# Configura regole personalizzate di snort locale in Snort2 su FTD

## Sommario



## Introduzione

In questo documento viene descritta la procedura per configurare le regole di snort locali personalizzate in Snort2 on Firewall Threat Defense (FTD).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Firepower Management Center (FMC)
- Firewall Threat Defense (FTD)

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

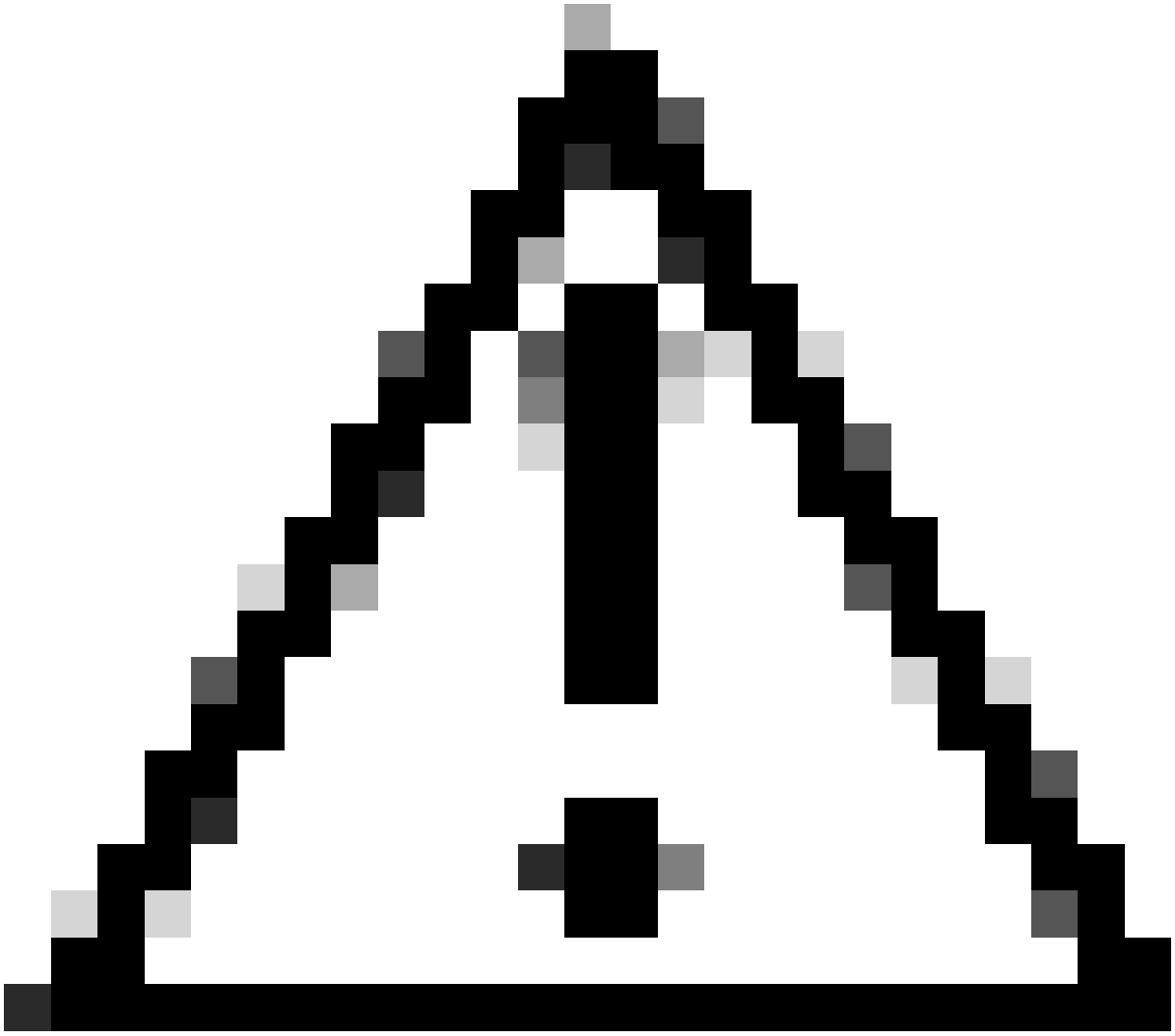
- Cisco Firepower Management Center per VMWare 7.4.1
- Cisco Firepower 2120 7.4.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

Custom Local Snort Rule si riferisce a una regola definita dall'utente che è possibile creare e implementare all'interno del sistema di rilevamento e prevenzione delle intrusioni Snort integrato nel FTD. Quando si crea una regola Snort locale personalizzata in Cisco FTD, si definisce essenzialmente un nuovo pattern o set di condizioni che il motore Snort è in grado di osservare. Se il traffico di rete soddisfa le condizioni specificate nella regola personalizzata, Snort può eseguire l'azione definita nella regola, ad esempio generare un avviso o eliminare il pacchetto. Gli amministratori utilizzano regole di tipo Snort locali personalizzate per gestire minacce specifiche non coperte dai set di regole generali.

In questo documento viene illustrato come configurare e verificare una regola di snort locale personalizzata progettata per rilevare ed eliminare pacchetti di risposta HTTP contenenti una stringa specifica (nome utente).

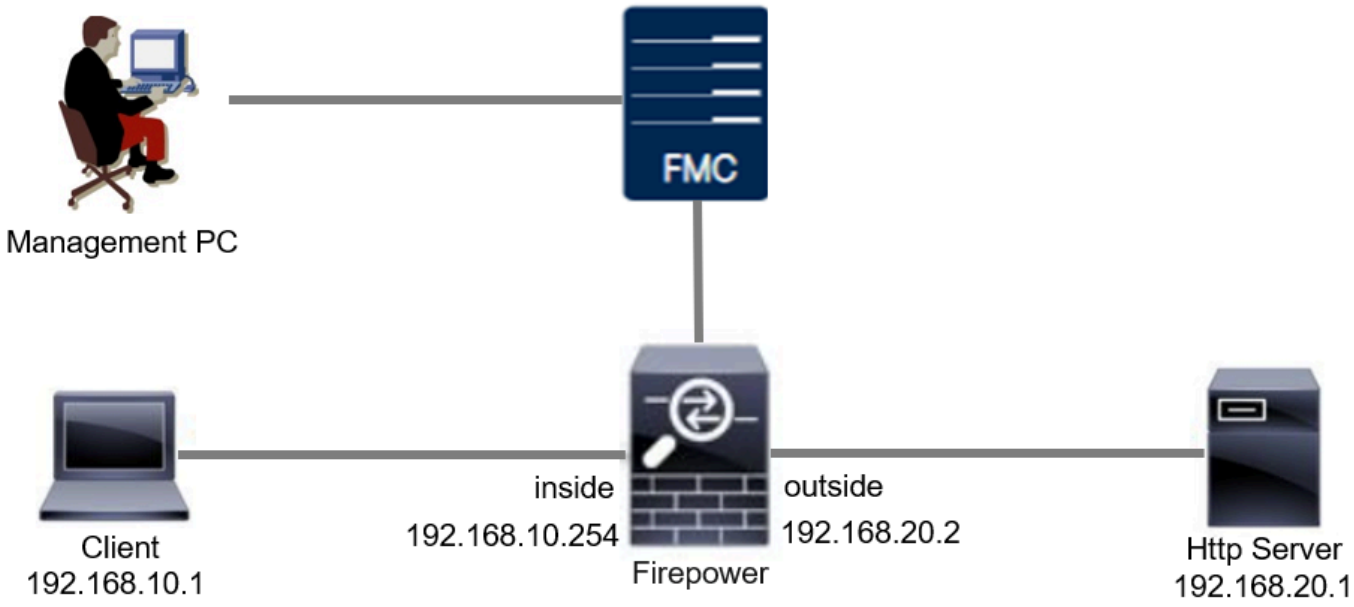


Attenzione: la creazione di regole personalizzate per lo snort locale e il relativo supporto esulano dalla copertura del supporto TAC. Pertanto, questo documento può essere utilizzato solo come riferimento e richiede la creazione e la gestione di queste regole personalizzate a propria discrezione e responsabilità.

# Configurazione

## Esempio di rete

In questo documento viene illustrata la configurazione e la verifica della Regola snort locale personalizzata in Snort2 nel diagramma.

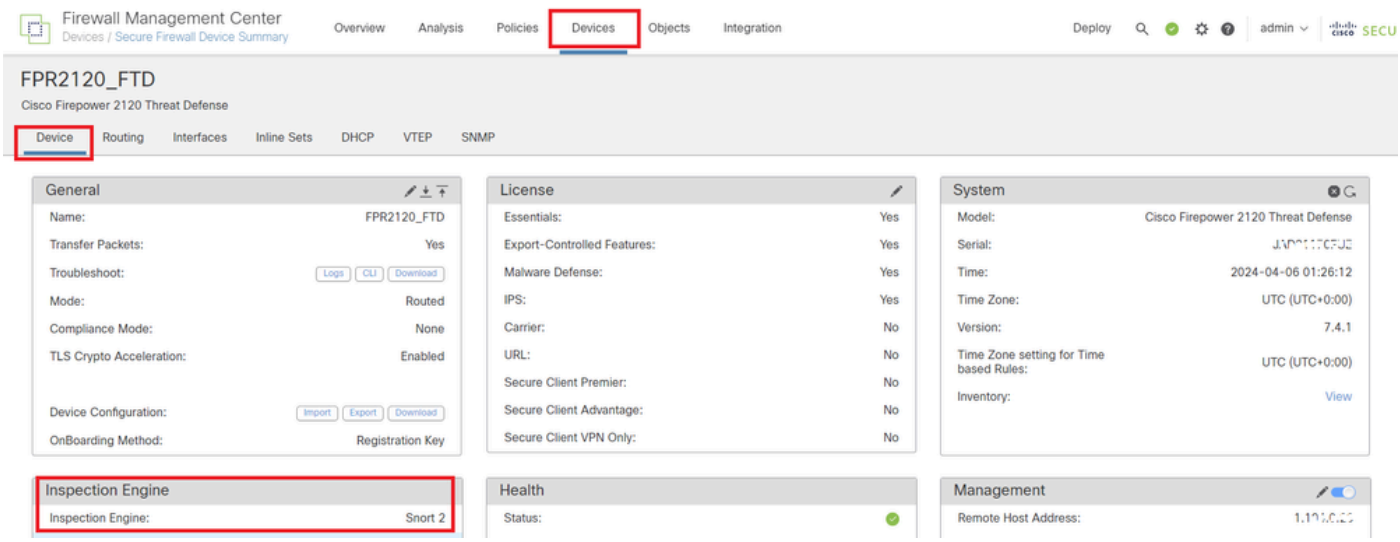



## Configurazione

Questa è la configurazione di Custom Local Snort Rule per rilevare ed eliminare i pacchetti di risposta HTTP contenenti una stringa specifica (nome utente).

Passaggio 1. Conferma versione snort

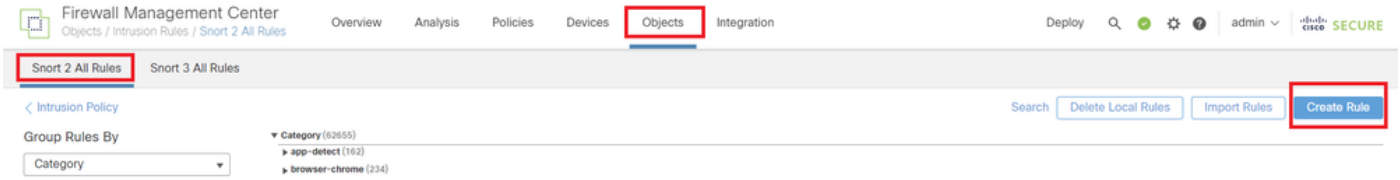
Selezionare Dispositivi > Gestione dispositivi in FMC, quindi fare clic su scheda Dispositivo. Confermare la versione snort è Snort2.




Versione snort

Passaggio 2. Creare una regola personalizzata per l'orientamento locale nell'angolo 2

Selezionare Oggetti > Regole intrusione > Ordina 2 tutte le regole in FMC, quindi fare clic sul pulsante Crea regola.

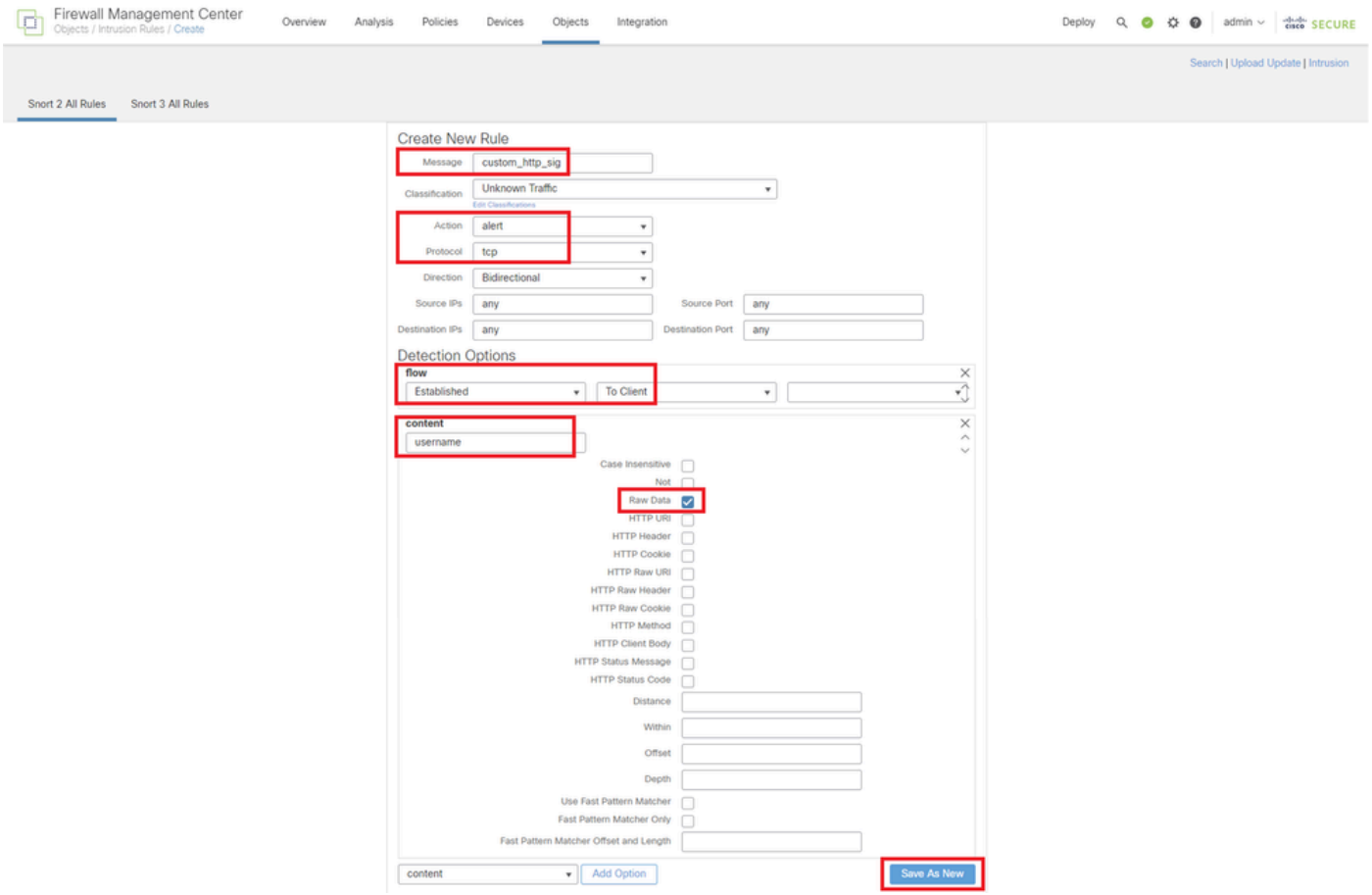



Crea regola personalizzata

Immettere le informazioni necessarie per la Regola snort locale personalizzata.

- Intrusione : custom_http_sig
- Azione : avviso
- Protocollo : tcp
- flusso : stabilito, al client

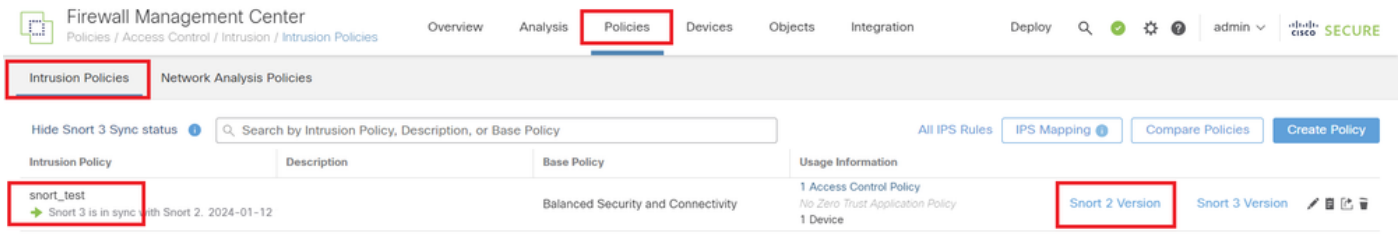
- content : nomeutente (dati non elaborati)




Inserisci le informazioni necessarie per la regola

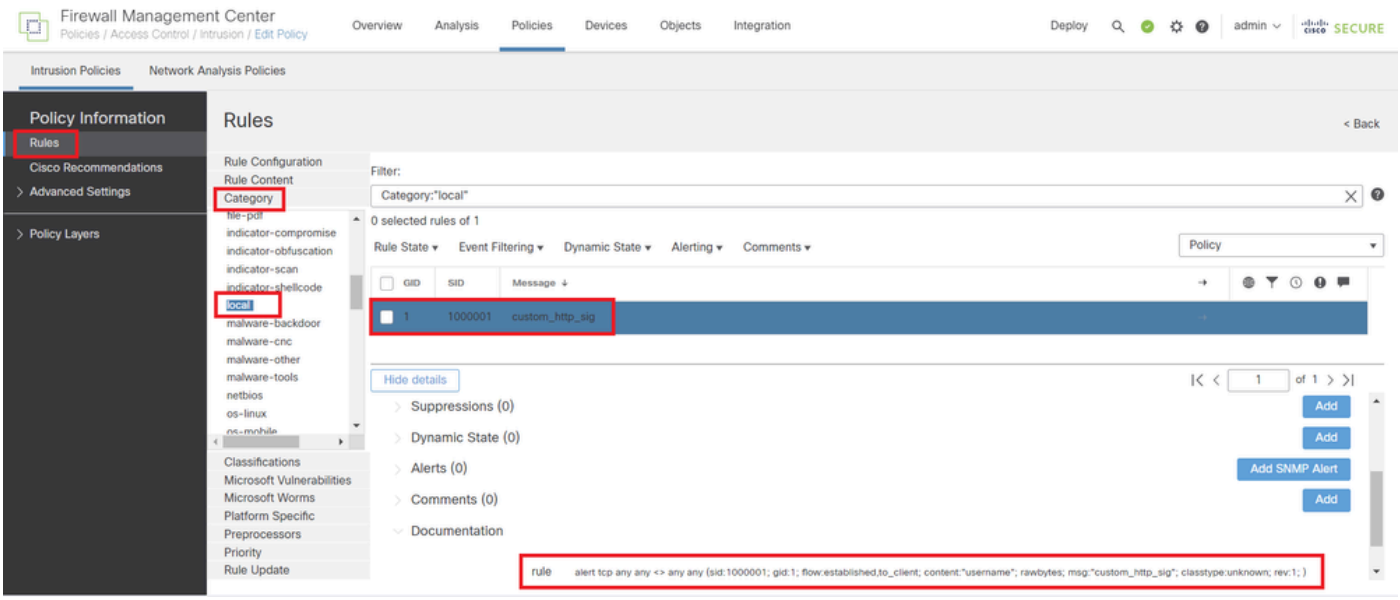
Passaggio 3. Conferma regola snort locale personalizzata

Selezionare Policies > Intrusion Policies on FMC (Policy > Intrusion Policies su FMC), quindi fare clic sul pulsante Snort 2 Version (Avvia versione).




Conferma regola personalizzata

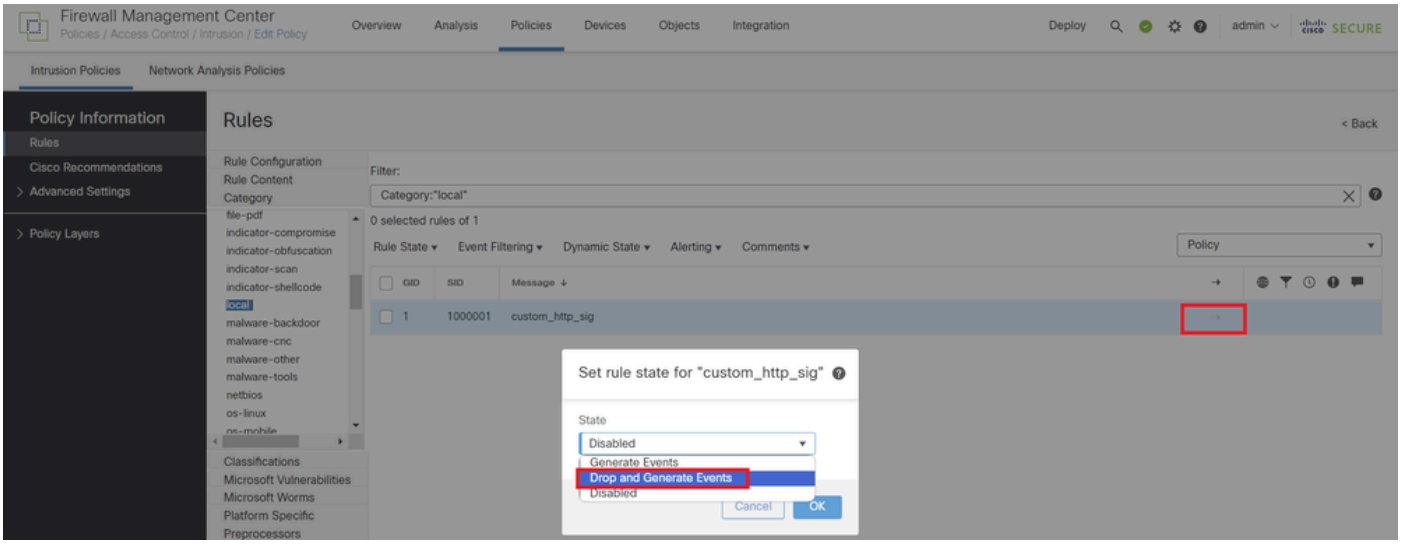
Passare a Regole > Categoria > locale in FMC, confermare i dettagli di Regola snort locale personalizzata.




Dettaglio regola personalizzata

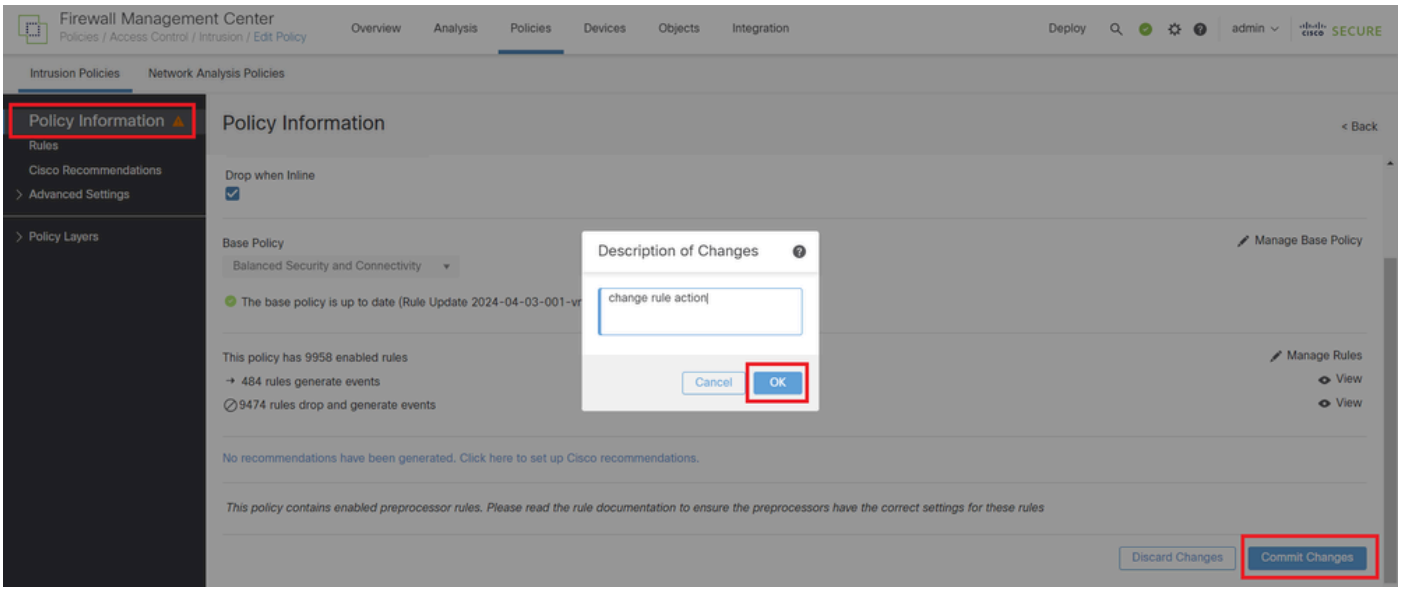
## Passaggio 4. Azione regola di modifica

Fare clic su pulsante Stato, impostare lo stato su Elimina e genera eventi e fare clic su OK pulsante.




Modifica azione regola

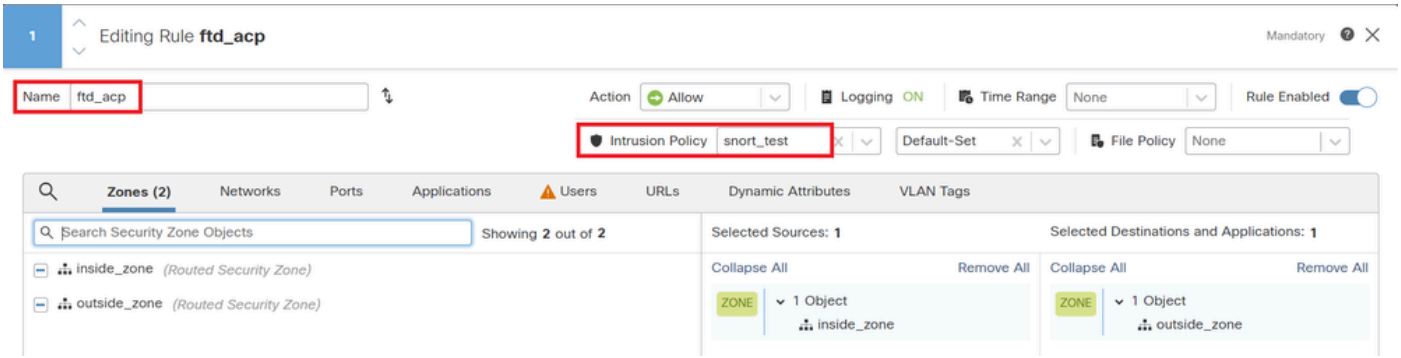
Fare clic su Informazioni criterio pulsante, fare clic su Conferma modifiche pulsante per salvare le modifiche.




Commit modifiche

Passaggio 5. Associa criterio di intrusione alla regola dei criteri di controllo di accesso (ACP)

Selezionare Policies > Access Control on FMC (Policy > Controllo di accesso su FMC), quindi Associare Intrusion Policy (Policy di intrusione) a ACP.




Associa a regola ACP

Passaggio 6. Distribuisci modifiche

Distribuire le modifiche in FTD.


Distribuisci modifiche

# Verifica

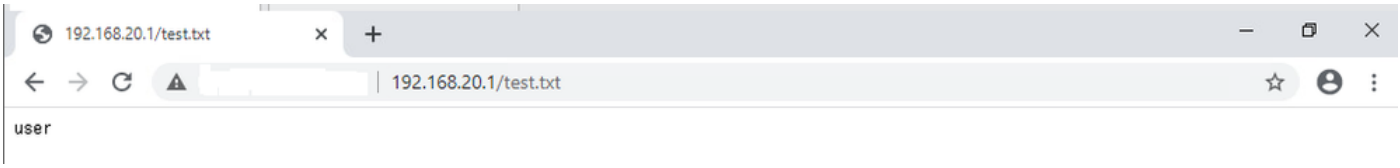
## Regola snort locale personalizzata non attivata

Passaggio 1. Imposta contenuto del file in HTTP Server

Impostare il contenuto del file test.txt sul lato server HTTP su user.

Passaggio 2. Richiesta HTTP iniziale

Accedere al server HTTP (192.168.20.1/test.txt) dal browser del client (192.168.10.1) e confermare che la comunicazione HTTP è consentita.




Richiesta HTTP iniziale

## Regola snort locale personalizzata attivata

Passaggio 1. Imposta contenuto del file in HTTP Server

Impostare il contenuto del file test.txt sul lato server HTTP su username.

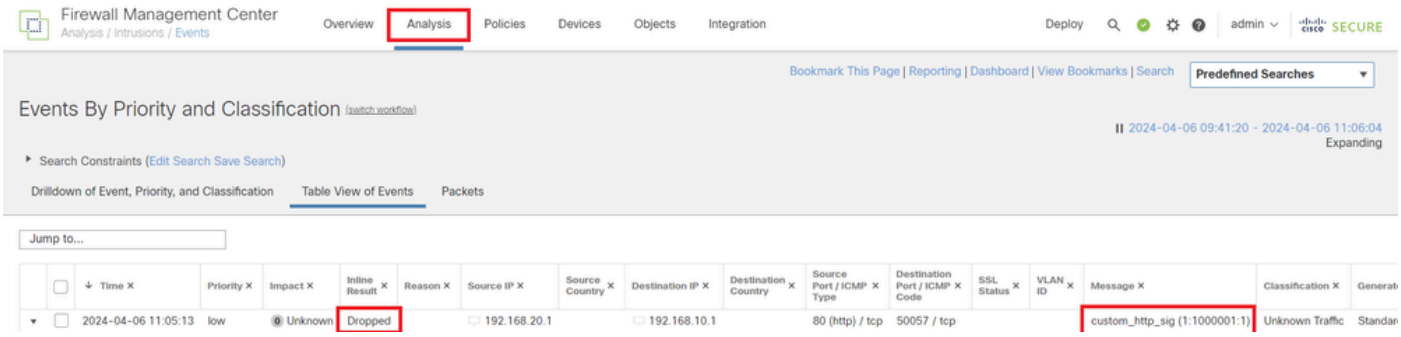
Passaggio 2. Richiesta HTTP iniziale

Accedere al server HTTP (192.168.20.1/test.txt) dal browser del client (192.168.10.1) e confermare che la comunicazione HTTP è bloccata.


Richiesta HTTP iniziale

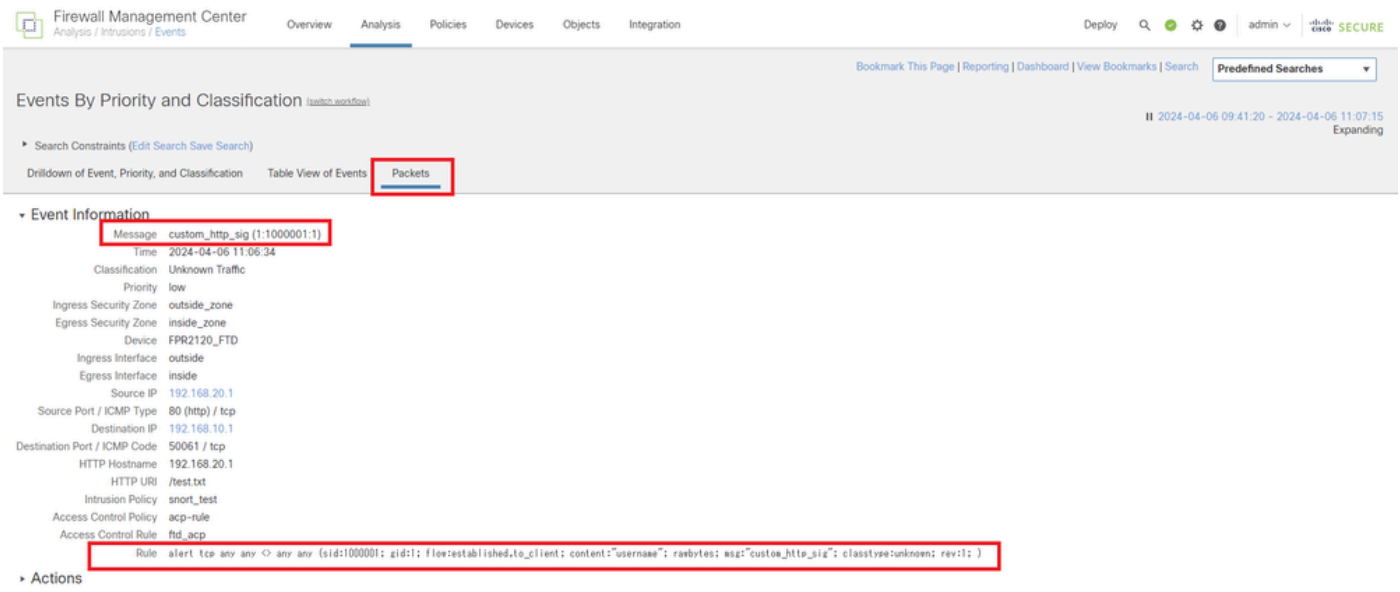
Passaggio 3. Conferma evento di intrusione

Passare ad Analisi > Intrusioni > Eventi in FMC, verificare che l'evento Intrusione sia generato dalla regola personalizzata di snort locale.




Evento Intrusion

Fare clic sulla scheda Packets, quindi confermare i dettagli di Intrusion Event.




Dettaglio dell'evento Intrusion

# Risoluzione dei problemi

Eseguire il comandosystem support trace per confermare il comportamento su FTD. Nell'esempio, il traffico HTTP è bloccato dalla regola IPS (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**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).