

Configura regole personalizzate di snort locale in Snort2 su FTD

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione](#)

[Passaggio 1. Conferma versione snort](#)

[Passaggio 2. Creare una regola personalizzata per l'orientamento locale nell'angolo 2](#)

[Passaggio 3. Conferma regola snort locale personalizzata](#)

[Passaggio 4. Azione regola di modifica](#)

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

[Passaggio 6. Distribuisci modifiche](#)

[Verifica](#)

[Regola snort locale personalizzata non attivata](#)

[Passaggio 1. Imposta contenuto del file nel server HTTP](#)

[Passaggio 2. Richiesta HTTP iniziale](#)

[Regola snort locale personalizzata attivata](#)

[Passaggio 1. Imposta contenuto del file nel server HTTP](#)

[Passaggio 2. Richiesta HTTP iniziale](#)

[Passaggio 3. ConfirmIntrusion_evento](#)

[Risoluzione dei problemi](#)

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:

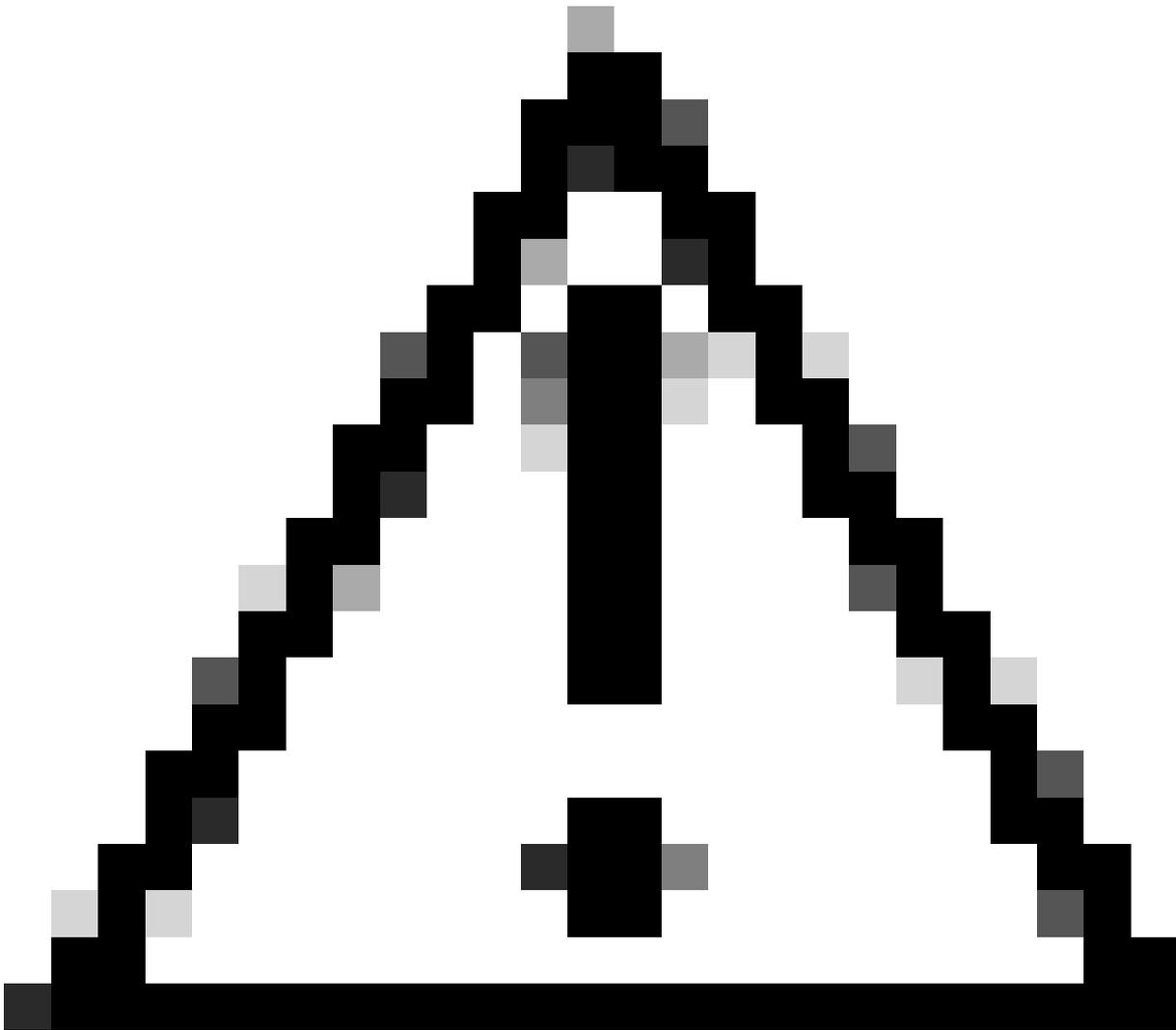
- Cisco Firepower Management Center per VMWare 7.4.1
- Cisco Firepower 2120 7.4.1

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).

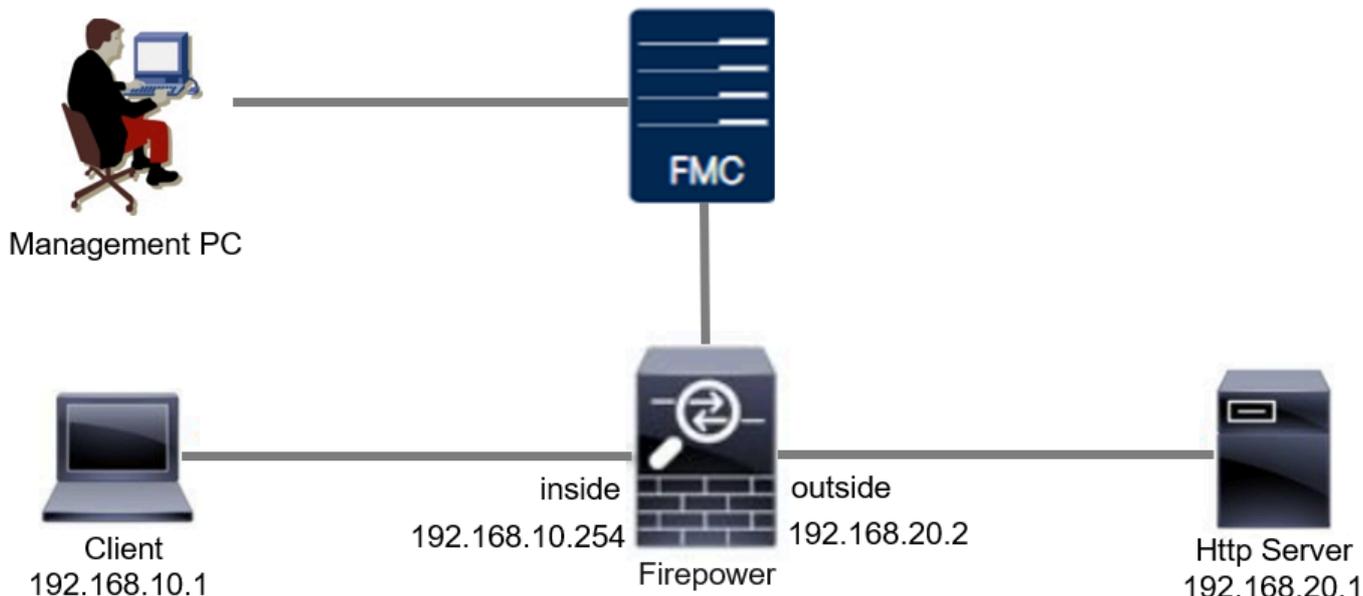


Attenzione: la creazione di regole personalizzate per lo snort locale e il relativo supporto esulano dalla copertura del supporto TAC. Pertanto, questo documento può essere utilizzato solo come riferimento e richiede la creazione e la gestione di queste regole personalizzate a propria discrezione e responsabilità.

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.

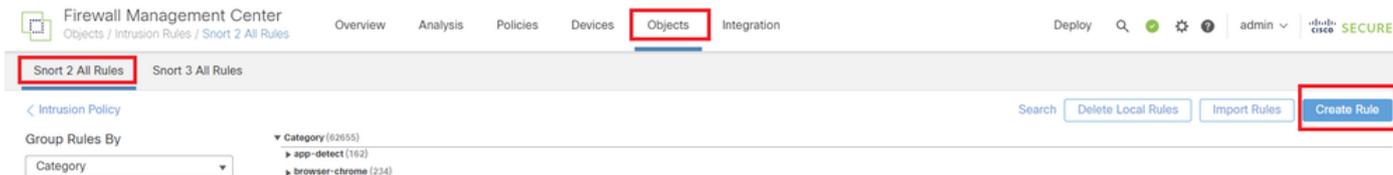
The screenshot shows the Cisco Firewall Management Center interface for device 'FPR2120_FTD'. The 'Devices' tab is selected. The configuration is as follows:

Section	Parameter	Value
General	Name:	FPR2120_FTD
	Transfer Packets:	Yes
	Troubleshoot:	Logs CLI Download
	Mode:	Routed
	Compliance Mode:	None
	TLS Crypto Acceleration:	Enabled
	OnBoarding Method:	Registration Key
License	Essentials:	Yes
	Export-Controlled Features:	Yes
	Malware Defense:	Yes
	IPS:	Yes
	Carrier:	No
	URL:	No
	Secure Client Premier:	No
System	Model:	Cisco Firepower 2120 Threat Defense
	Time:	2024-04-06 01:26:12
	Time Zone:	UTC (UTC+0:00)
Inspection Engine	Inspection Engine:	Snort 2
	Health Status:	Green
	Management Remote Host Address:	1.1.1.1

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.

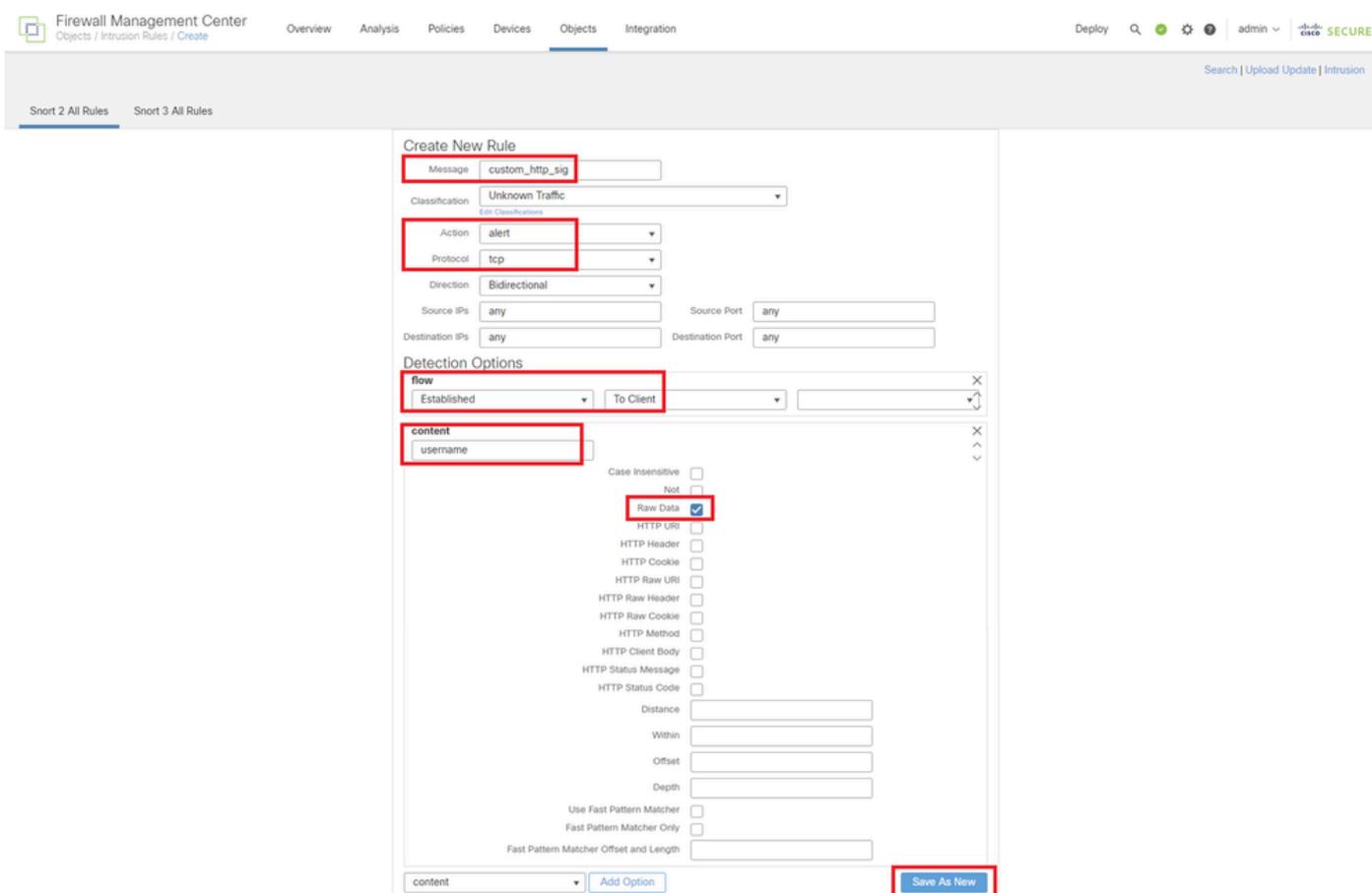


Crea regola personalizzata

Immettere le informazioni necessarie per la Regola snort locale personalizzata.

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

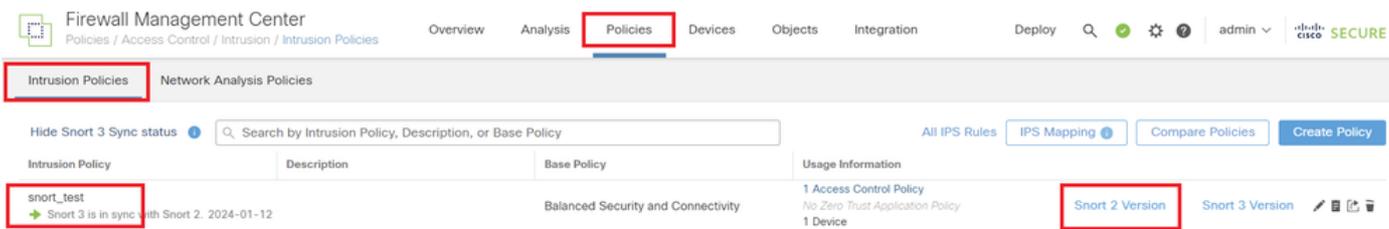
- content : nomeutente (dati non elaborati)



Inserisci le informazioni necessarie per la regola

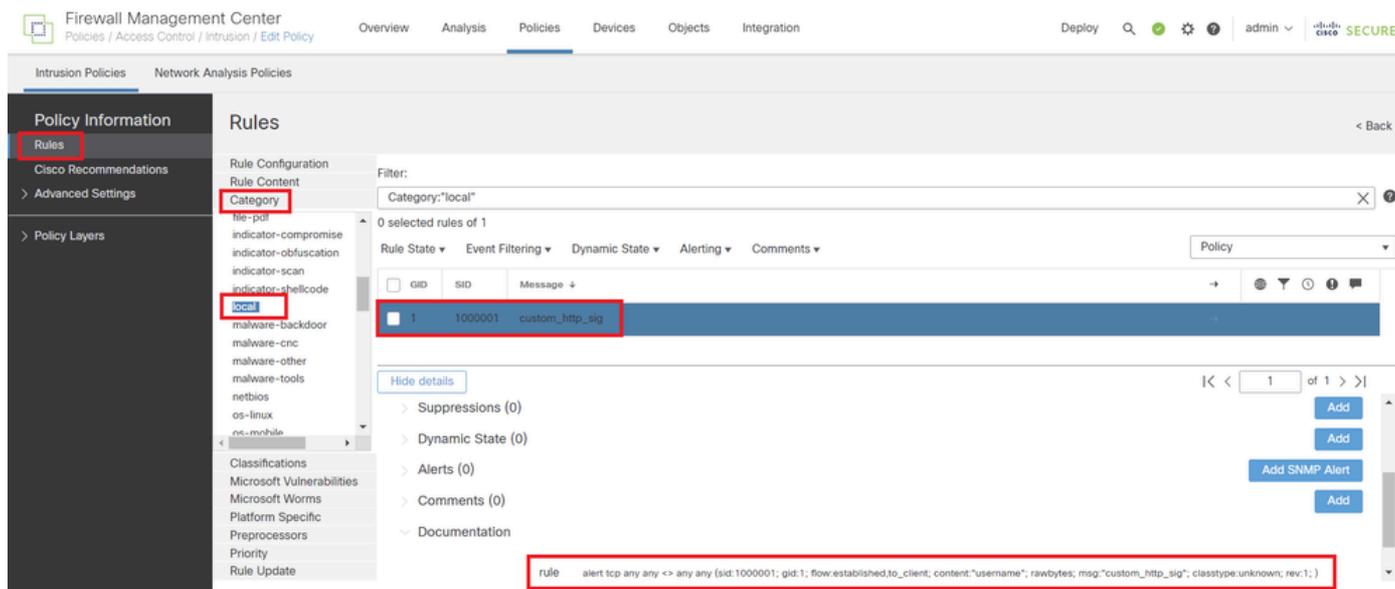
Passaggio 3. Conferma regola snort locale personalizzata

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



Conferma regola personalizzata

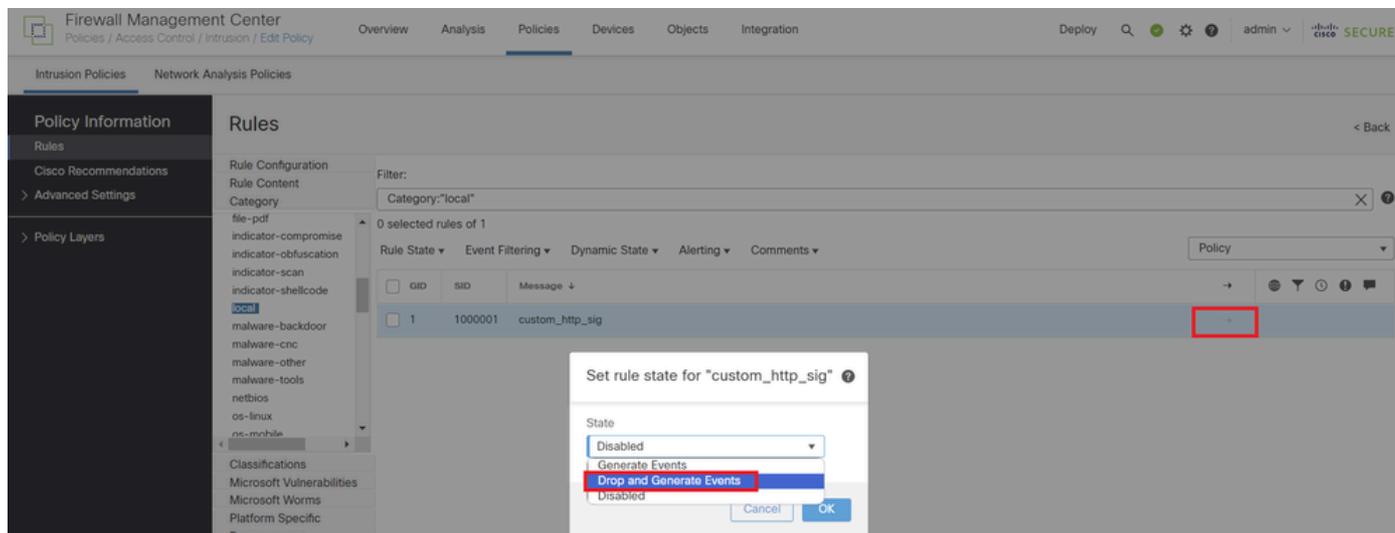
Passare a Regole > Categoria > locale in FMC, confermare i dettagli di Regola snort locale personalizzata.



Dettaglio regola personalizzata

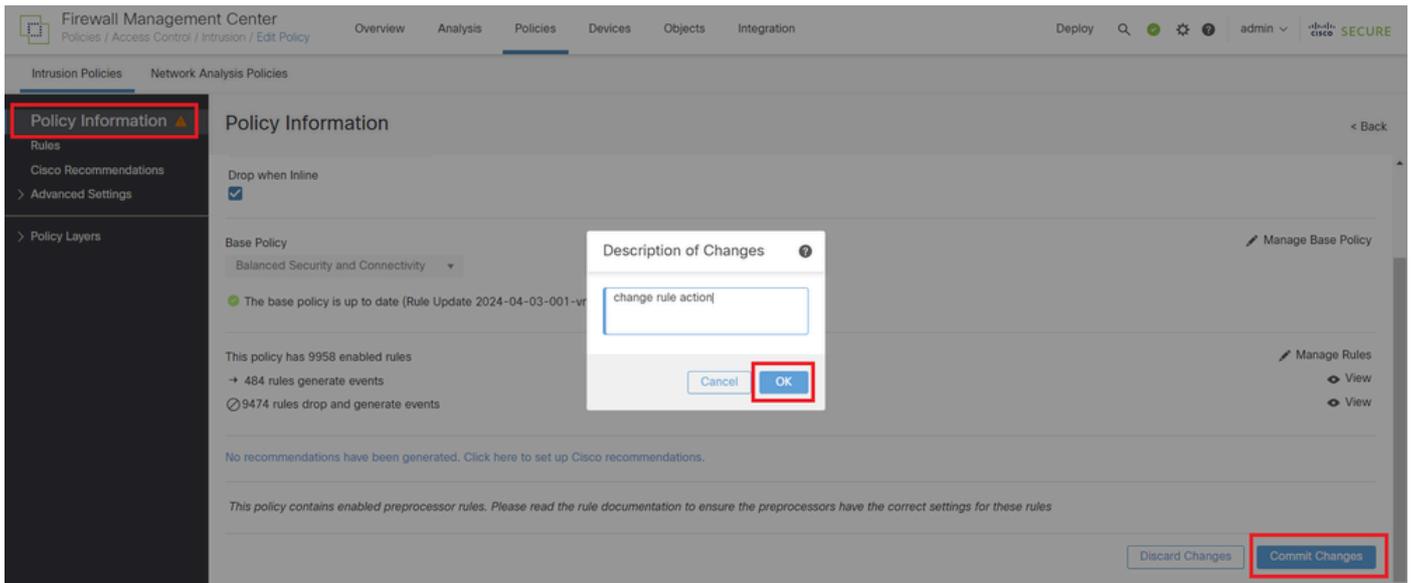
Passaggio 4. Azione regola di modifica

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



Modifica azione regola

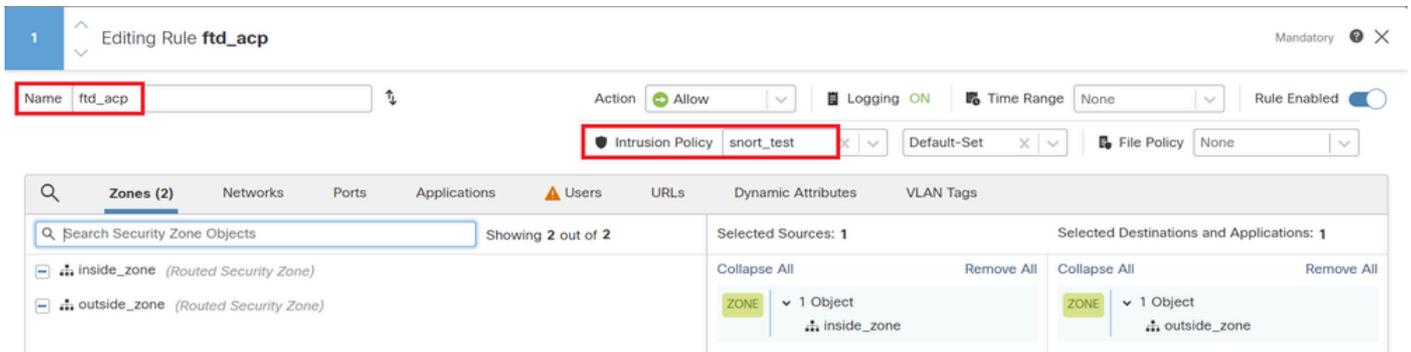
Fare clic su Informazioni criterio pulsante, fare clic su Conferma modifiche pulsante per salvare le modifiche.



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.

Firewall Management Center
Analysis / Intrusions / Events

Overview **Analysis** Policies Devices Objects Integration

Deploy 🔍 ⚙️ ⚠️ admin 🔒 Cisco **SECURE**

Bookmark This Page | Reporting | Dashboard | View Bookmarks | Search **Predefined Searches**

Events By Priority and Classification [\[switch workflow\]](#)

2024-04-06 09:41:20 - 2024-04-06 11:06:04 Expanding

Search Constraints [\[Edit Search Save Search\]](#)

Drilldown of Event, Priority, and Classification **Table View of Events** Packets

Jump to...

	Time	Priority	Impact	Inline Result	Reason	Source IP	Source Country	Destination IP	Destination Country	Source Port / ICMP Type	Destination Port / ICMP Code	SSL Status	VLAN ID	Message	Classification	Generated
<input type="checkbox"/>	2024-04-06 11:05:13	low	Unknown	Dropped		192.168.20.1		192.168.10.1		80 (http) / tcp	50057 / tcp			custom_http_sig (1:1000001:1)	Unknown Traffic	Standard

Evento Intrusion

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

Firewall Management Center
Analysis / Intrusions / Events

Overview **Analysis** Policies Devices Objects Integration

Deploy 🔍 ⚙️ ⚠️ admin 🔒 Cisco **SECURE**

Bookmark This Page | Reporting | Dashboard | View Bookmarks | Search **Predefined Searches**

Events By Priority and Classification [\[switch workflow\]](#)

2024-04-06 09:41:20 - 2024-04-06 11:07:15 Expanding

Search Constraints [\[Edit Search Save Search\]](#)

Drilldown of Event, Priority, and Classification **Table View of Events** **Packets**

Event Information

Message: custom_http_sig (1:1000001:1)

Time: 2024-04-06 11:06:34

Classification: Unknown Traffic

Priority: low

Ingress Security Zone: outside_zone

Egress Security Zone: inside_zone

Device: FPR2120_FTD

Ingress Interface: outside

Egress Interface: inside

Source IP: 192.168.20.1

Source Port / ICMP Type: 80 (http) / tcp

Destination IP: 192.168.10.1

Destination Port / ICMP Code: 50061 / tcp

HTTP Hostname: 192.168.20.1

HTTP URI: /test.txt

Intrusion Policy: snort_test

Access Control Policy: acp-rule

Access Control Rule: ftd_acp

Rule: alert tcp any any <> any any (sid:1000001; gid:1; flow:established,to_client; content:"username"; rsnbytes; siz:"custom_http_sig"; classtype:unknown; rev:1;)

Actions

Dettaglio dell'evento Intrusion

Risoluzione dei problemi

Eseguire il comando `system 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).