Configura regole personalizzate di snort locale in Snort3 su FTD

Sommario

Introduzione

In questo documento viene descritta la procedura per configurare le regole di snort locali personalizzate in Snort3 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:

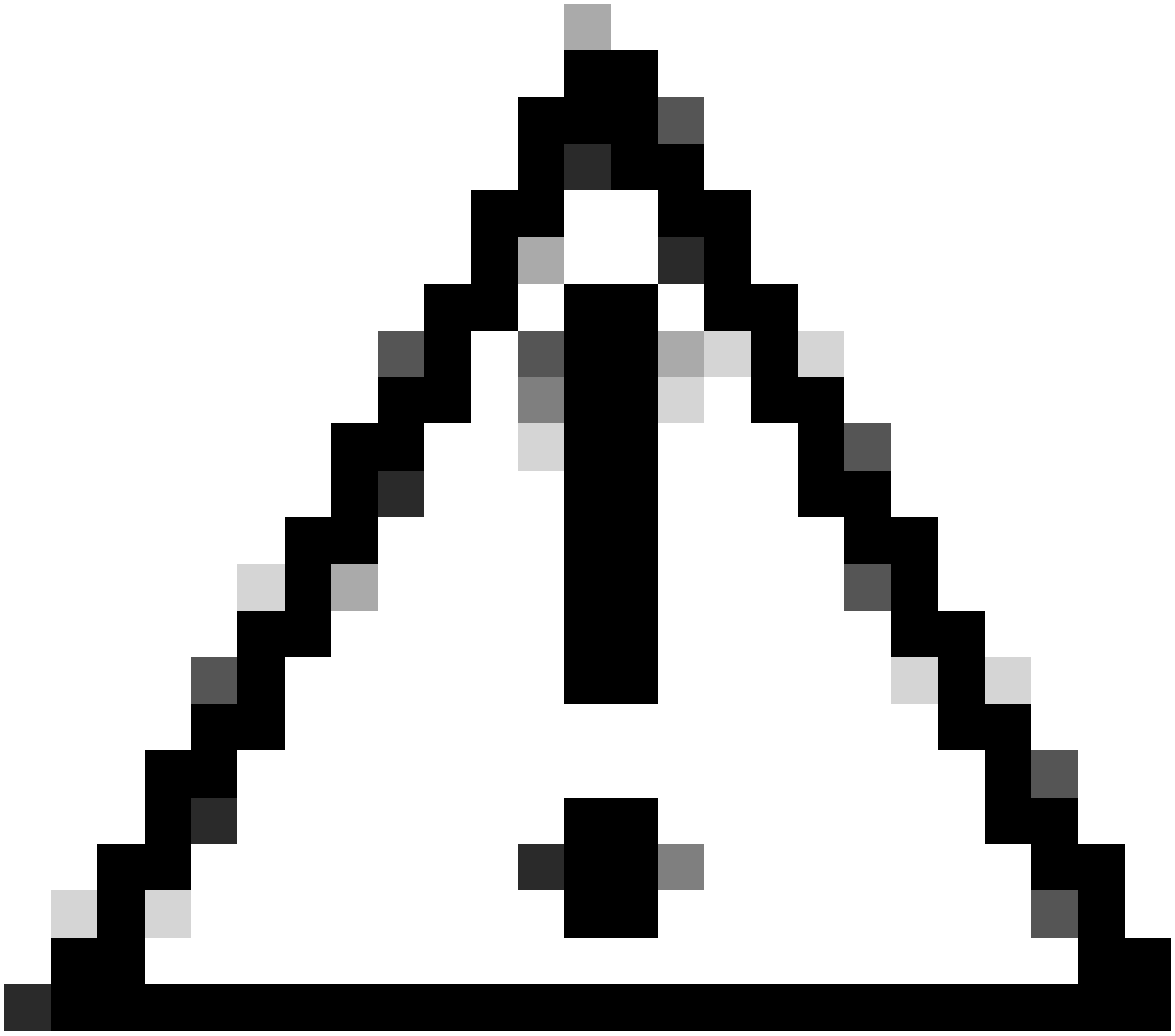
- Cisco Firepower Management Center per VMWare 7.4.1
- Cisco Firepower 2120 7.4.1

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

Il supporto per lo Snort 3 nella difesa dalle minacce con il centro di gestione inizia nella versione 7.0. Per i dispositivi nuovi e sottoposti a re-imaging della versione 7.0 e successive, Snort 3 è il motore di ispezione di default.

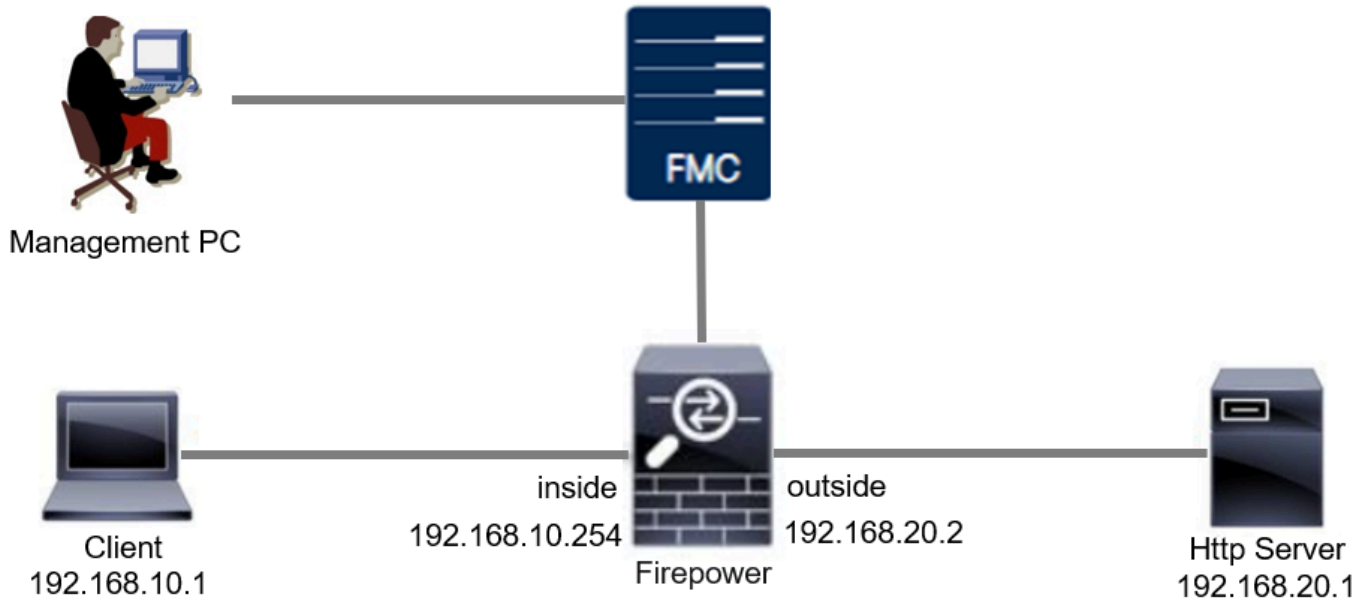
In questo documento viene illustrato un esempio di personalizzazione delle regole di snort per Snort 3 e un esempio pratico di verifica. In particolare, viene illustrato come configurare e verificare un criterio di intrusione con una regola Snort personalizzata per eliminare i pacchetti HTTP che contengono una determinata stringa (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.

Esempio di rete

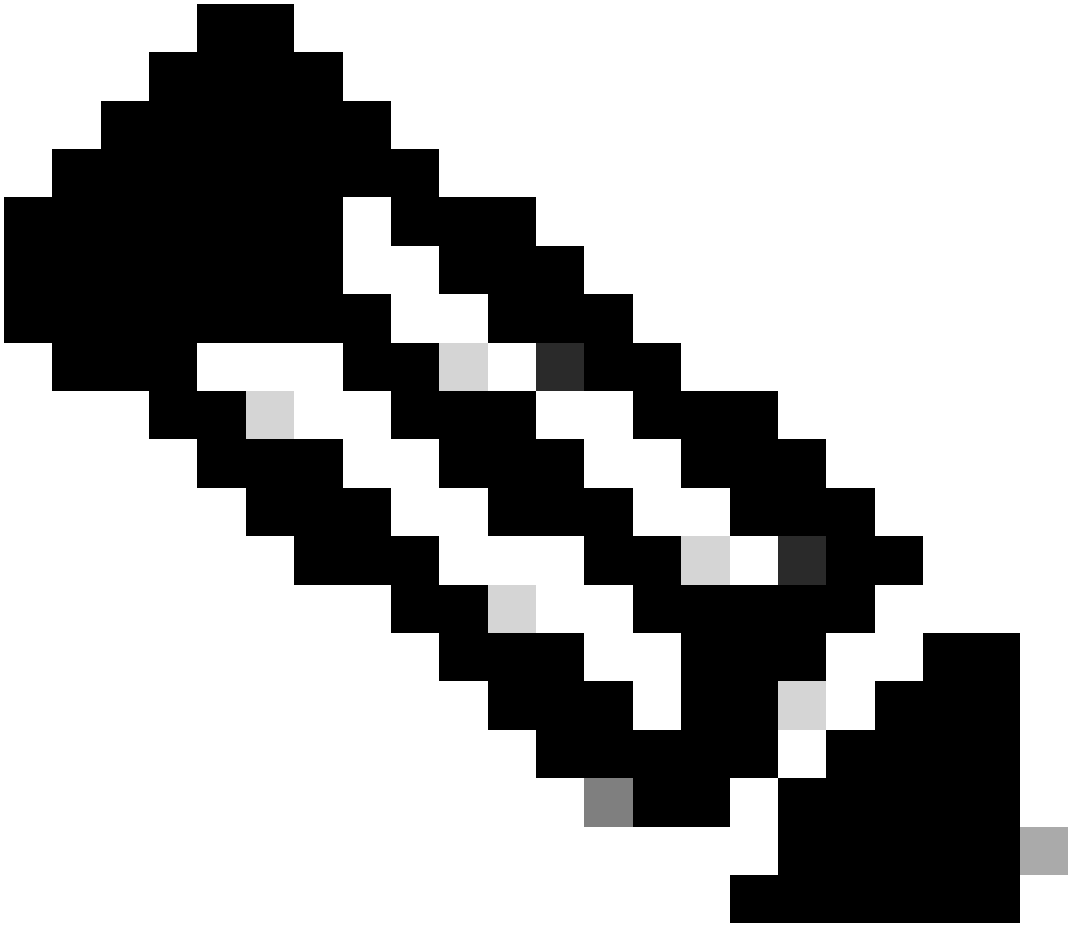
In questo documento viene illustrata la configurazione e la verifica della Regola snort locale personalizzata in Snort3 nel diagramma.



Esempio di rete

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).

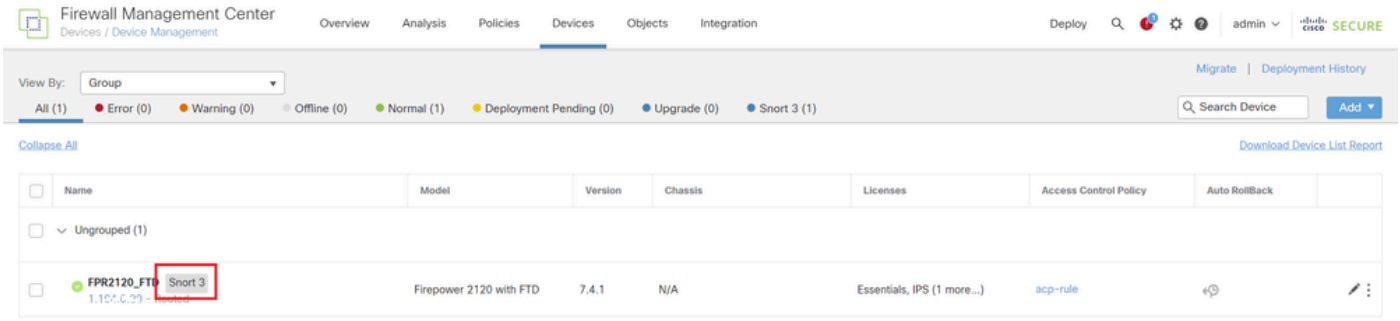


Nota: al momento non è possibile aggiungere regole personalizzate per l'ascolto locale dalla pagina Snort 3 All Rules nell'interfaccia utente di FMC. È necessario utilizzare il metodo illustrato in questo documento.

Metodo 1. Importa da Snort 2 a Snort 3

Passaggio 1. Conferma versione snort

Passare aDispositivi>Gestione dispositivi in FMC, fare clic su Scheda Dispositivo. Confermate che la versione snort sia Snort3.



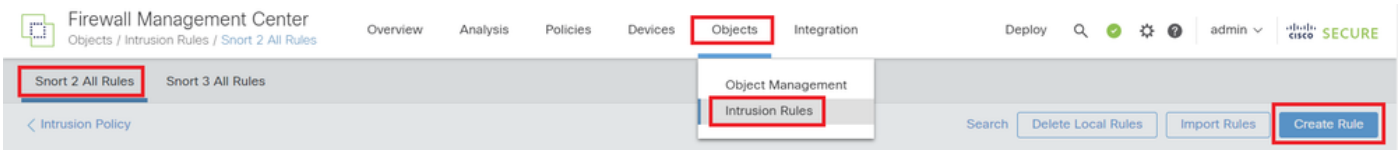
Versione snort

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

Selezionare Oggetti > Regole intrusione > Ordina 2 tutte le regole in FMC. Fate clic su Crea regola (Create Rule) per aggiungere una regola di snort locale personalizzata oppure selezionate Oggetti (Objects) > Regole intrusione (Intrusion Rules) > Snort 2 tutte le regole (Snort 2 All Rules) > Regole locali (Local Rules) su FMC (FMC). Fate clic sul pulsante Modifica (Edit) per modificare una regola di snort locale personalizzata esistente.

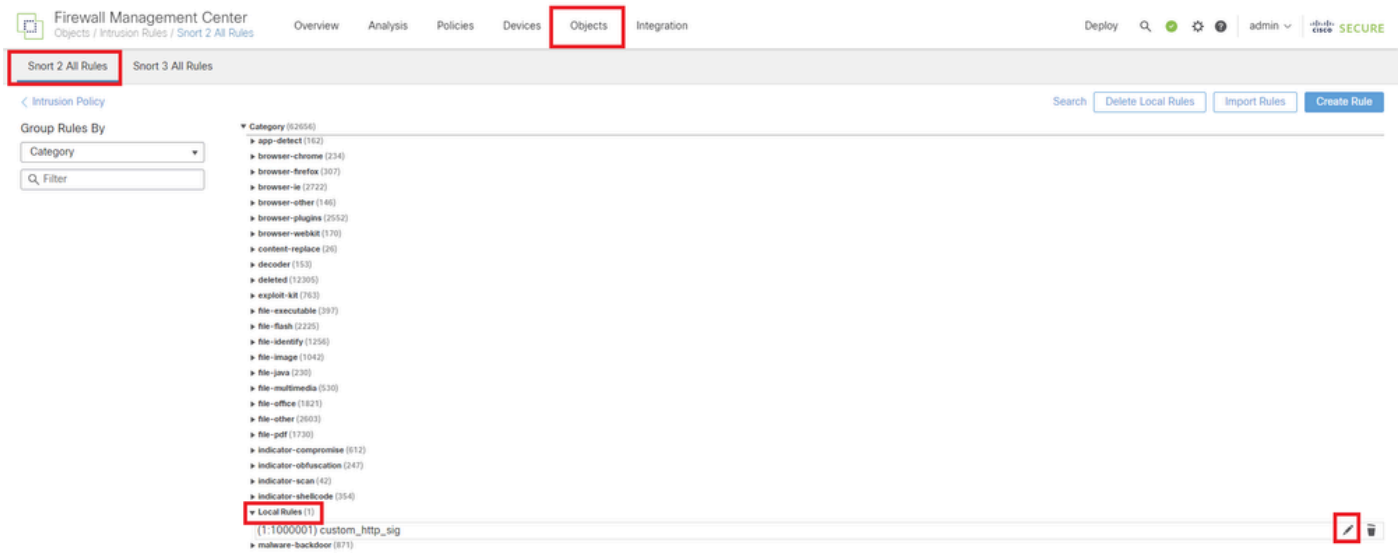
Per istruzioni su come creare regole di snort locali personalizzate nell'Snort 2, fare riferimento a [Configure Local Snort Rules in Snort2 on FTD](#) (Configura regole di snort locali personalizzate nell'Snort2 su FTD).

Aggiungete una nuova Regola snort locale personalizzata come mostrato nell'immagine.



Aggiungi nuova regola personalizzata

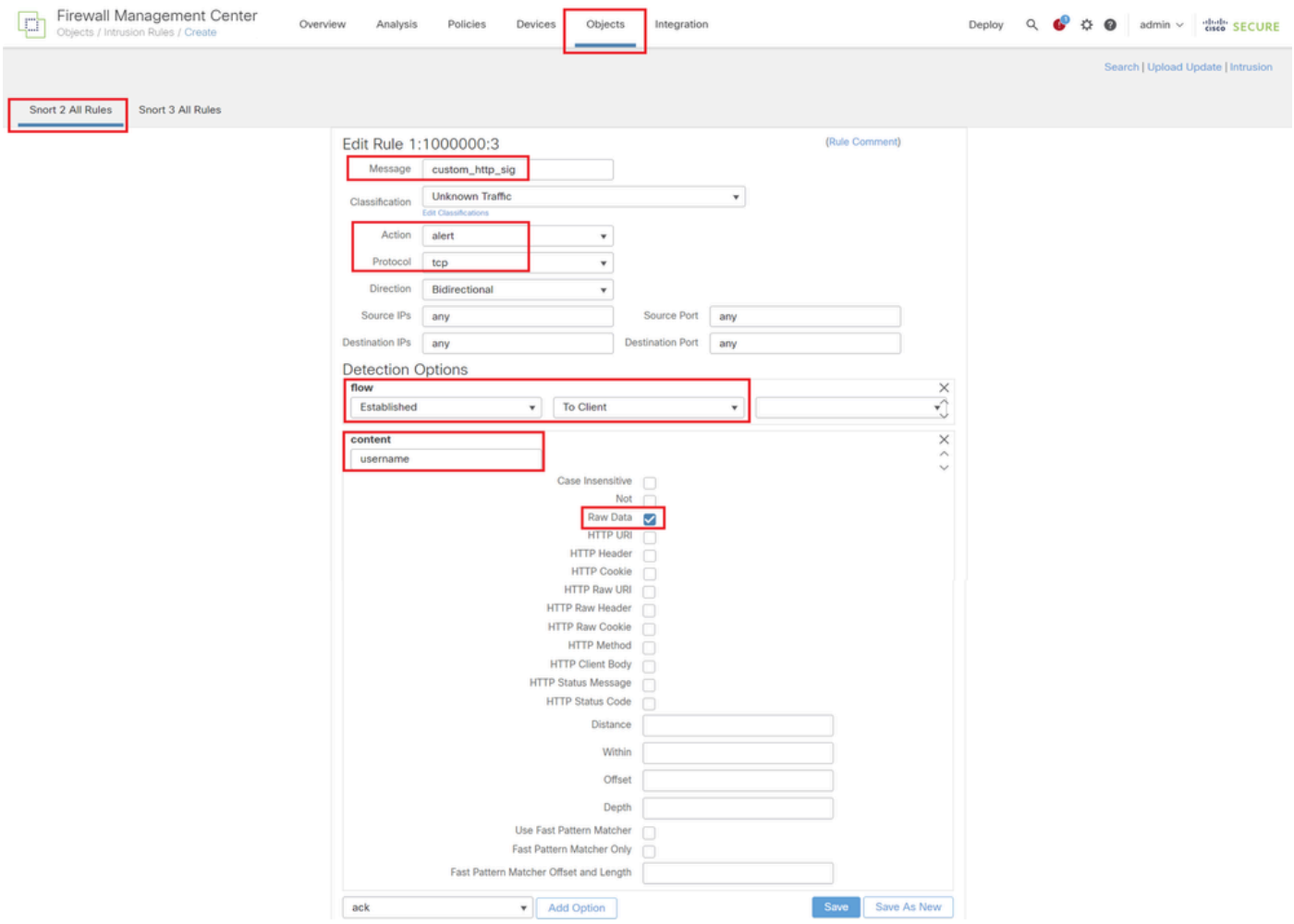
Modificate una regola di snort locale esistente come mostrato nell'immagine. In questo esempio viene modificata una regola personalizzata esistente.



Modificare una regola personalizzata esistente

Immettere le informazioni sulla firma per rilevare i pacchetti HTTP contenenti una stringa specifica (nome utente).

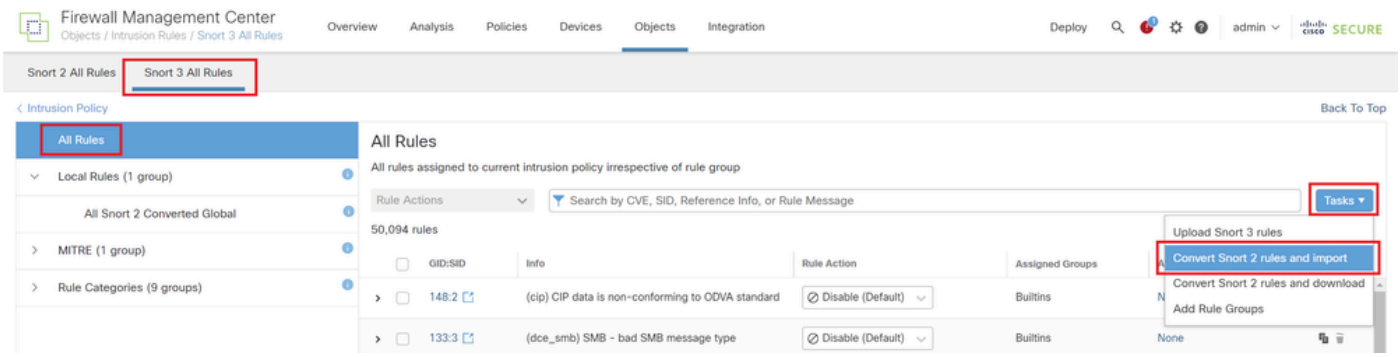
- Messaggio : custom_http_sig
- Azione : avviso
- Protocollo : tcp
- flusso : stabilito, al client
- content : nomeutente (dati non elaborati)



Inserisci le informazioni necessarie per la regola

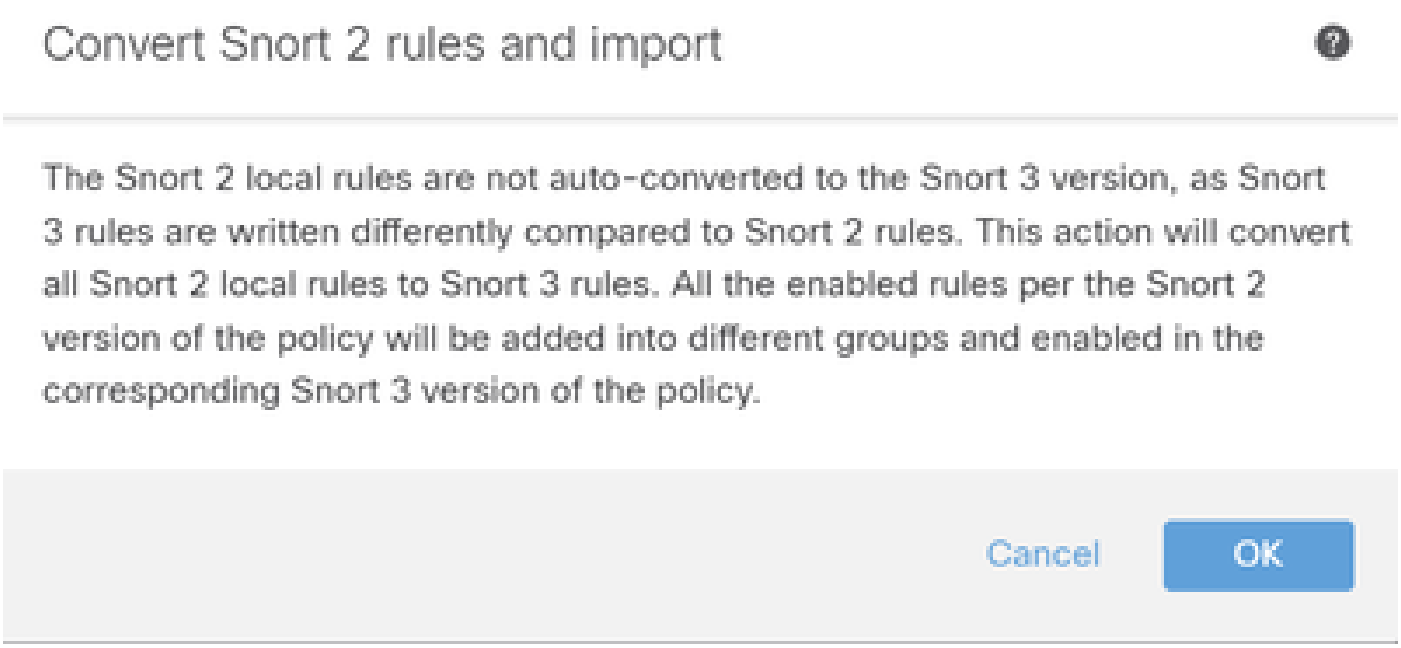
Passaggio 3. Importa regole personalizzate di snort locale dall'snort 2 all'snort 3

Selezionare Oggetti > Regole intrusione > Ordina 3 Tutte le regole > Tutte le regole in FMC, fare clic su Converti regole Ordina 2 e Importa dall'elenco a discesa Task.



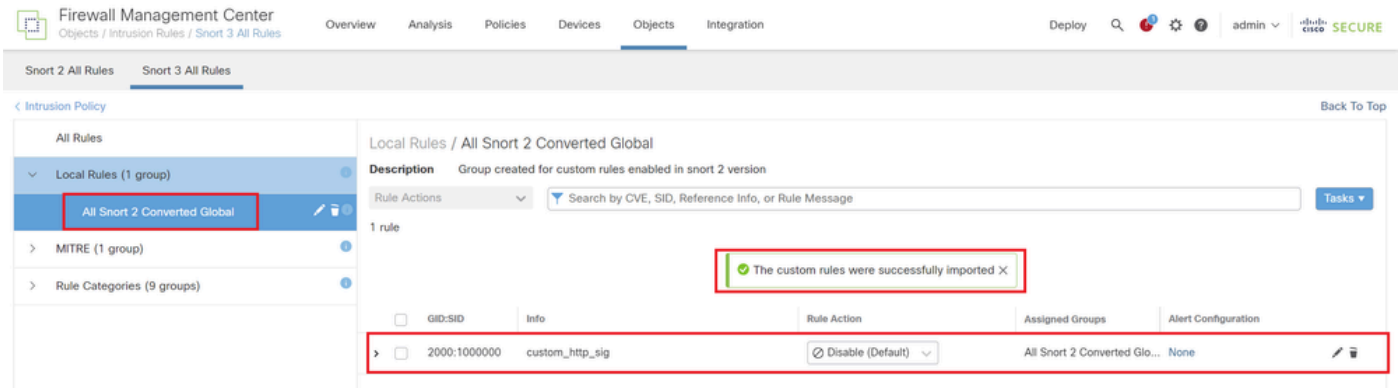
Importa regola personalizzata per snort 3

Controllare il messaggio di avviso e fare clic su OK.



Messaggio di avviso

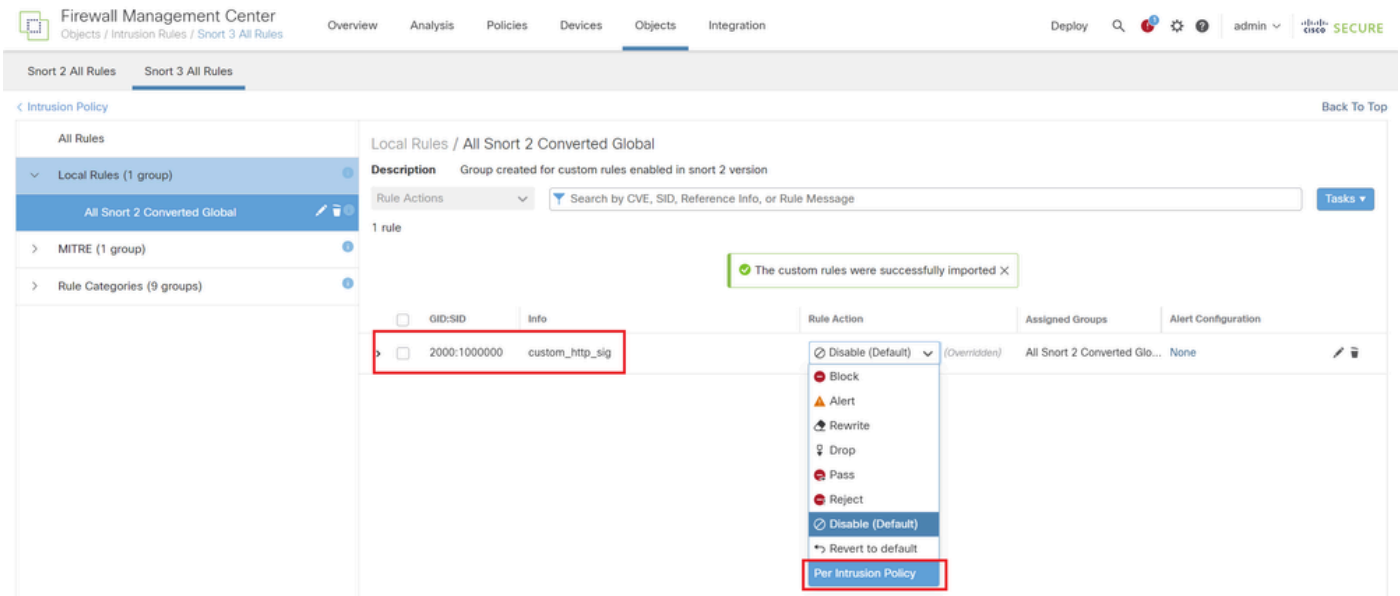
Passare a Oggetti > Regole intrusione > Ordina 3 Tutte le regole in FMC, fare clic su Tutte le regole di ordinamento 2 convertite globali per confermare la regola di ordinamento locale personalizzata importata.



Conferma regola personalizzata importata

Passaggio 4. Azione regola di modifica

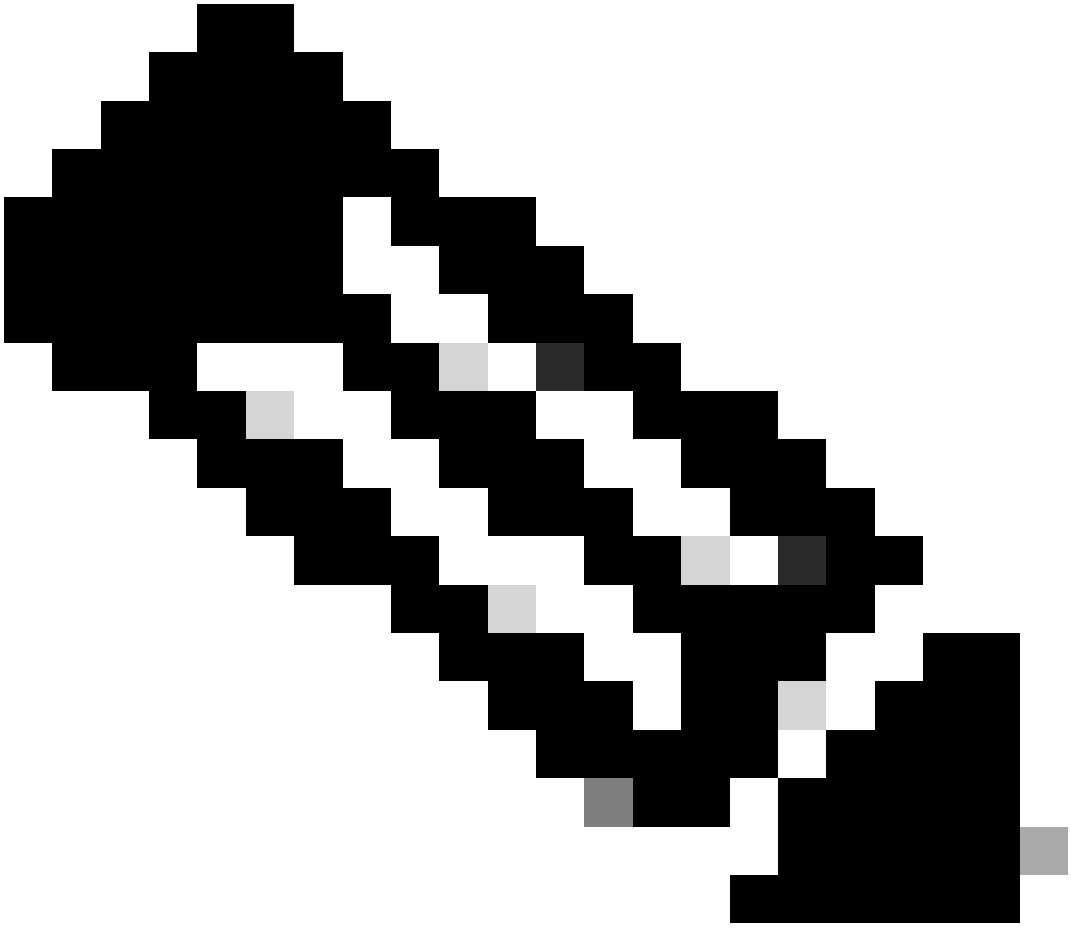
Fare clic su Criteri per intrusione in base all'Azione regola della regola personalizzata di destinazione.



Azione regola di modifica

Nella schermata Modifica azione regola immettere le informazioni per il criterio e l'azione regola.

- Criterio : snort_test
- Azione regola: BLOCK



Nota: le azioni delle regole sono:

Blocca: genera un evento, blocca il pacchetto corrispondente corrente e tutti i pacchetti successivi in questa connessione.

Avviso: genera solo eventi per il pacchetto corrispondente e non elimina il pacchetto o la connessione.

Riscrivi: genera l'evento e sovrascrive il contenuto del pacchetto in base all'opzione di sostituzione nella regola.

Pass: non viene generato alcun evento, consente il passaggio del pacchetto senza un'ulteriore valutazione da parte delle successive regole Snort.

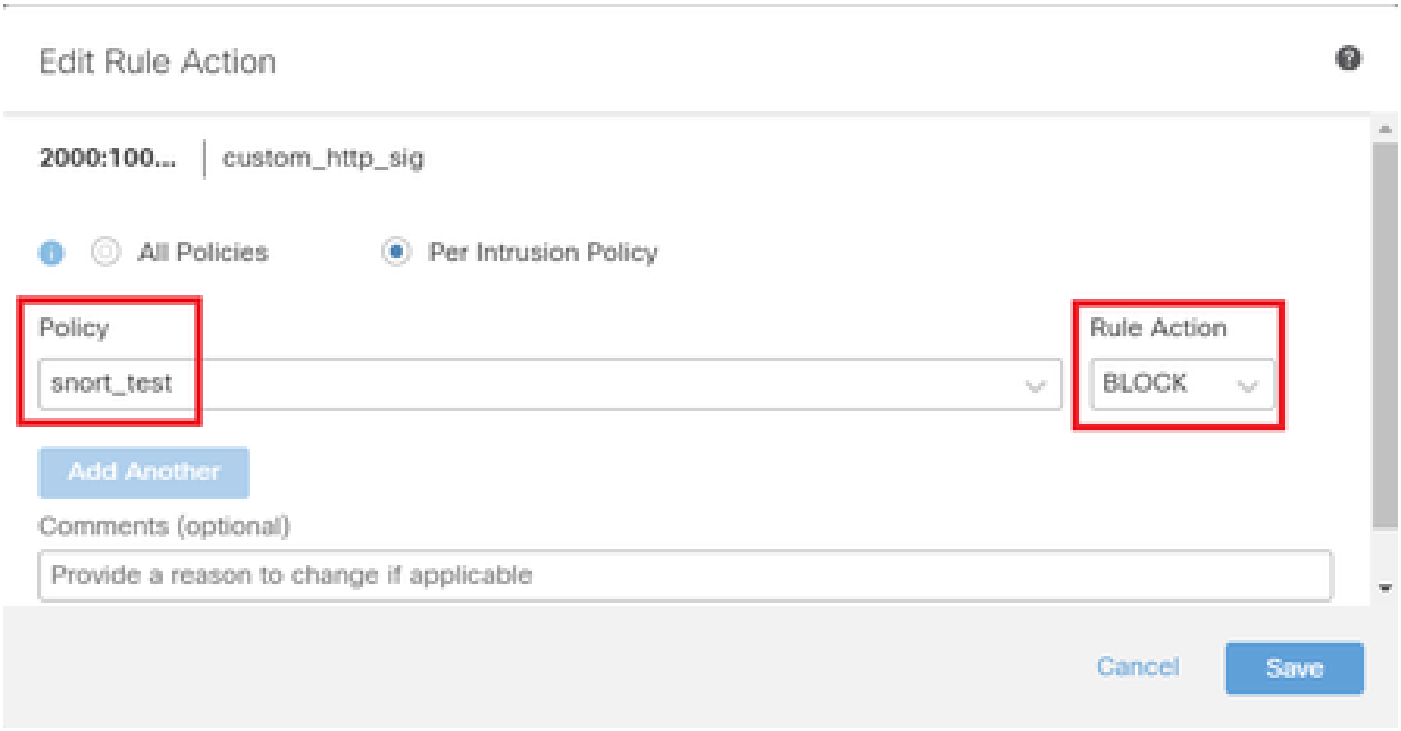
Drop: genera l'evento, scarta il pacchetto corrispondente e non blocca ulteriore traffico in questa connessione.

Rifiuta: genera eventi, elimina pacchetti corrispondenti, blocca ulteriore traffico in questa connessione e invia la reimpostazione TCP se si tratta di un protocollo TCP agli host di

origine e di destinazione.

Disabilita: il traffico non viene confrontato con questa regola. Nessun evento generato.

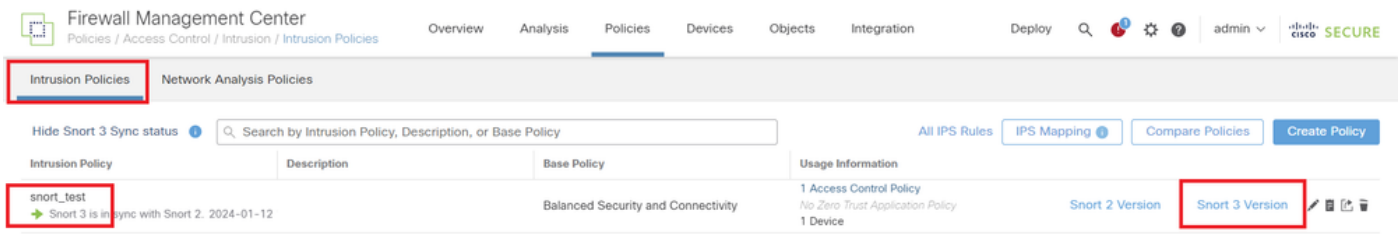
Default - Ripristina l'azione di default del sistema.



Modifica azione regola

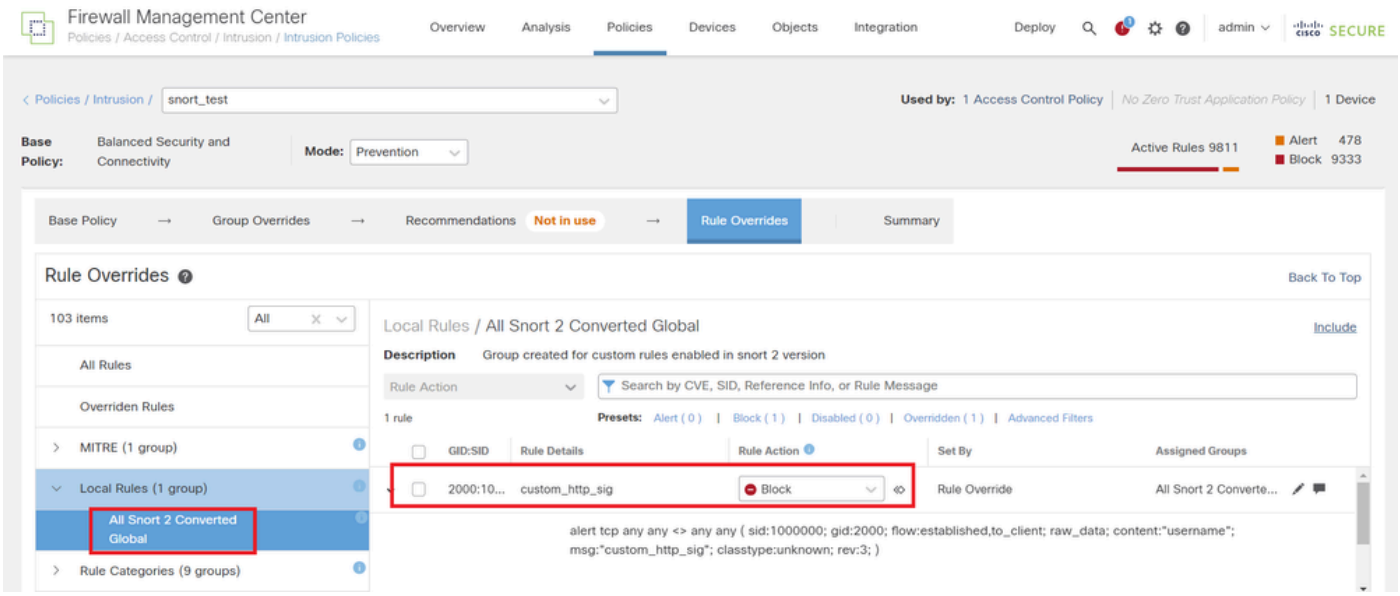
Passaggio 5. Conferma regola di ordinamento locale personalizzata importata

Selezionare Policies > Intrusion Policies on FMC (Policy di intrusione), quindi fare clic su Snort 3 Version (Snort. 3 Versione) corrispondente al criterio di intrusione di destinazione nella riga.



Conferma regola personalizzata importata

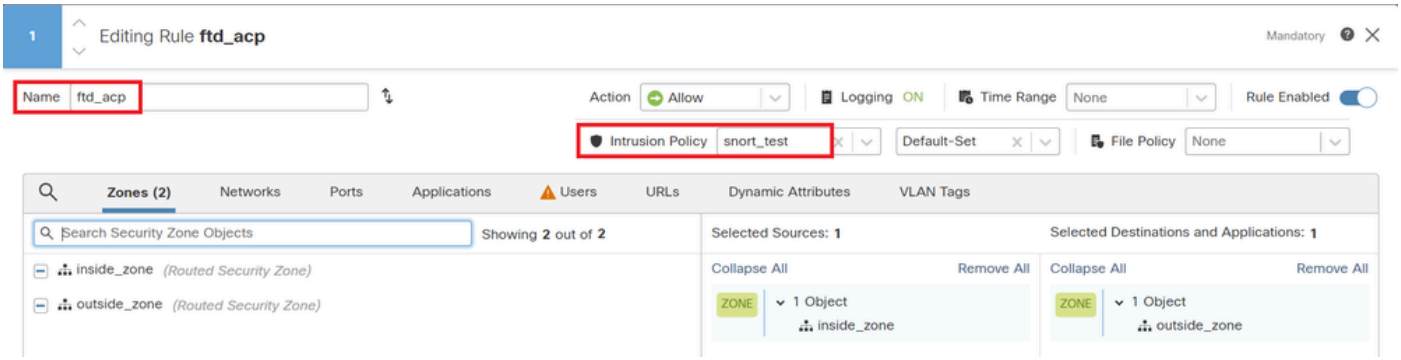
Fate clic su Regole locali (Local Rules) > Tutte le regole di snort 2 (All Snort 2 Converted Global) per controllare i dettagli della regola di snort locale personalizzata.



Conferma regola personalizzata importata

Passaggio 6. Associa criterio di intrusione alla regola dei criteri di controllo di accesso (ACP)

Passare a Criteri>Controllo accesso FMC, associare il criterio di intrusione al provider di servizi di audioconferenza.



Associa a regola ACP

Passaggio 7. Distribuisci modifiche

Distribuire le modifiche in FTD.

Distribuisci modifiche

Metodo 2. Carica file locale

Passaggio 1. Conferma versione snort

Come per il passaggio 1 del metodo 1.

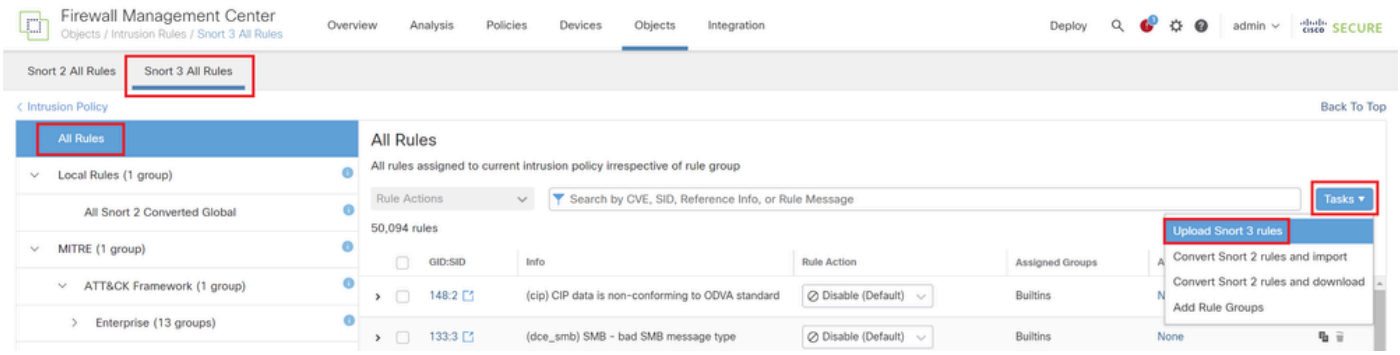
Passaggio 2. Creare una regola di snort locale personalizzata

Creare manualmente una Regola snort locale personalizzata e salvarla in un file locale denominato custom-rules.txt.

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

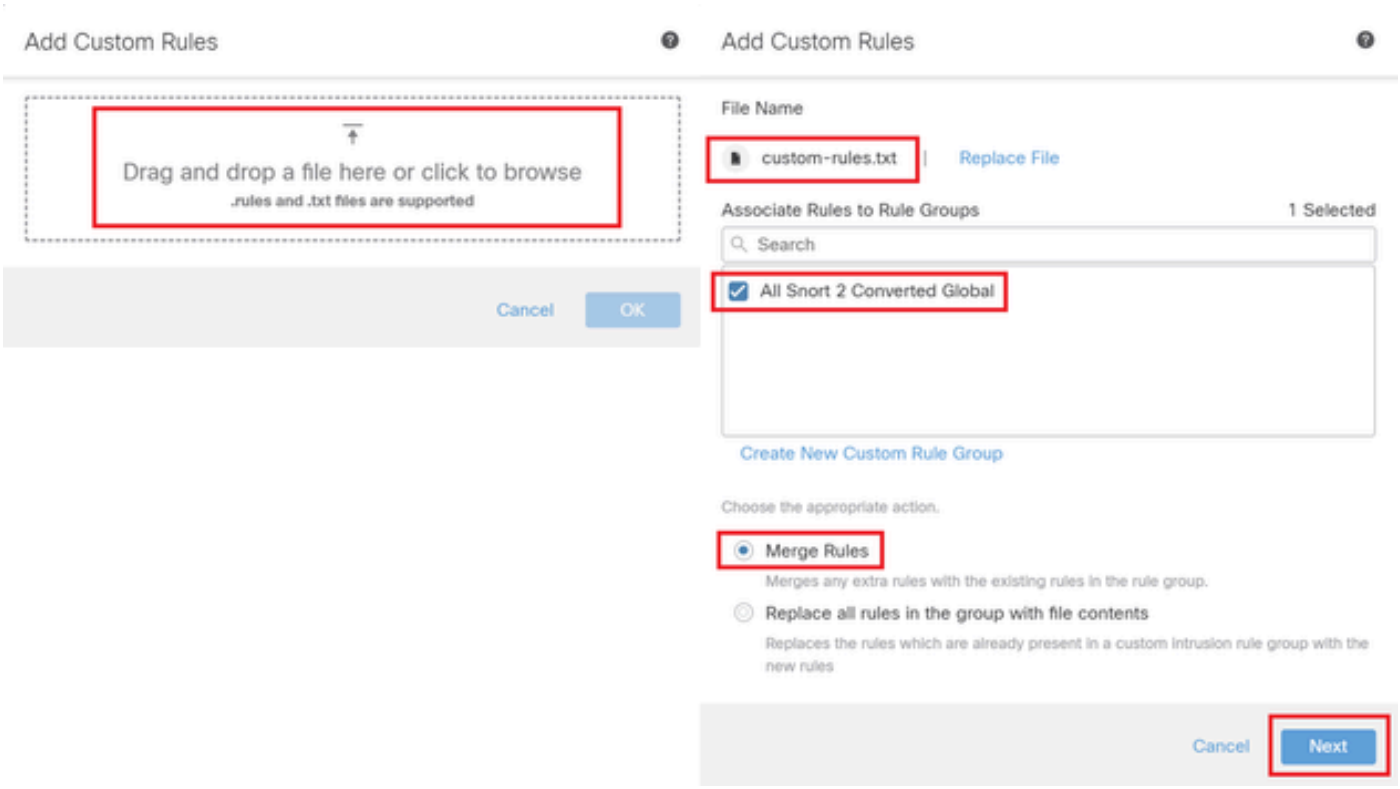
Passaggio 3. Carica la regola di snort locale personalizzata

Selezionare Oggetti > Regole intrusione > Ordina 3 Tutte le regole > Tutte le regole in FMC, quindi fare clic su Carica regole Avanza 3 dall'elenco a discesa Task.



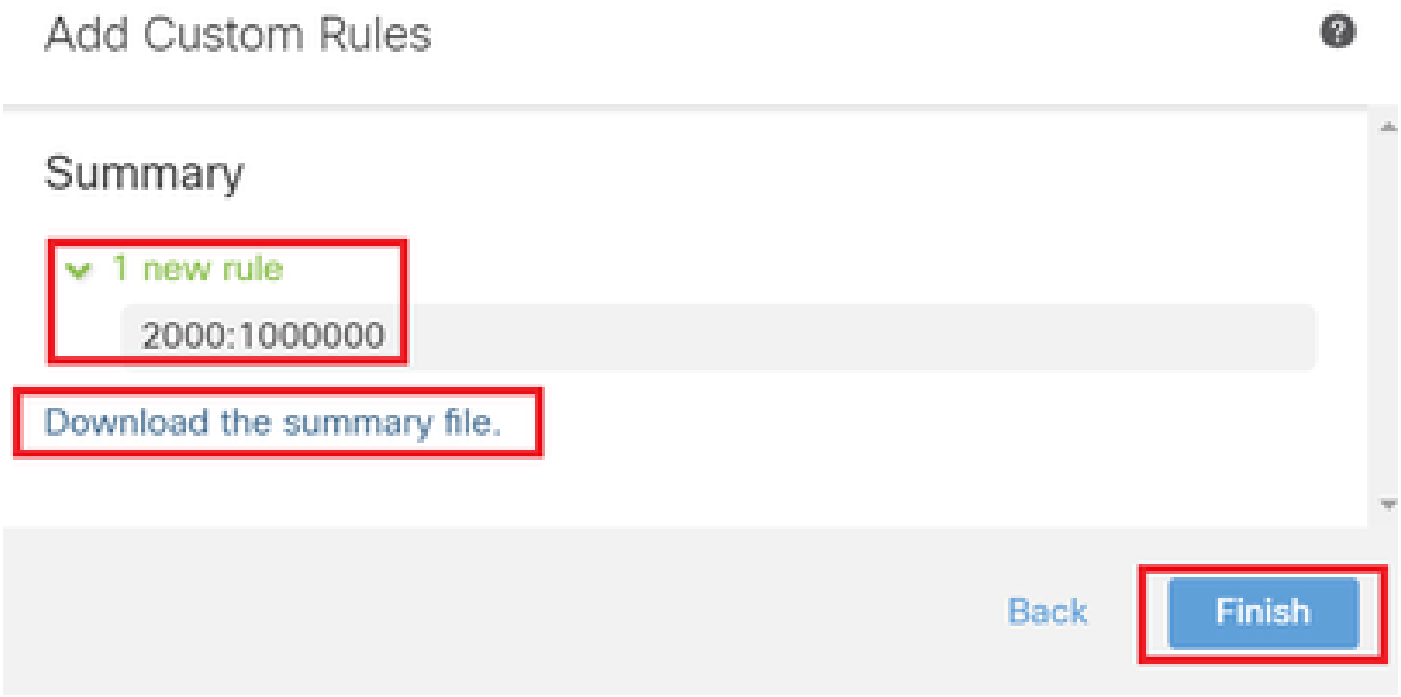
Carica regola personalizzata

Nella schermata Aggiungi regole personalizzate trascinare il file custom-rules.txt locale, selezionare i gruppi di regole e l'azione appropriata (in questo esempio, Unisci regole), quindi fare clic sul pulsante Avanti.



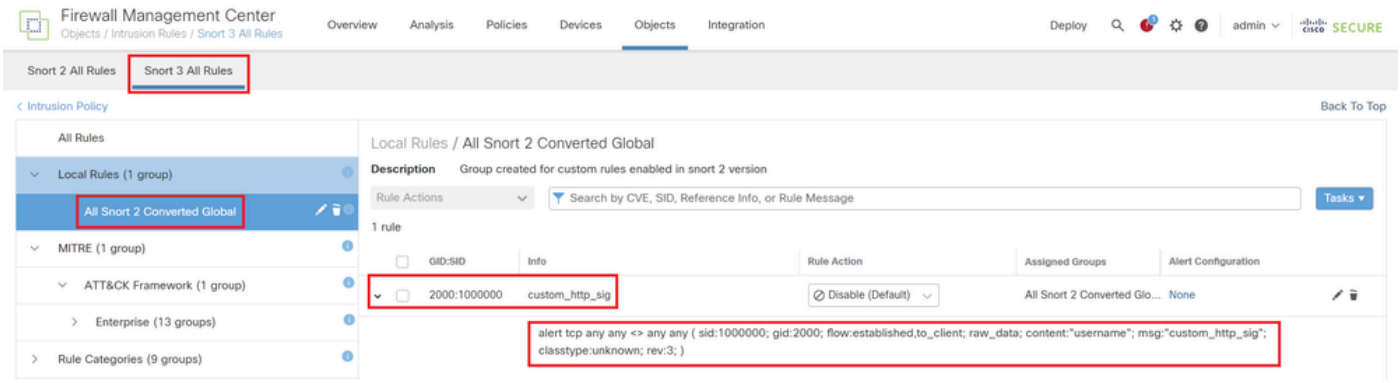
Aggiungi regola personalizzata

Confermare che il file delle regole locali è stato caricato correttamente.



Conferma risultato caricamento

Selezionare Oggetti > Regole intrusione > Ordina 3 Tutte le regole in FMC, quindi fare clic su Tutte le regole di ordinamento 2 convertite globali per confermare la regola di ordinamento locale personalizzata caricata.



Dettaglio regola personalizzata

Passaggio 4. Azione regola di modifica

Come al passaggio 4 del metodo 1.

Passaggio 5. Conferma regola di ordinamento locale personalizzata caricata

Come per il passaggio 5 del metodo 1.

Passaggio 6. Associa criterio di intrusione alla regola dei criteri di controllo di accesso (ACP)

Come per il passaggio 6 del metodo 1.

Passaggio 7. Distribuisci modifiche

Come per il passaggio 7 del metodo 1.

Verifica

Passaggio 1. Imposta contenuto del file nel server HTTP

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

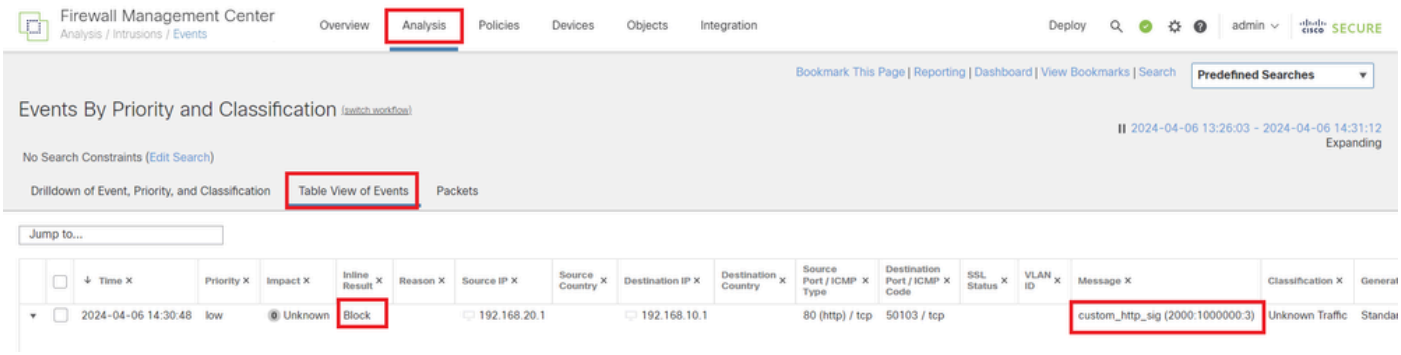
Passaggio 2. Richiesta HTTP iniziale

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

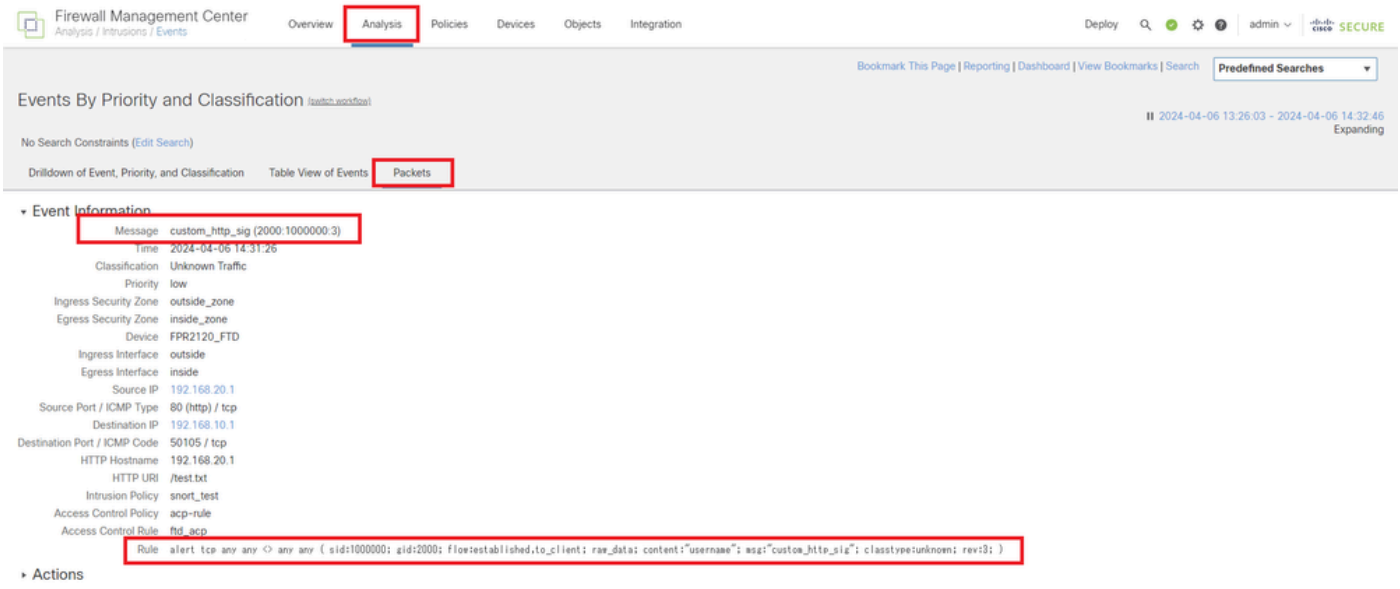
Passaggio 3. Conferma evento di intrusione

Passare ad Analisi>Intrusioni>Eventi su FMC, verificare che l'evento Intrusion sia generato dalla regola personalizzata Snort locale.



Evento Intrusion

Fare clic su Packetstab, quindi confermare i dettagli di Evento intrusione.



Dettaglio dell'evento Intrusion

Domande frequenti (FAQ)

Q : Qual è la scelta consigliata, Snort 2 o Snort 3 ?
R: Rispetto allo Snort 2, lo Snort 3 offre velocità di elaborazione migliorate e nuove funzionalità, che lo rendono l'opzione più consigliata.

D : Dopo l'aggiornamento da una versione di FTD precedente alla 7.0 alla versione 7.0 o successiva, la versione snort viene automaticamente aggiornata alla versione Snort 3 ?
A : No, il motore di ispezione rimane sullo Snort 2. Per utilizzare Snort 3 dopo l'aggiornamento, è necessario attivarlo esplicitamente. Si noti che lo snort 2 sarà obsoleto in una versione futura e si consiglia di smetterla di utilizzarlo ora.

D : Nell'ambiente 3 è possibile modificare una regola personalizzata esistente?
R: No, non è possibile modificarlo. Per modificare una regola personalizzata specifica, è necessario eliminare la regola pertinente e ricrearla.

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 (2000:1000000:3).

```
<#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
```

Riferimento

[Guida alla configurazione di Cisco Secure Firewall Management Center Snort 3]

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).