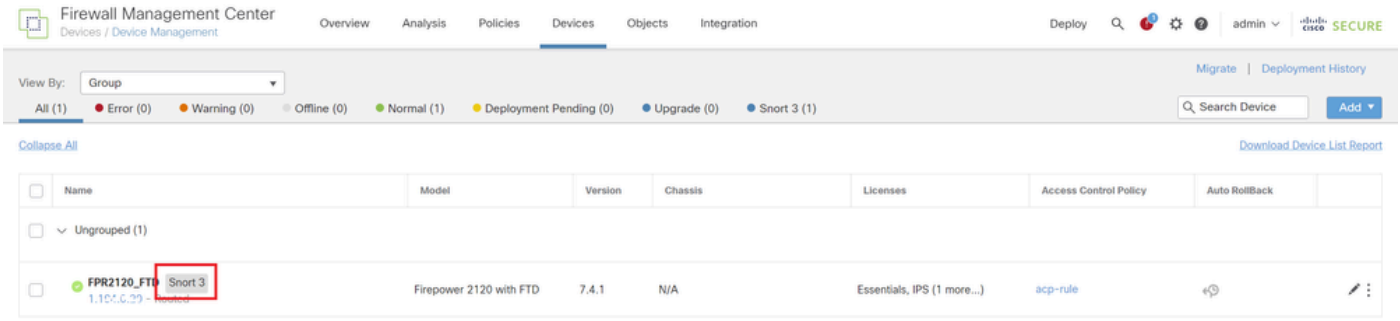


Hinweis: Ab sofort ist es nicht möglich, benutzerdefinierte lokale Snort-Regeln von der Snort 3 All Rules-Seite in der FMC-GUI hinzuzufügen. Sie müssen die in diesem Dokument eingeführte Methode verwenden.

## Methode 1: Von Snort 2 nach Snort 3 importieren

Schritt 1: Snort-Version bestätigen

Navigieren Sie zuGeräte>Geräteverwaltung auf FMC, und klicken Sie auf Registerkarte Gerät. Bestätigen Sie, dass die Snort-Version Snort3 ist.



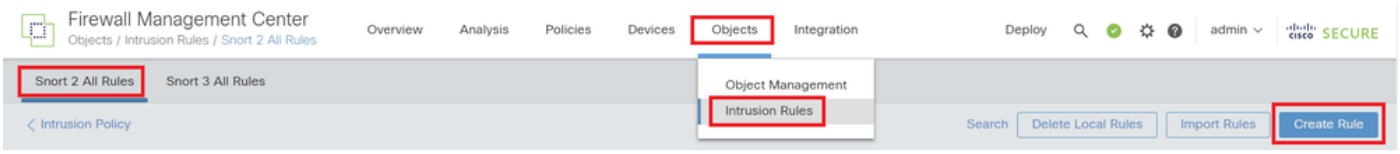

Snort-Version

Schritt 2: Erstellen oder Bearbeiten einer benutzerdefinierten lokalen Snort-Regel in Snort 2

Navigieren Sie zu Objekte > Intrusion Rules > Snort 2 All Ruleson FMC. Klicken Sie auf Create Rule (Regel erstellen), um eine benutzerdefinierte lokale Snort-Regel hinzuzufügen, oder Navigieren Sie zu Objects > Intrusion Rules > Snort 2 All Rules > Local Rules on FMC. Klicken Sie auf Edit (Bearbeiten), um eine vorhandene benutzerdefinierte lokale Snort-Regel zu bearbeiten.

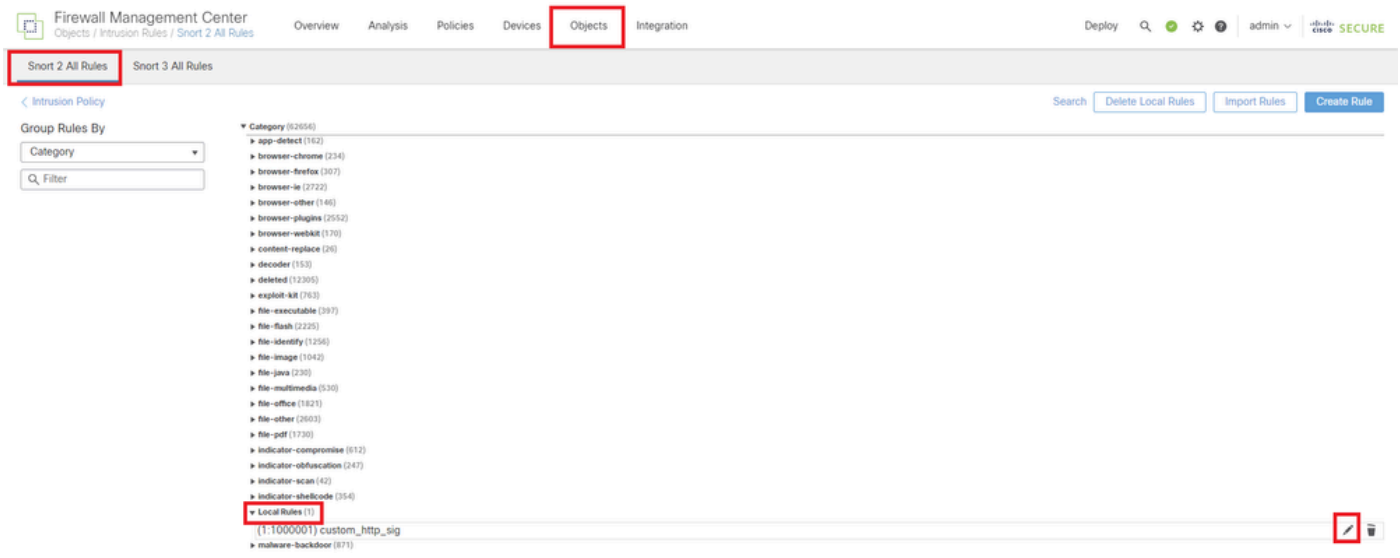
Anweisungen zum Erstellen von benutzerdefinierten lokalen Snort-Regeln in Snort 2 finden Sie unter Konfigurieren von benutzerdefinierten lokalen Snort-Regeln in Snort2 auf FTD.

Fügen Sie eine neue benutzerdefinierte lokale Snort-Regel hinzu, wie im Bild angezeigt.




Hinzufügen einer neuen benutzerdefinierten Regel

Bearbeiten Sie eine vorhandene benutzerdefinierte lokale Snort-Regel, wie im Bild angezeigt. In diesem Beispiel wird eine vorhandene benutzerdefinierte Regel bearbeitet.

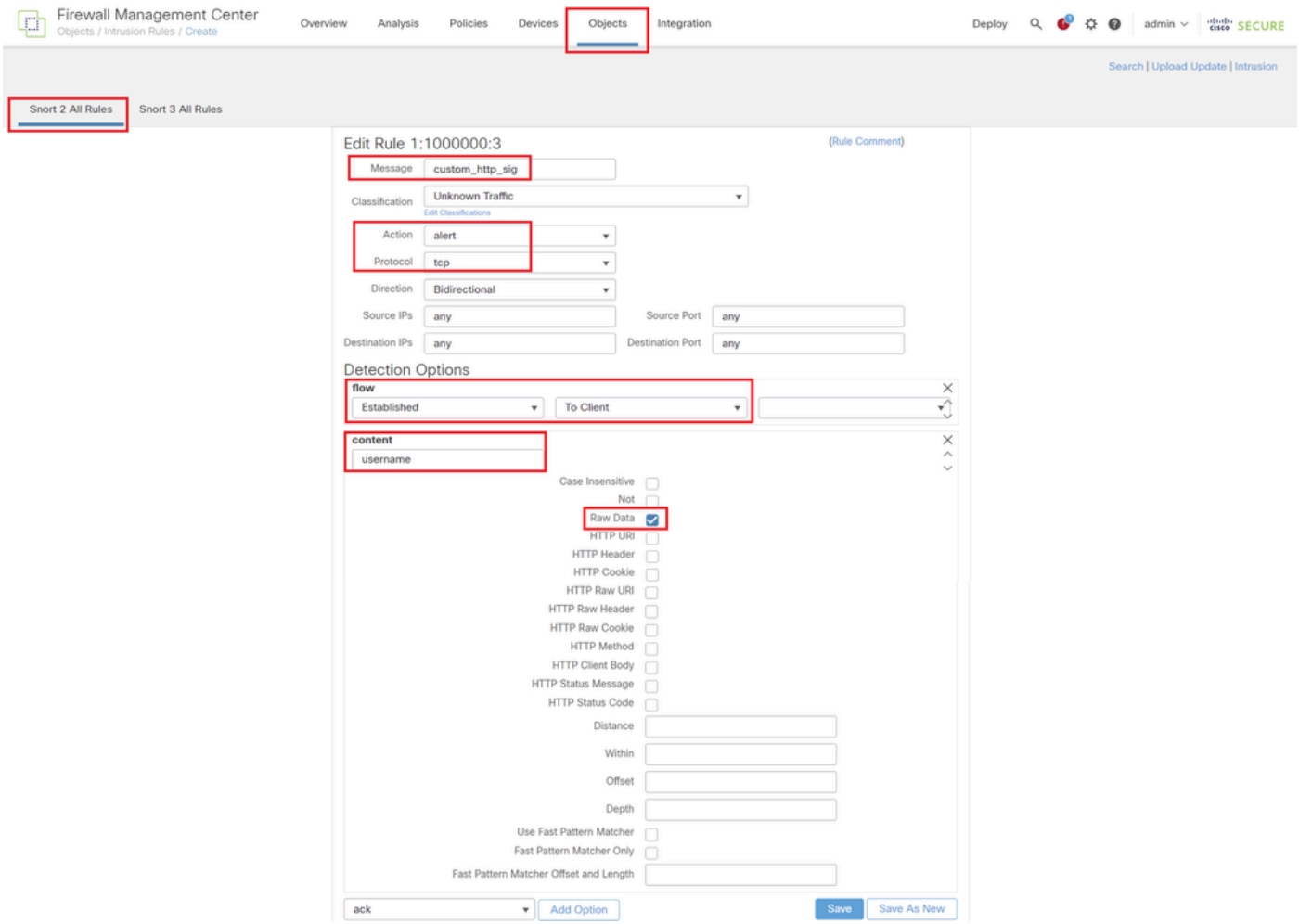



Bearbeiten einer vorhandenen benutzerdefinierten Regel

Geben Sie die Signaturinformationen ein, um HTTP-Pakete mit einer bestimmten Zeichenfolge

(Benutzername) zu erkennen.

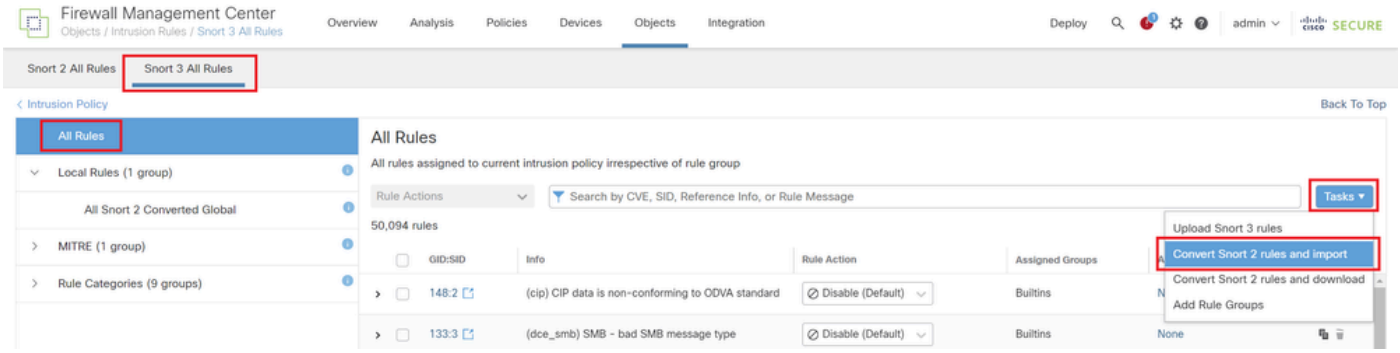
- Nachricht: custom_http_sig
- Aktion: alert
- Protokoll: TCP
- Fluss: etabliert, an Client
- Inhalt : Benutzername (Rohdaten)



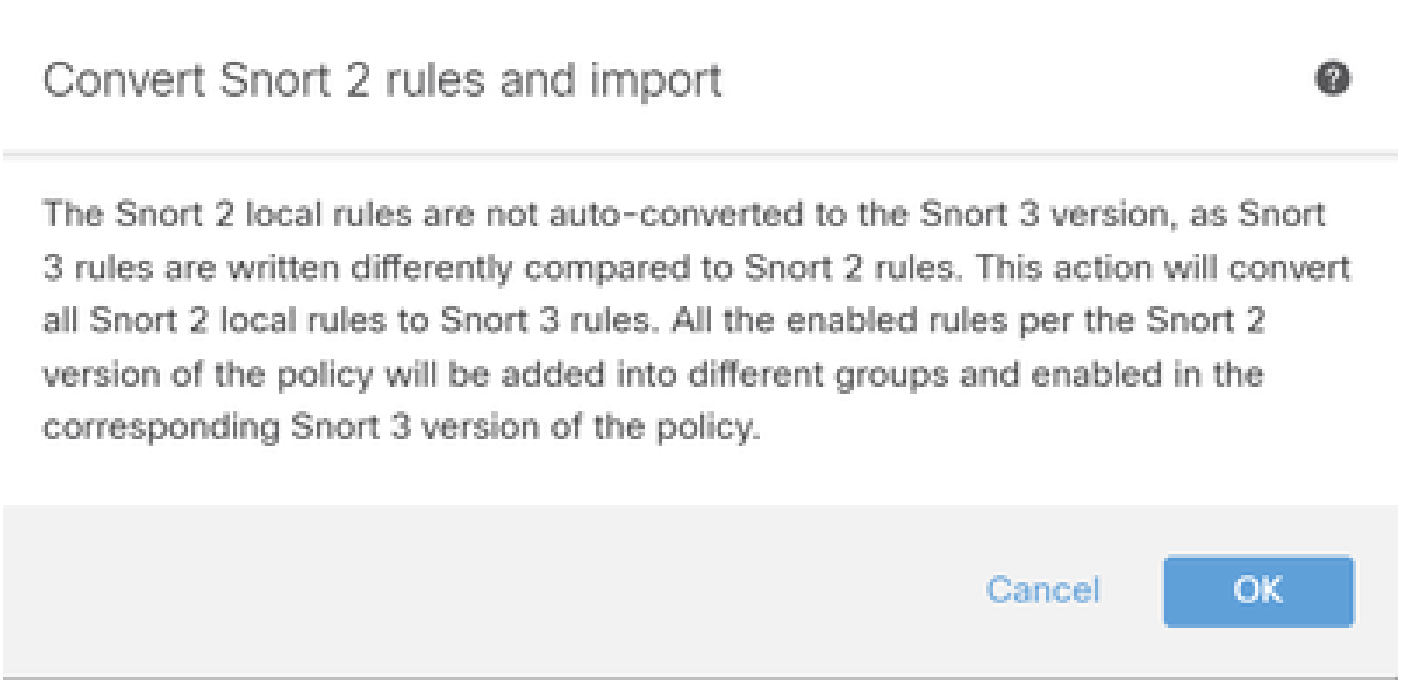

Eingabe der erforderlichen Informationen für Regel

Schritt 3: Importieren von benutzerdefinierten lokalen Snort-Regeln von Snort 2 nach Snort 3

Navigieren Sie zu Objekte > Intrusion Rules > Snort 3 All Rules > All Rules on FMC, und klicken Sie auf Convert Snort 2 rules and Import from Tasks-Pulldown-Liste.

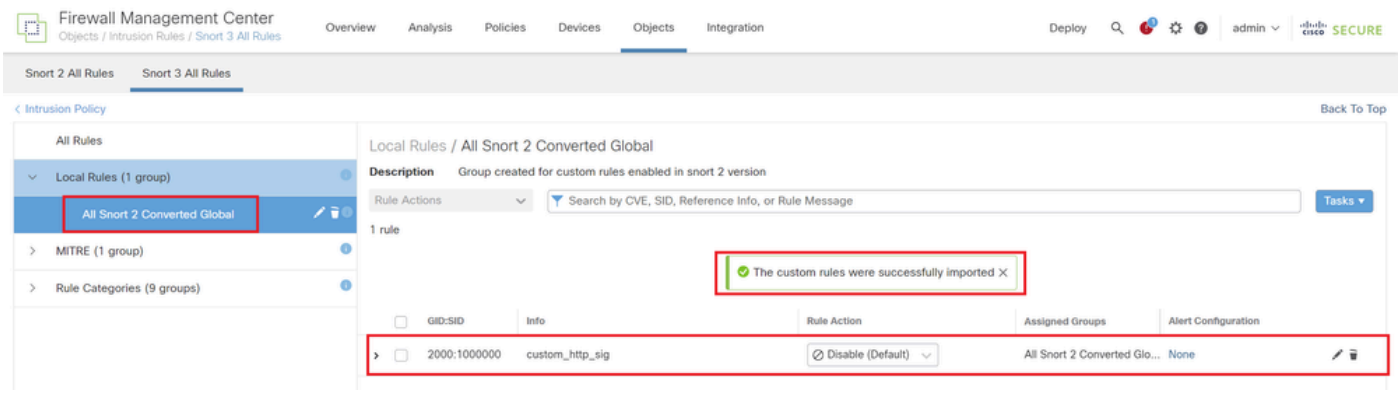


Überprüfen Sie die Warnmeldung, und klicken Sie auf OK.




Warnmeldung

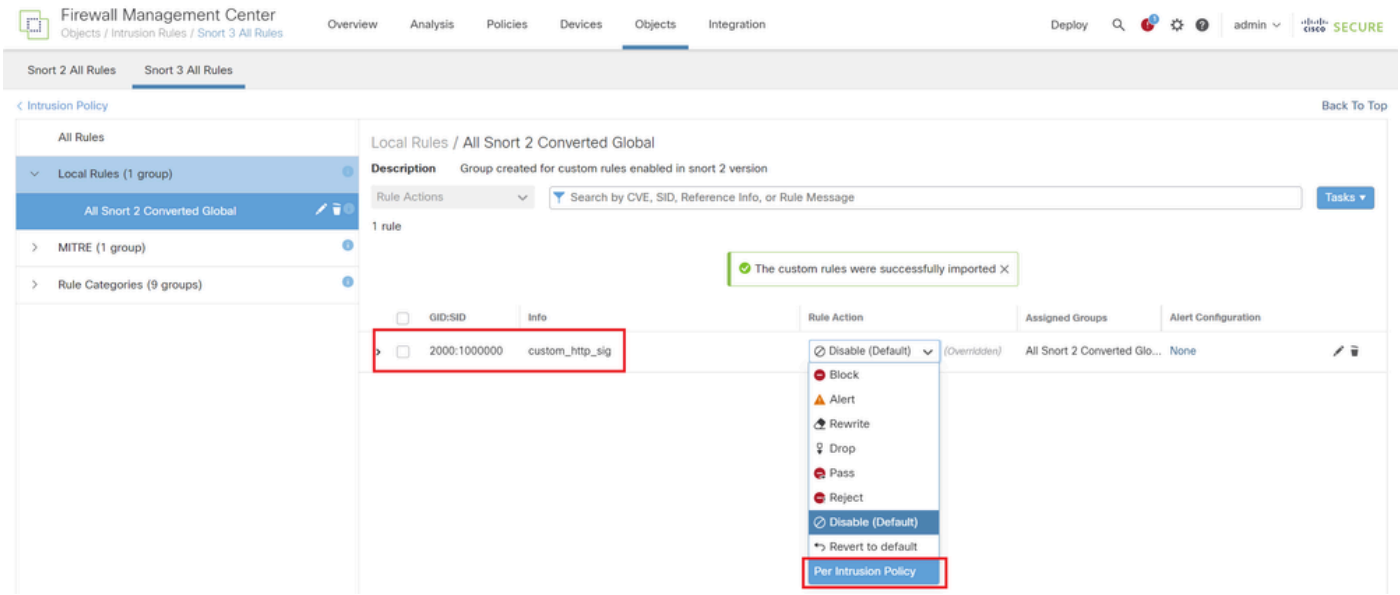
Navigieren Sie zu Objekte > Intrusion Rules > Snort 3 All Rules on FMC, und klicken Sie auf All Snort 2 Converted Global, um die importierte benutzerdefinierte lokale Snort-Regel zu bestätigen.




Importierte benutzerdefinierte Regel bestätigen

Schritt 4: Regelaktion ändern

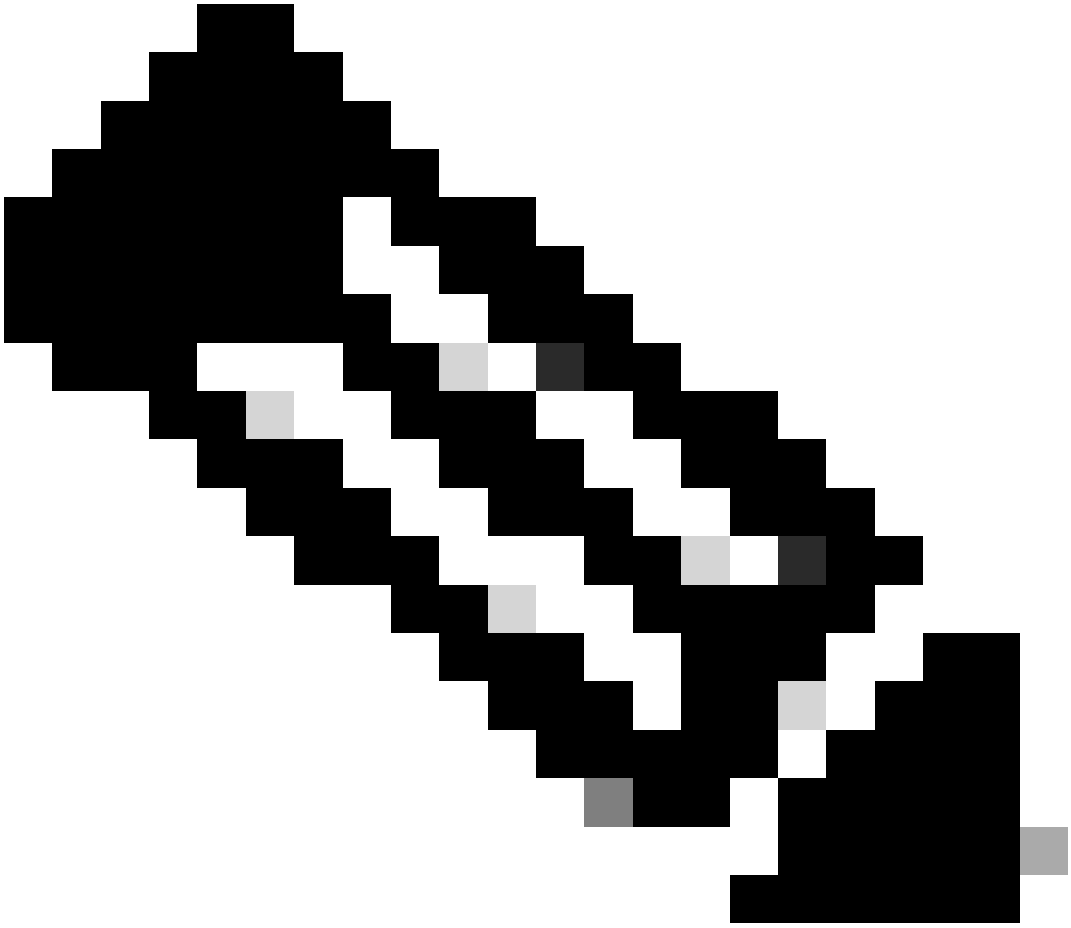
Klicken Sie gemäß der Regelaktion der benutzerdefinierten Zielregel auf Pro Angriffsrichtlinie.




Regelaktion ändern

Geben Sie im Bildschirm Edit Rule Action (Regelaktion bearbeiten) die Informationen für die Richtlinie und die Regelaktion ein.

- Richtlinie: snort_test
- Regelaktion: BLOCKIEREN



Hinweis: Regelaktionen sind:

Block (Blockieren): Generiert ein Ereignis, blockiert das aktuell übereinstimmende Paket und alle nachfolgenden Pakete in dieser Verbindung.

Warnung - Generiert nur Ereignisse für übereinstimmende Pakete und verwirft keine Pakete oder Verbindungen.

Rewrite (Umschreiben) - Generiert Ereignis und überschreibt Paketinhalt basierend auf der Ersetzungsoption in der Regel.

Pass (Übergeben) - Es werden keine Ereignisse generiert. Das Paket kann ohne weitere Evaluierung durch nachfolgende Snort-Regeln übergeben werden.

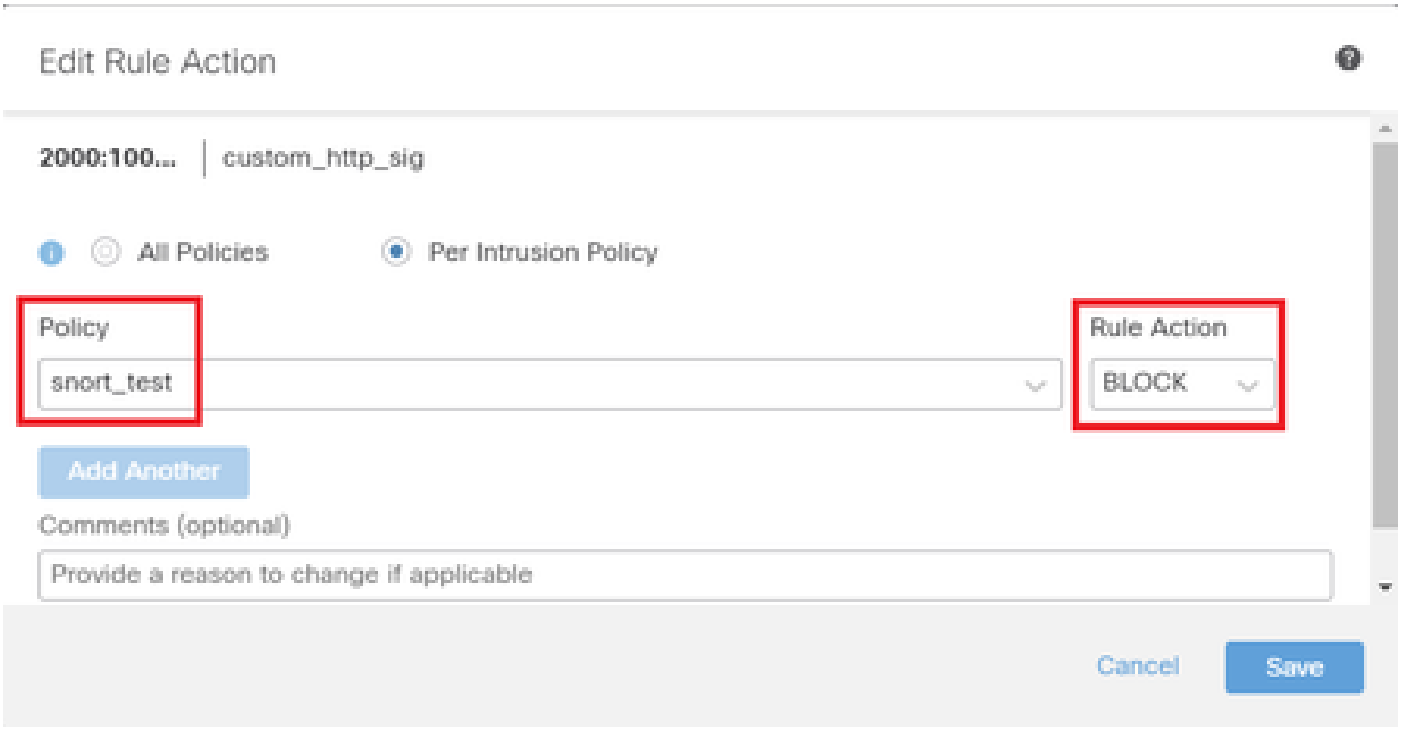
Drop - Generiert Ereignis, verwirft passendes Paket und blockiert keinen weiteren Datenverkehr in dieser Verbindung.

Reject (Ablehnen) - Erzeugt ein Ereignis, verwirft passende Pakete, blockiert weiteren Datenverkehr in dieser Verbindung und sendet TCP-Reset, wenn es sich um ein TCP-

Protokoll handelt, an Quell- und Zielhosts.

Disable (Deaktivieren): Der Datenverkehr wird nicht mit dieser Regel abgeglichen. Es werden keine Ereignisse generiert.

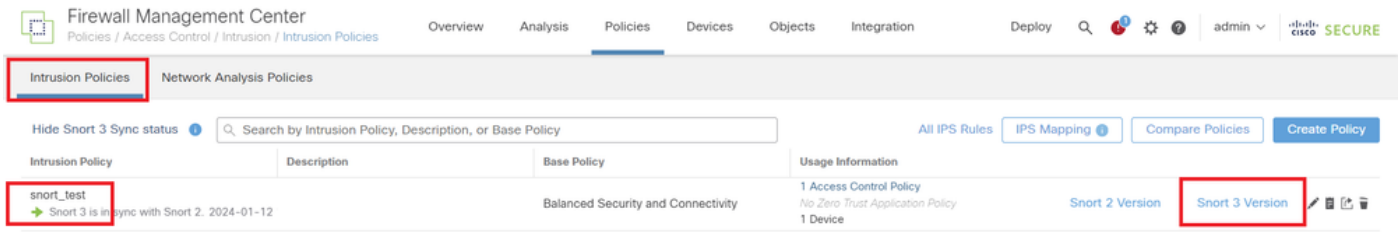
Default (Standard) - Stellt die Standardaktion des Systems wieder her.




Regelaktion bearbeiten

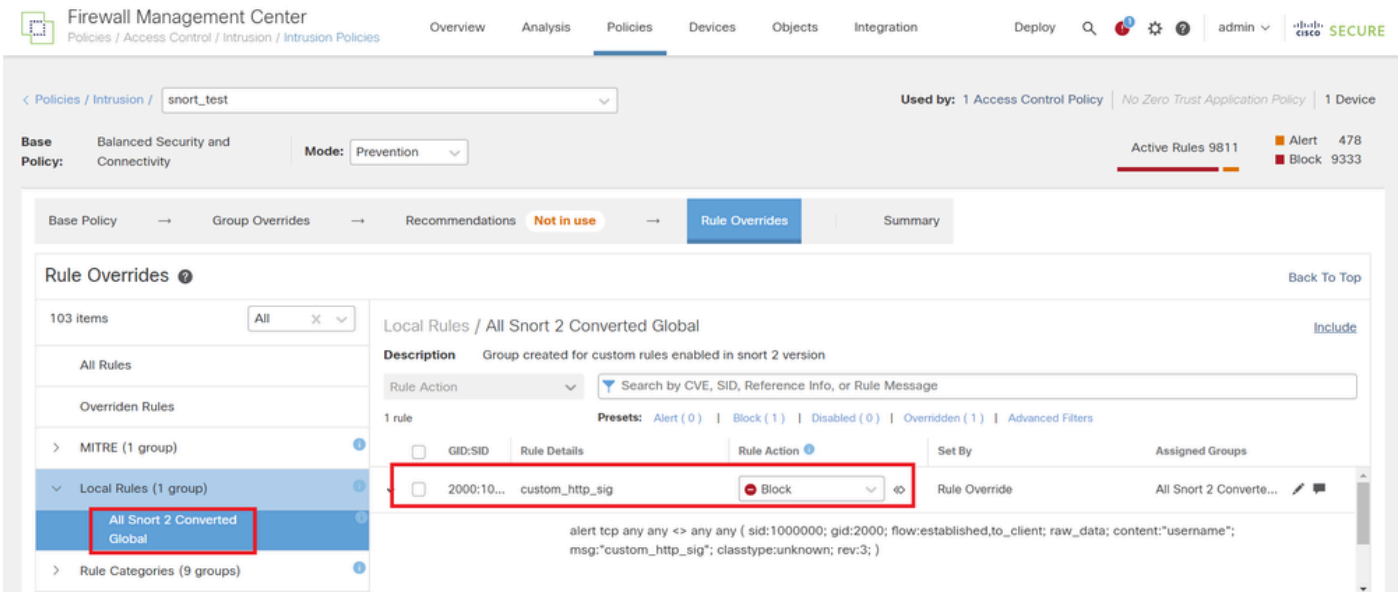
Schritt 5: Importierte benutzerdefinierte lokale Snort-Regel bestätigen

Navigieren Sie zu Policies > Intrusion Policies auf FMC, und klicken Sie auf Snort 3 Version, die der gewünschten Intrusion Policy in der Zeile entspricht.




Importierte benutzerdefinierte Regel bestätigen

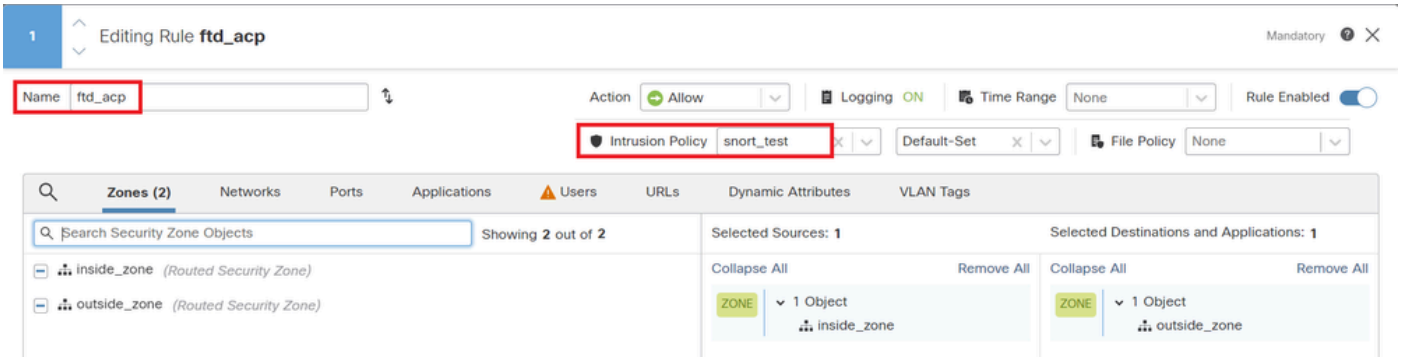
Klicken Sie auf Local Rules > All Snort 2 Converted Global, um die Details der benutzerdefinierten lokalen Snort-Regel zu überprüfen.




Importierte benutzerdefinierte Regel bestätigen

Schritt 6: Zuordnen einer Richtlinie für Sicherheitsrisiken zur Zugriffskontrollrichtlinie (ACP)

Navigieren Sie zu Policies>Access Control FMC, und ordnen Sie Intrusion Policy dem ACP zu.




Mit AKP-Regel verknüpfen

Schritt 7. Änderungen bereitstellen

Stellen Sie die Änderungen auf FTD ein.


Änderungen bereitstellen

## Methode 2. Lokale Datei hochladen

Schritt 1: Snort-Version bestätigen

Wie Schritt 1 in Methode 1.

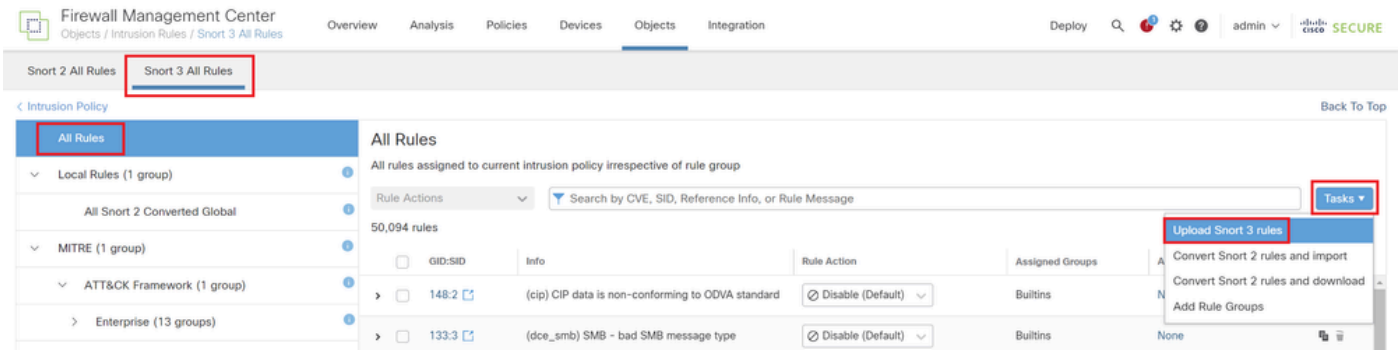
Schritt 2: Erstellen einer benutzerdefinierten lokalen Snort-Regel

Erstellen Sie manuell eine benutzerdefinierte lokale Snort-Regel, und speichern Sie sie in einer lokalen Datei mit dem Namen custom-rules.txt.

```
alert tcp any any <> any any ( sid:1000000; flow:established,to_client; raw_data; content:"username"; m
```

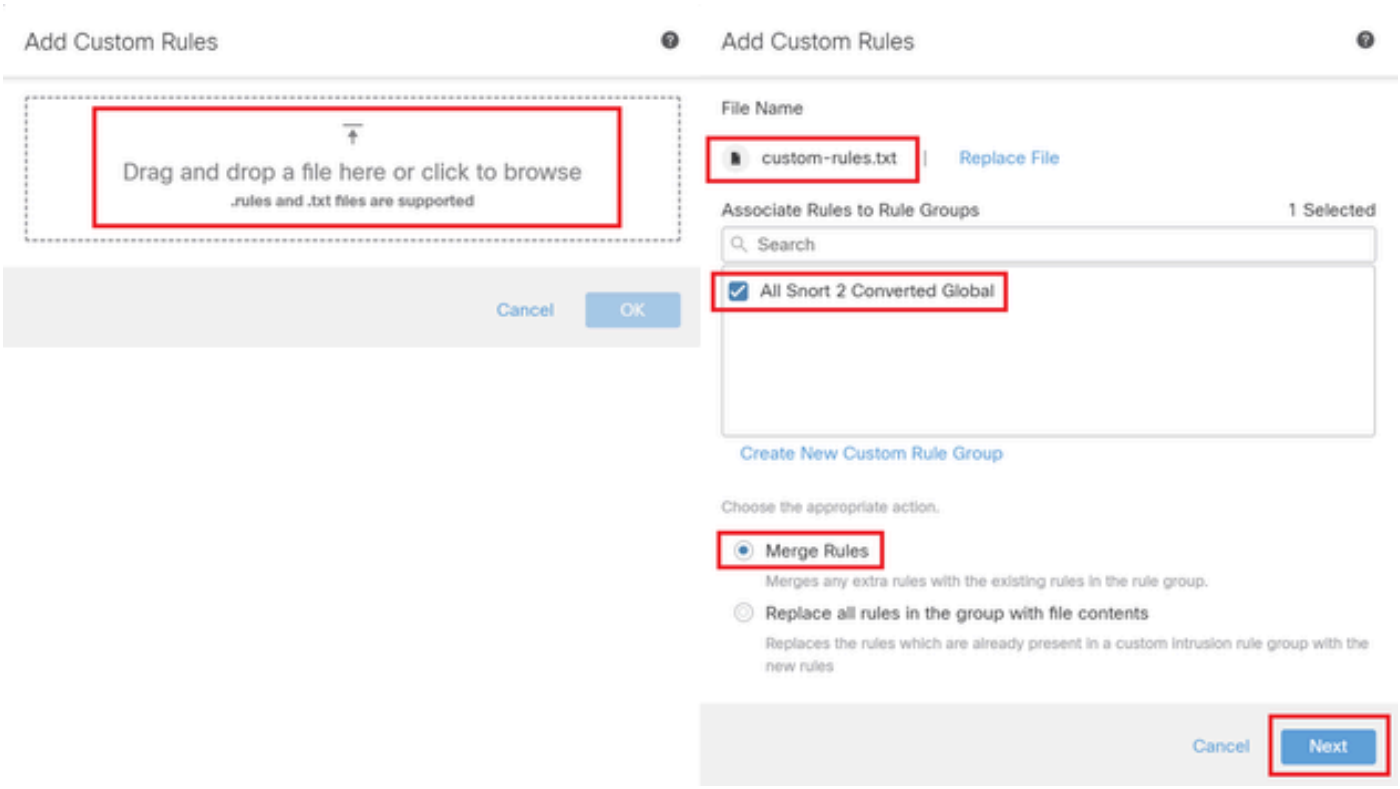
Schritt 3: Benutzerdefinierte lokale Snort-Regel hochladen

Navigieren Sie zu Objekte > Intrusion Rules > Snort 3 All Rules > All Rules on FMC, und klicken Sie auf Upload Snort 3 rules from Tasks Pulldown list.



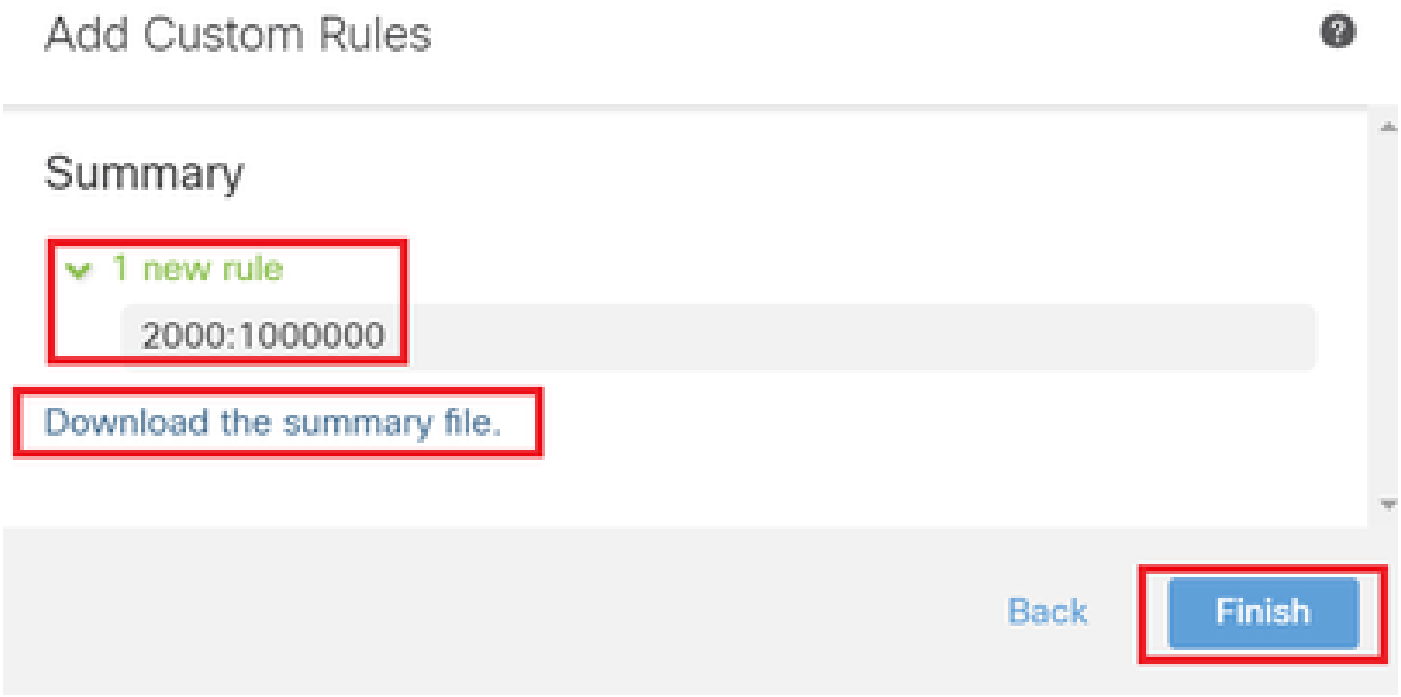

Benutzerdefinierte Regel hochladen

Ziehen Sie im Bildschirm Benutzerdefinierte Regeln hinzufügen die lokale Datei custom-rules.txt, legen Sie die Regelgruppen und die entsprechende Aktion (in diesem Beispiel Regeln zusammenführen) fest, und klicken Sie dann auf die Schaltfläche Weiter.



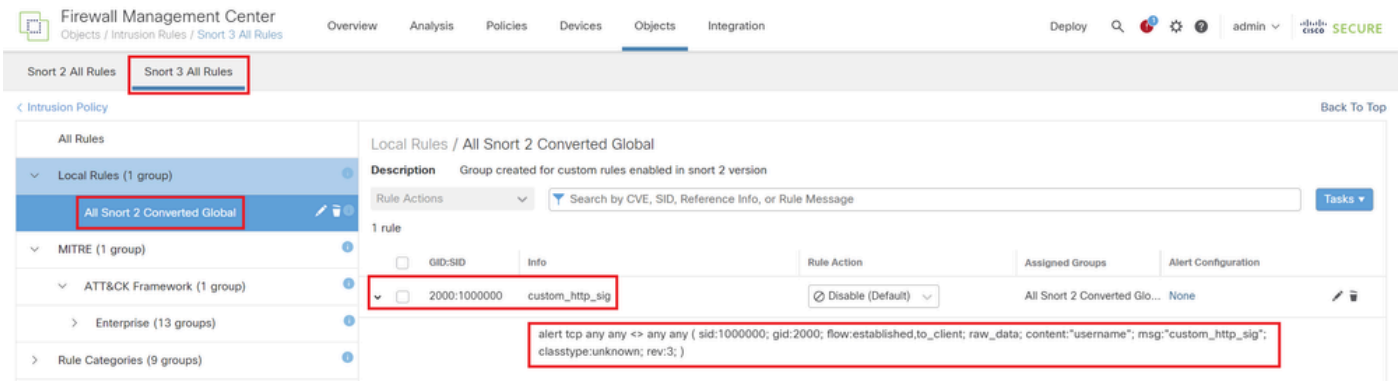

Benutzerdefinierte Regel hinzufügen

Bestätigen Sie, dass die lokale Regeldatei erfolgreich hochgeladen wurde.




Uploadergebnis bestätigen

Navigieren Sie zu Objects > Intrusion Rules > Snort 3 All Rules on FMC, und klicken Sie auf All Snort 2 Converted Global, um die hochgeladene benutzerdefinierte lokale Snort-Regel zu bestätigen.




Detail der benutzerdefinierten Regel

Schritt 4: Regelaktion ändern

Wie Schritt 4 in Methode 1.

Schritt 5: Hochgeladene benutzerdefinierte lokale Snort-Regel bestätigen

Wie Schritt 5 in Methode 1.

Schritt 6: Zuordnen einer Richtlinie für Sicherheitsrisiken zur Zugriffskontrollrichtlinie (ACP)

Wie Schritt 6 in Methode 1.

Schritt 7. Änderungen bereitstellen

Wie Schritt 7 in Methode 1.

# Überprüfung

Schritt 1: Festlegen des Inhalts der Datei auf dem HTTP-Server

Legen Sie den Inhalt der Datei test.txt auf der Seite des HTTP-Servers auf username fest.

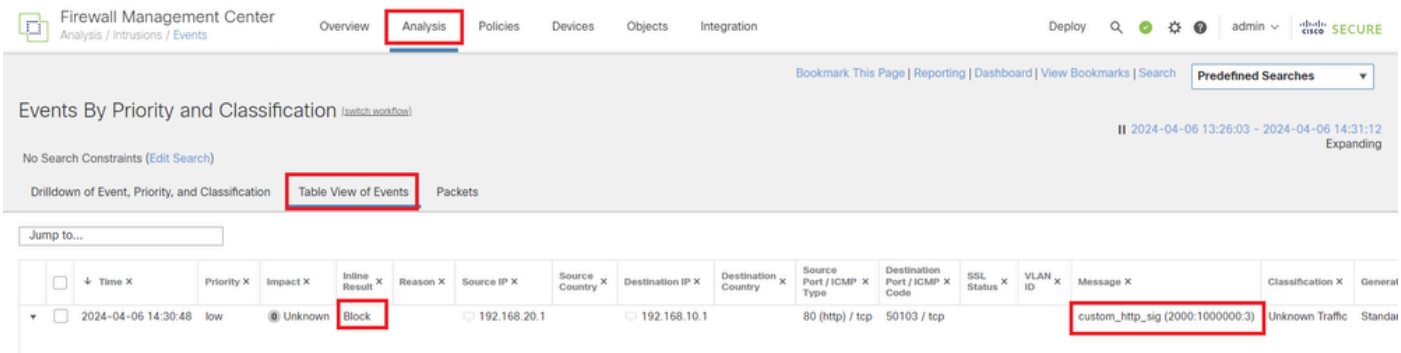
Schritt 2: Erste HTTP-Anfrage

Greifen Sie vom Browser des Clients (192.168.10.1) auf den HTTP-Server (192.168.20.1/test.txt) zu, und bestätigen Sie, dass die HTTP-Kommunikation blockiert ist.


Erste HTTP-Anfrage

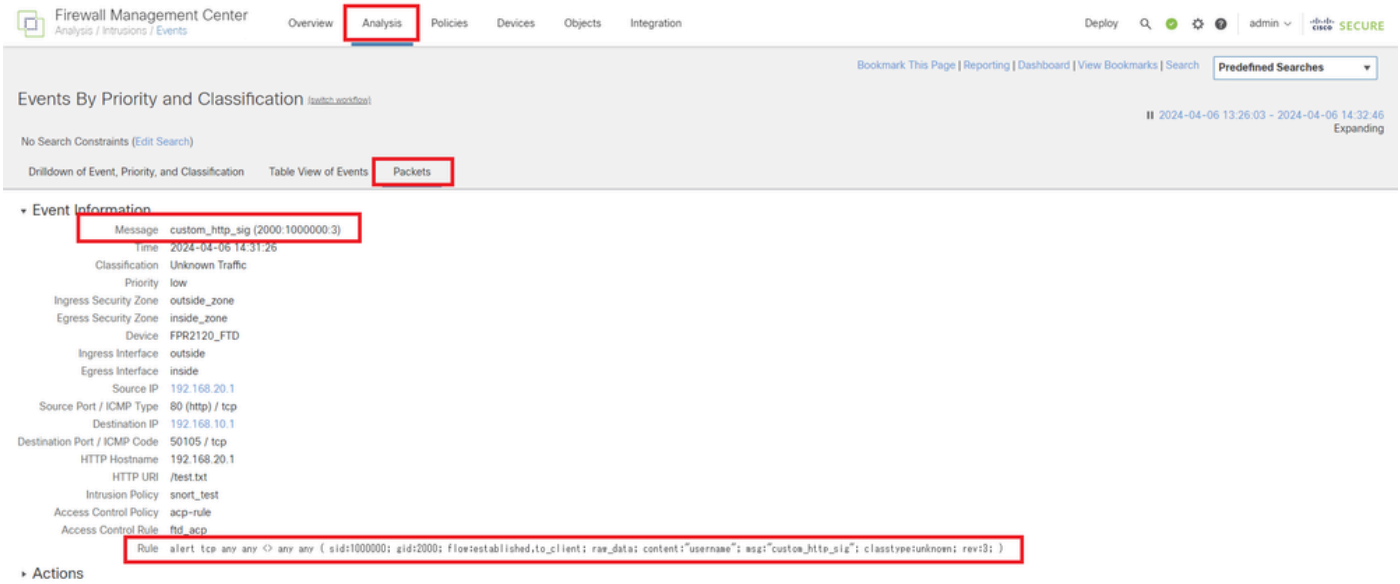
Schritt 3: Angriffsereignis bestätigen

Navigieren Sie zuAnalysis>Intrusions>EventIn FMC, und bestätigen Sie, dass das Intrusion-Ereignis von der benutzerdefinierten lokalen Snort-Regel generiert wird.




Intrusion-Ereignis

ClickPacketTabelle, überprüfen Sie die Details des Angriffsereignisses.




Details des Angriffsereignisses

# Häufig gestellte Fragen

F: Welche Empfehlung erhalten Sie, Snort 2 oder Snort 3?
A : Verglichen mit Snort 2 bietet Snort 3 verbesserte Verarbeitungsgeschwindigkeiten und neue Funktionen, was es zu der empfohlenen Option macht.

F : Wird nach dem Upgrade von einer FTD-Version vor 7.0 auf eine Version 7.0 oder höher die Snort-Version automatisch auf Snort 3 aktualisiert?
A : Nein, die Prüfungs-Engine läuft weiterhin auf Snort 2. Um Snort 3 nach dem Upgrade zu verwenden, müssen Sie es explizit aktivieren. Beachten Sie, dass Snort 2 in einer zukünftigen Version veraltet sein soll, und es wird dringend empfohlen, die Verwendung von Snort 2 jetzt einzustellen.

F: Ist es in Snort 3 möglich, eine bestehende benutzerdefinierte Regel zu bearbeiten?
A : Nein, Sie können es nicht bearbeiten. Um eine bestimmte benutzerdefinierte Regel zu bearbeiten, müssen Sie die entsprechende Regel löschen und neu erstellen.

# Fehlerbehebung

Führen Sie einen Befehl aus`system support trace`, um das Verhalten auf FTD zu bestätigen. In diesem Beispiel wird der HTTP-Datenverkehr durch die IPS-Regel (2000:1000000:3) blockiert.

```
<#root>

>

system support trace


Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
```

```
Please specify a client IP address: 192.168.10.1
Please specify a client port:
Please specify a server IP address: 192.168.20.1
Please specify a server port:

192.168.10.1 50104 -> 192.168.20.1 80 6 AS=0 ID=4 GR=1-1 Firewall: allow rule, '
```

**ftd_acp**

```
', allow

192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1
```

**Event**

```
:
```

**2000:1000000:3**

```
, Action
```

**block**

```
192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict: blacklist
192.168.20.1 80 -> 192.168.10.1 50103 6 AS=0 ID=4 GR=1-1 Verdict Reason:
```

**ips, block**

Referenz

Konfigurationsleitfaden für Cisco Secure Firewall Management Center Snort 3

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.