Benutzerdefinierte lokale Snort-Regeln in Snort2 auf FTD konfigurieren

Inhalt

Einleitung

In diesem Dokument wird das Verfahren zur Konfiguration benutzerdefinierter lokaler Snort-Regeln in Snort2 auf dem FTD (Firewall Threat Defense) 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:

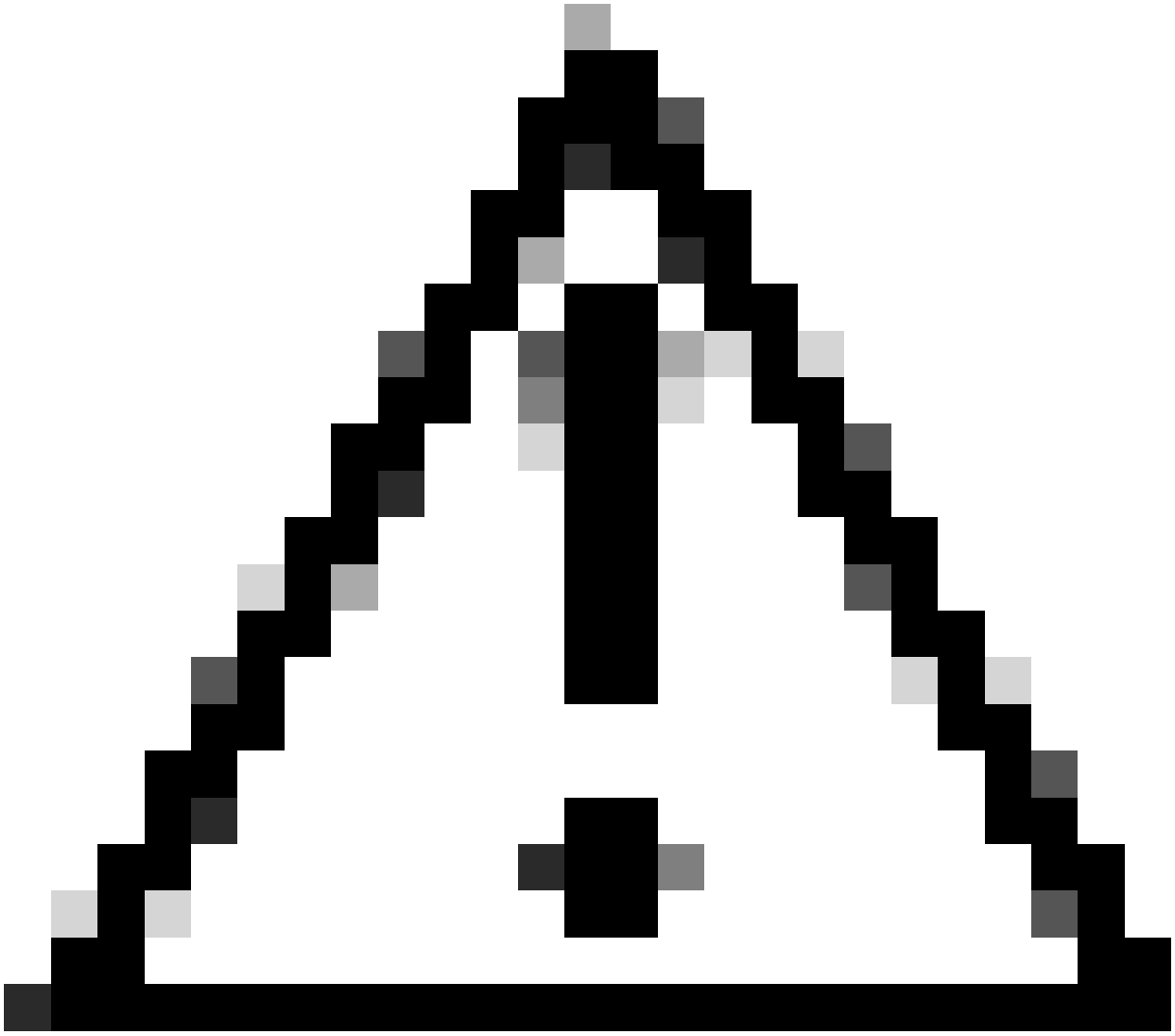
- Cisco FirePOWER Management Center für VMware 7.4.1
- Cisco FirePOWER 2120 7.4.1

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

Benutzerdefinierte lokale Snort-Regel bezieht sich auf eine benutzerdefinierte Regel, die Sie innerhalb des Snort Intrusion Detection and Prevention Systems erstellen und implementieren können, das in die FTD integriert ist. Wenn Sie eine benutzerdefinierte lokale Snort-Regel in Cisco FTD erstellen, definieren Sie im Wesentlichen ein neues Muster oder eine Reihe von Bedingungen, auf die die Snort-Engine achten kann. Wenn der Netzwerkverkehr die in der benutzerdefinierten Regel festgelegten Bedingungen erfüllt, kann Snort die in der Regel definierte Aktion ausführen, z. B. eine Warnung generieren oder das Paket verwerfen. Administratoren verwenden benutzerdefinierte lokale Snort-Regeln, um bestimmte Bedrohungen zu bekämpfen, die nicht von den allgemeinen Regelsätzen abgedeckt werden.

In diesem Dokument wird erläutert, wie Sie eine benutzerdefinierte lokale Snort-Regel konfigurieren und überprüfen, die zum Erkennen und Verwerfen von HTTP-Antwortpaketen mit einer bestimmten Zeichenfolge (Benutzername) entwickelt wurde.

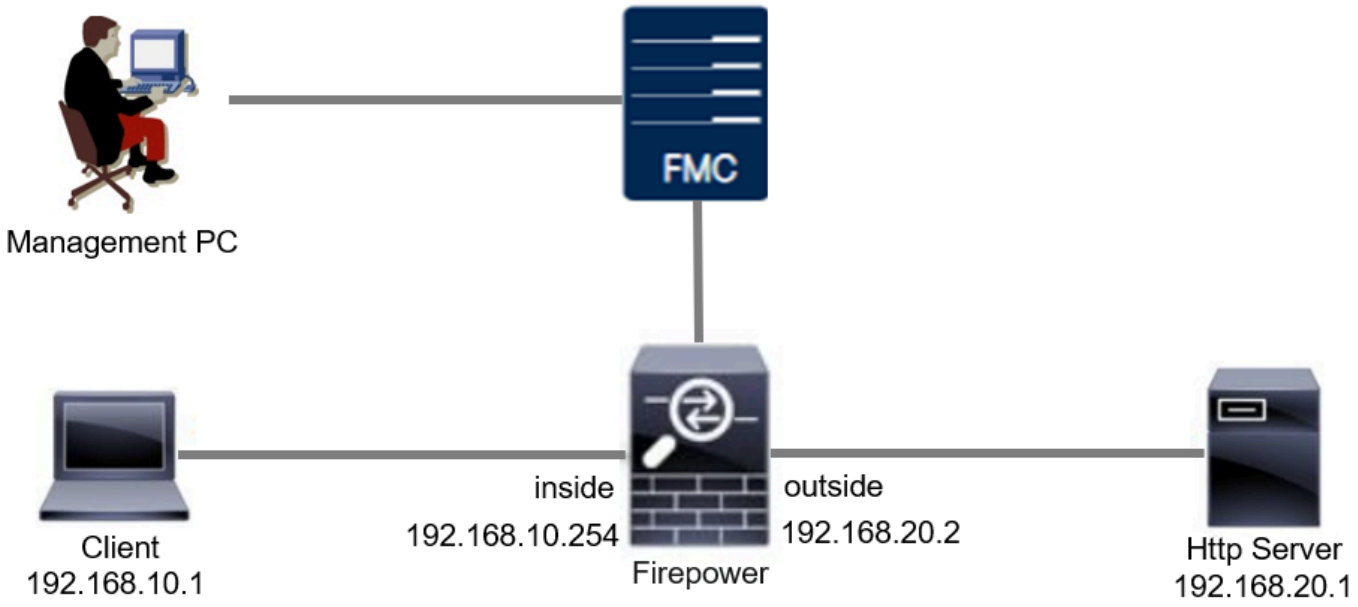


Vorsicht: Das Erstellen benutzerdefinierter lokaler Snort-Regeln und die Bereitstellung von Support hierfür fallen nicht unter den TAC-Support. Daher kann dieses Dokument nur als Referenz verwendet werden und Sie bitten, diese benutzerdefinierten Regeln nach eigenem Ermessen und mit eigener Verantwortung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

Konfigurieren

Netzwerkdiagramm

In diesem Dokument wird die Konfiguration und Überprüfung der benutzerdefinierten lokalen Snort-Regel in Snort2 in diesem Diagramm vorgestellt.

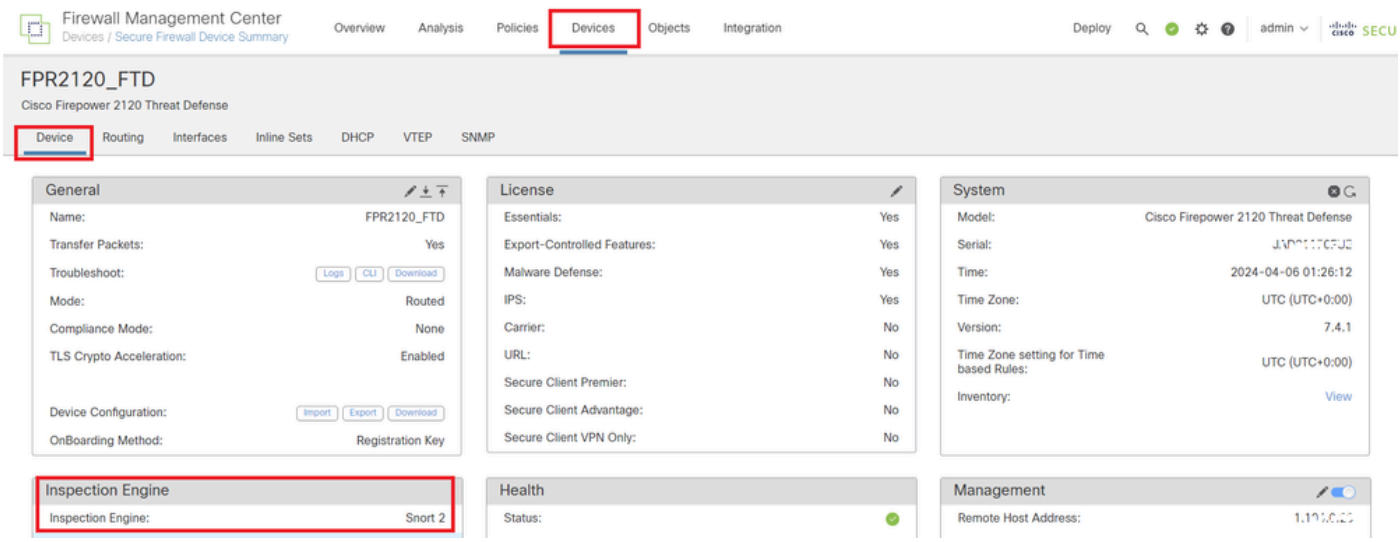


Konfiguration

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

Schritt 1: Snort-Version bestätigen

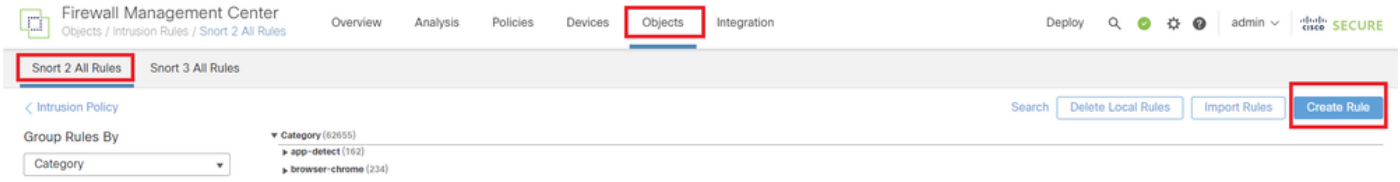
Navigieren Sie zu Geräte > Geräteverwaltung auf FMC, und klicken Sie auf die Registerkarte Gerät. Bestätigen Sie, dass die Snort-Version Snort2 ist.



Snort-Version

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

Navigieren Sie zu Objekte > Intrusion Rules > Snort 2 All Rules on FMC, und klicken Sie auf Create Rule (Regel erstellen).

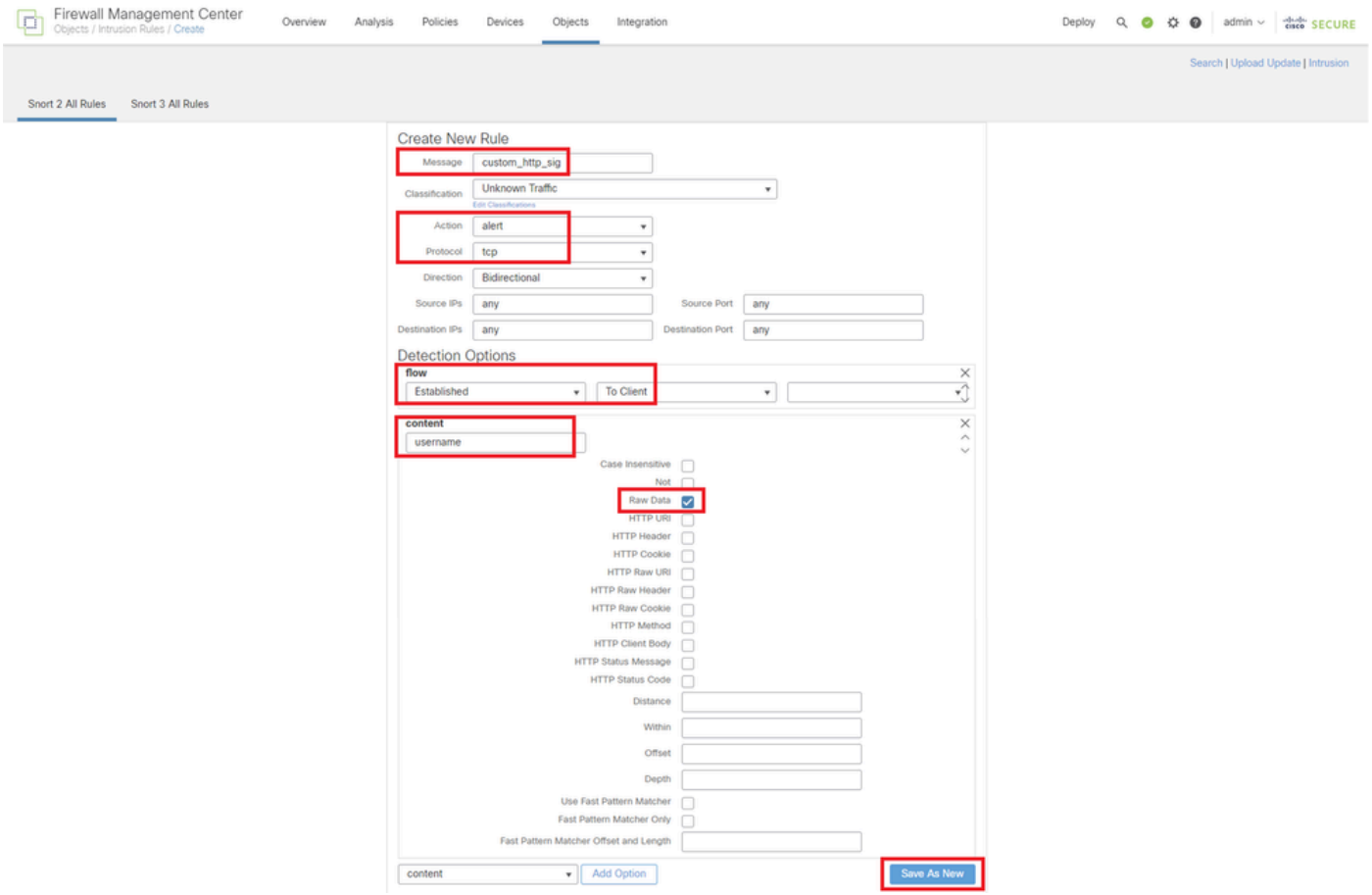


Benutzerdefinierte Regel erstellen

Geben Sie die erforderlichen Informationen für die benutzerdefinierte lokale Snort-Regel ein.

- Eindringen: custom_http_sig
- Aktion: alert
- Protokoll: TCP
- Fluss: etabliert, an Client

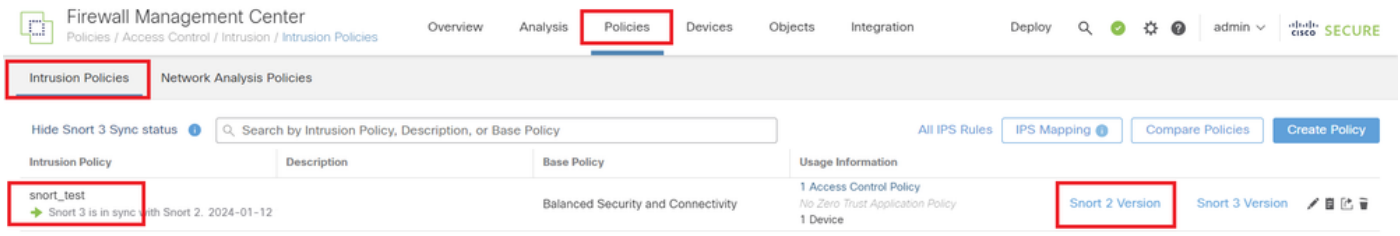
- Inhalt : Benutzername (Rohdaten)



Eingabe der erforderlichen Informationen für Regel

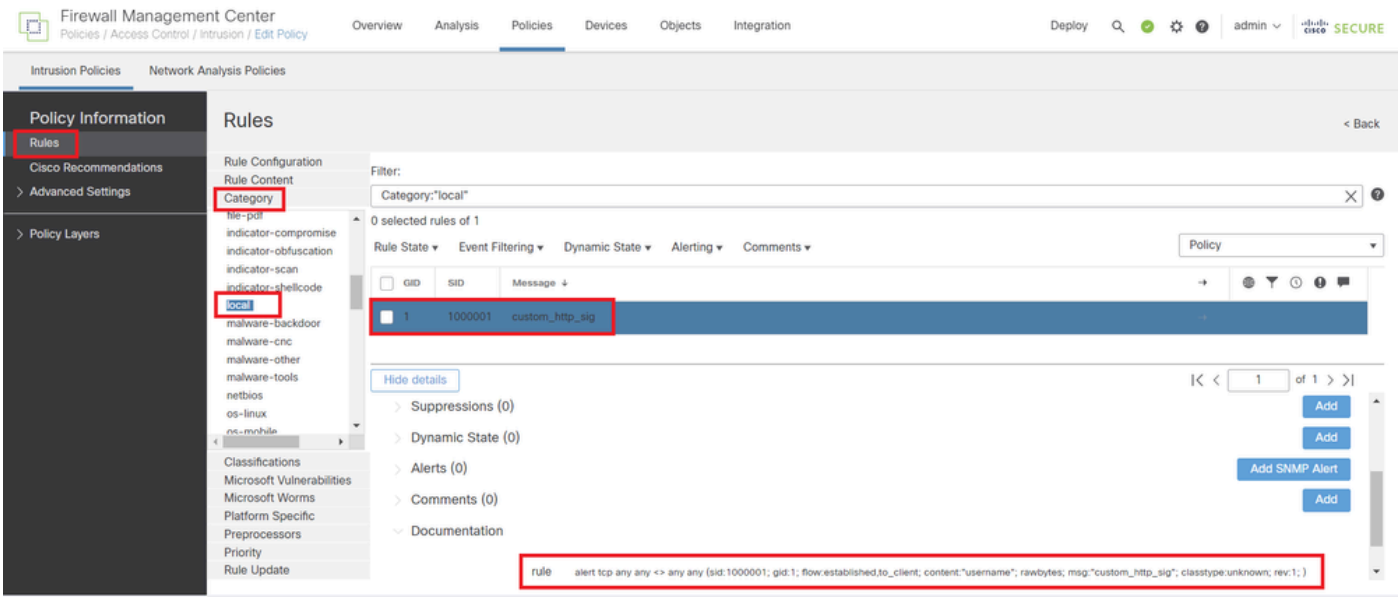
Schritt 3: Benutzerdefinierte lokale Snort-Regel bestätigen

Navigieren Sie zu Policies > Intrusion Policies on FMC, und klicken Sie auf die Schaltfläche Snort 2 Version.



Benutzerdefinierte Regel bestätigen

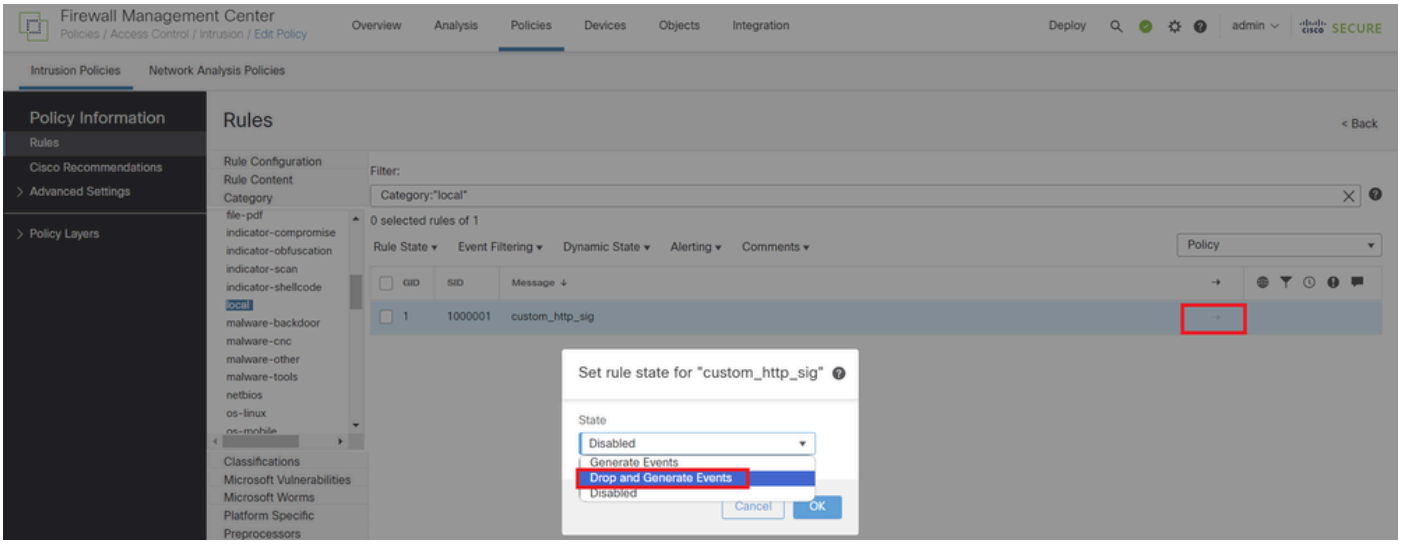
Navigieren Sie zu Regeln > Kategorie > lokal auf FMC, und bestätigen Sie die Details der benutzerdefinierten lokalen Snort-Regel.



Detail der benutzerdefinierten Regel

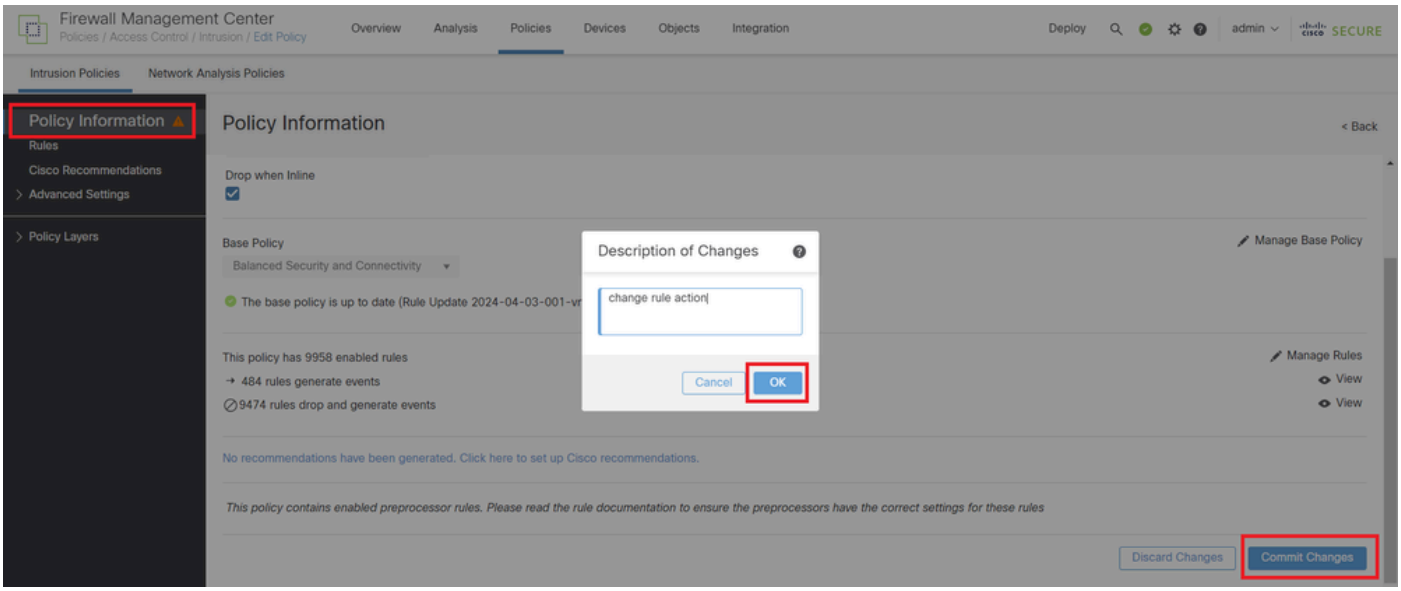
Schritt 4: Regelaktion ändern

Klicken Sie auf die Schaltfläche State (Status), legen Sie den Status auf Drop and Generate Events (Löschen und Generieren von Ereignissen) fest, und klicken Sie auf die Schaltfläche OK.



Ändern der Regelaktion

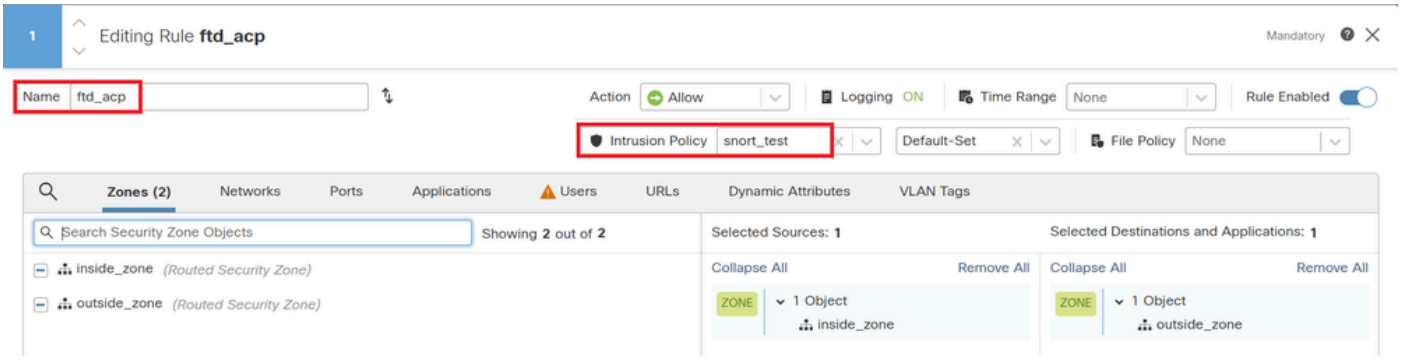
Klicken Sie auf die Schaltfläche "Richtlinieninformationen" und dann auf die Schaltfläche "Änderungen bestätigen", um die Änderungen zu speichern.



Änderungen bestätigen

Schritt 5: Zuordnen einer Richtlinie für Sicherheitsrisiken zur Zugriffskontrollrichtlinie (ACP)

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



Mit AKP-Regel verknüpfen

Schritt 6: Änderungen bereitstellen

Stellen Sie die Änderungen auf FTD ein.

Änderungen bereitstellen

Überprüfung

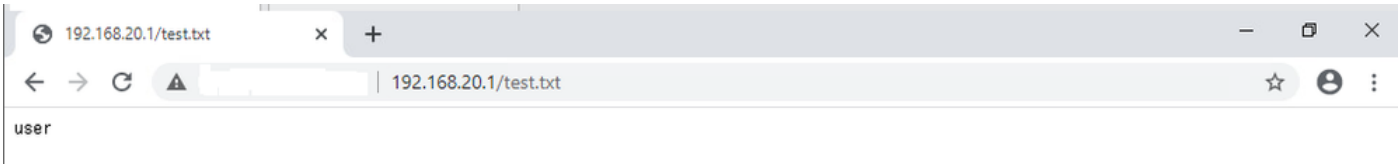
Benutzerdefinierte lokale Snort-Regel wird nicht ausgelöst

Schritt 1: Festlegen des Inhalts der Datei im HTTP-Server

Legen Sie den Inhalt der Datei test.txt auf der Seite des HTTP-Servers auf user 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 zulässig ist.



Erste HTTP-Anfrage

Benutzerdefinierte lokale Snort-Regel wird ausgelöst

Schritt 1: Festlegen des Inhalts der Datei im HTTP-Server

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

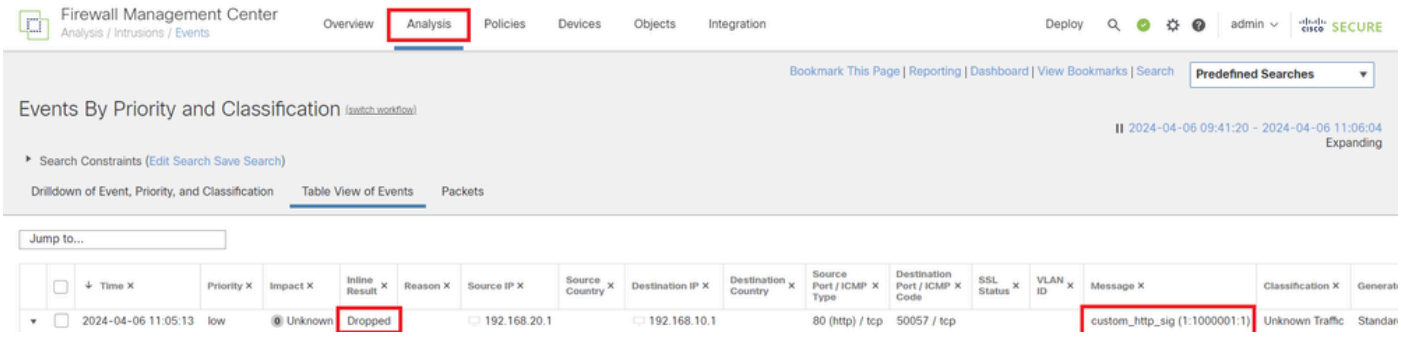
Schritt 2: Erste HTTP-Anfrage

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

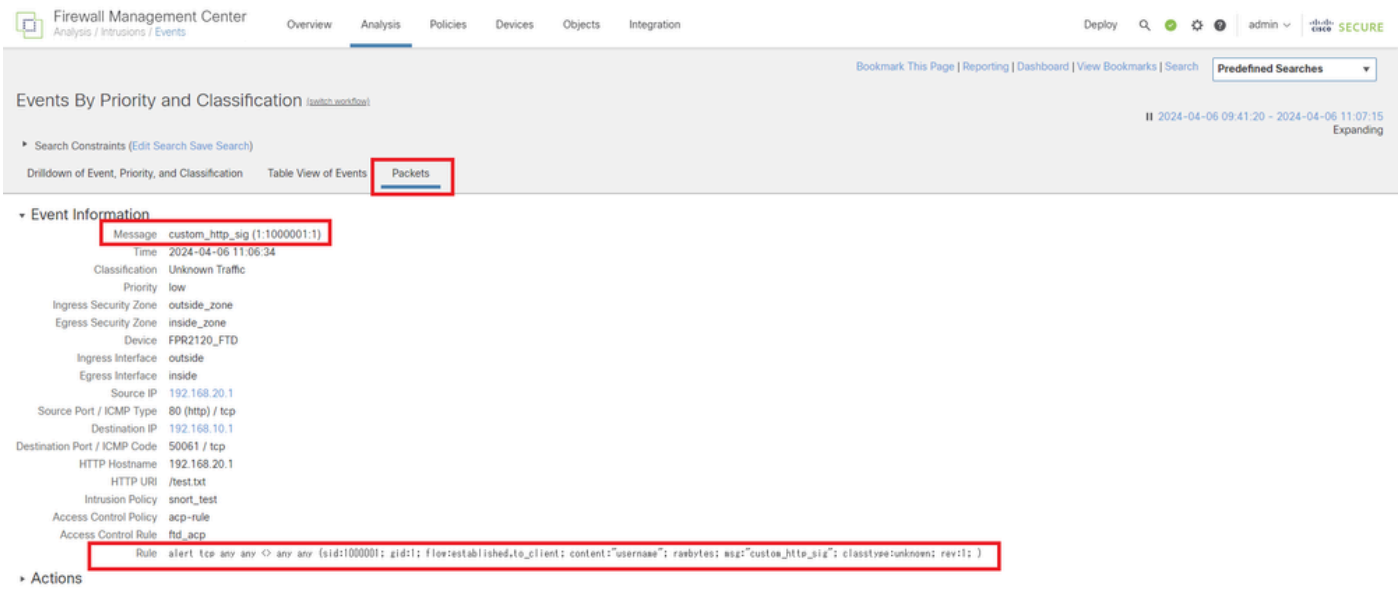
Schritt 3: Angriffsereignis bestätigen

Navigieren Sie zu Analyse > Sicherheitsrisiken > Ereignisse in FMC, und bestätigen Sie, dass das Sicherheitsverletzungsereignis von der benutzerdefinierten lokalen Snort-Regel generiert wird.



Intrusion-Ereignis

Klicken Sie auf die Registerkarte Packets, und bestätigen Sie die Details des Angriffsereignisses.



Details des Angriffsereignisses

Fehlerbehebung

Führen Sie einen Befehl ausSystem support trace, um das Verhalten auf FTD zu bestätigen. In diesem Beispiel wird der HTTP-Datenverkehr durch die IPS-Regel blockiert (gid 1, sid 1000001).

<#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:

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Firewall: allow rule, '
```

ftd_acp

', allow
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0

IPS Event

:

gid 1

,

sid 1000001

, drop

192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 Snort id 3, NAP id 2, IPS id 1, Verdict BLOCKFLOW
192.168.20.1-80 - 192.168.10.1-50075 6 AS 1-1 CID 0 ===>

Blocked by IPS

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.