

# Configura regole personalizzate di snort locale in Snort3 su FTD

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Configurazione](#)

[Metodo 1. Importa da Snort 2 a Snort 3](#)

[Passaggio 1. Conferma versione snort](#)

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

[Passaggio 3. Importa regole personalizzate di snort locale dall'snort 2 all'snort 3](#)

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

[Passaggio 5. Conferma regola di ordinamento locale personalizzata importata](#)

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

[Passaggio 7. Distribuisci modifiche](#)

[Metodo 2. Carica file locale](#)

[Passaggio 1. Conferma versione snort](#)

[Passaggio 2. Creare una regola di snort locale personalizzata](#)

[Passaggio 3. Carica la regola di snort locale personalizzata](#)

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

[Passaggio 5. Conferma regola di ordinamento locale personalizzata caricata](#)

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

[Passaggio 7. Distribuisci modifiche](#)

[Verifica](#)

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

[Passaggio 2. Richiesta HTTP iniziale](#)

[Passaggio 3. Conferma evento di intrusione](#)

[Domande frequenti \(FAQ\)](#)

[Risoluzione dei problemi](#)

[Riferimento](#)

---

## 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:

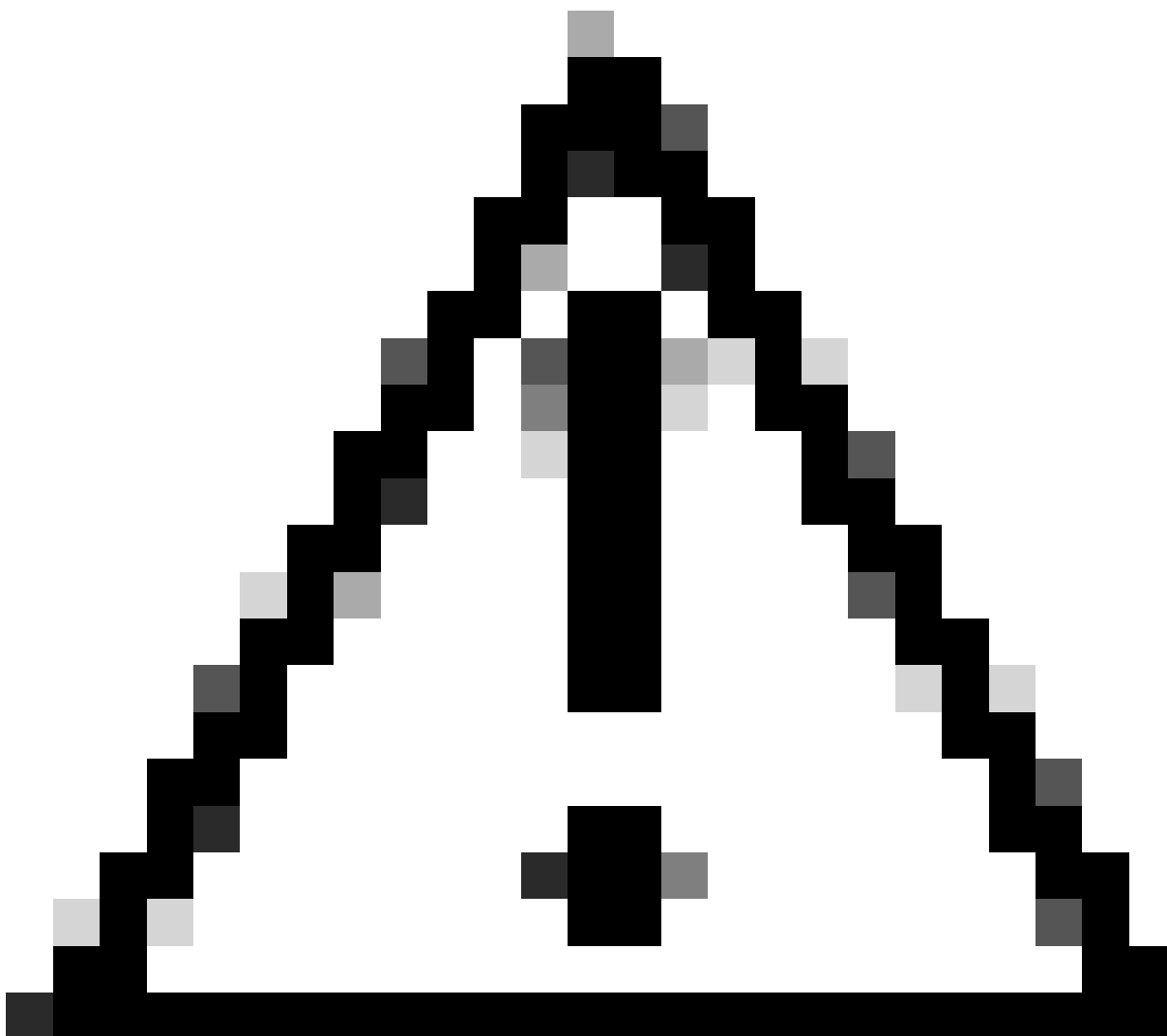
- Cisco Firepower Management Center per VMWare 7.4.1
- Cisco Firepower 2120 7.4.1

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).

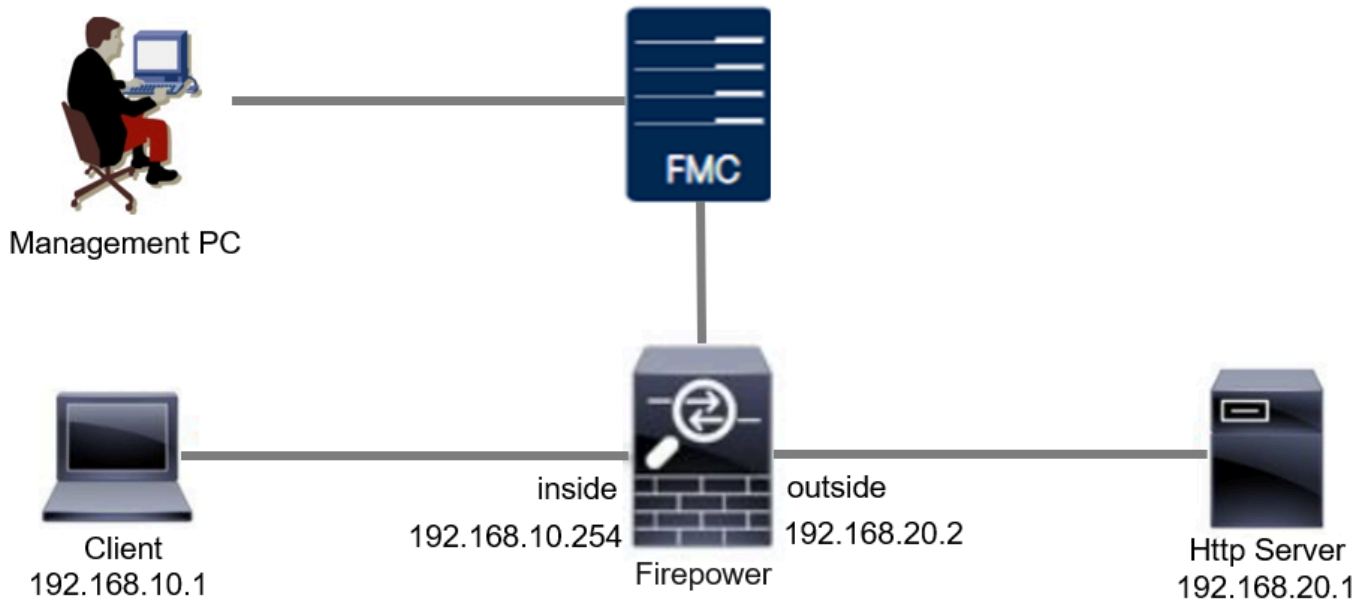


Attenzione: la creazione di regole personalizzate per lo snort locale e il relativo supporto esulano dalla copertura del supporto TAC. Pertanto, questo documento può essere utilizzato solo come riferimento e richiede la creazione e la gestione di queste regole personalizzate a propria discrezione e responsabilità.

---

## 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 a [Dispositivi](#) > [Gestione dispositivi](#) in FMC, fare clic su Scheda Dispositivo. Confermate che la versione snort sia Snort3.

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Ungrouped (1)						
FPR2120_FTD 1.10°C.29	Firepower 2120 with FTD	7.4.1	N/A	Essentials, IPS (1 more...)	acp-rule	

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.

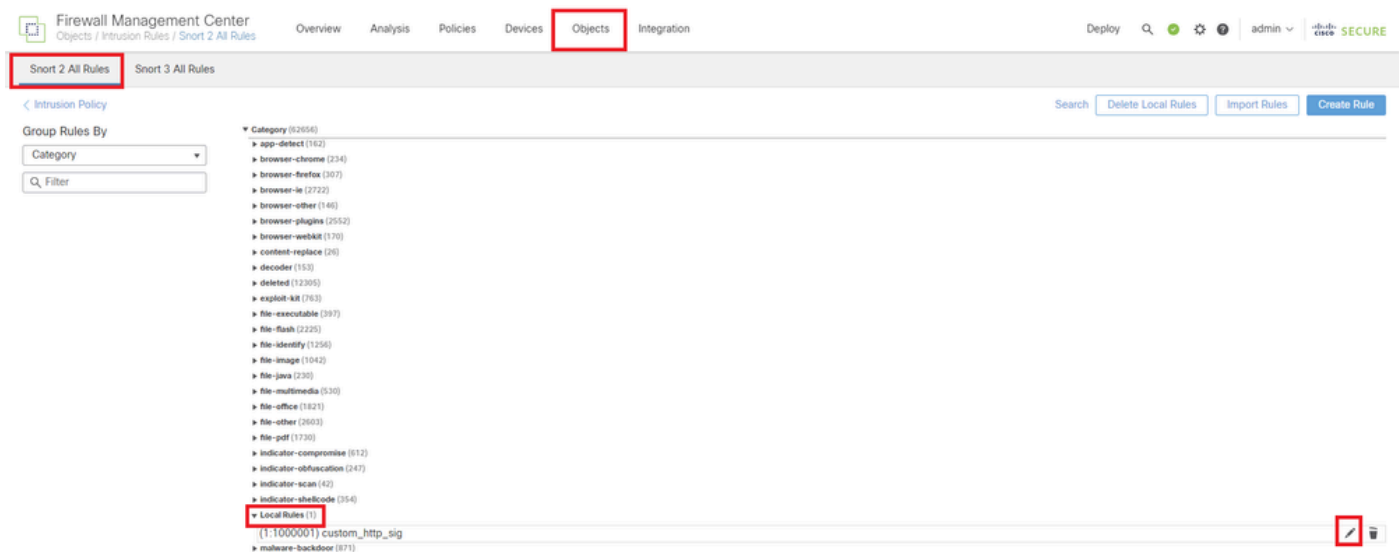
Per istruzioni su come creare regole di snort locali personalizzate nell'Snort 2, fare riferimento a [Configure Local Snort Rules in Snort2 on FTD](#) (Configura regole di snort locali personalizzate nell'Snort2 su FTD).

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)

Firewall Management Center  
Objects / Intrusion Rules / Create

Overview Analysis Policies Devices **Objects** Integration

Deploy Search admin cisco SECURE

Search | Upload Update | Intrusion

Snort 2 All Rules Snort 3 All Rules

Edit Rule 1:1000000:3 (Rule Comment)

Message: custom\_http\_sig

Classification: Unknown Traffic

Action: alert

Protocol: tcp

Direction: Bidirectional

Source IPs: any Source Port: any

Destination IPs: any Destination Port: any

Detection Options

flow: Established To Client

content: username

Case Insensitive: Not

Raw Data:

HTTP URI:

HTTP Header:

HTTP Cookie:

HTTP Raw URI:

HTTP Raw Header:

HTTP Raw Cookie:

HTTP Method:

HTTP Client Body:

HTTP Status Message:

HTTP Status Code:

Distance:

Within:

Offset:

Depth:

Use Fast Pattern Matcher:

Fast Pattern Matcher Only:

Fast Pattern Matcher Offset and Length:

ack Add Option Save Save As New

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.

Firewall Management Center  
Objects / Intrusion Rules / Snort 3 All Rules

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ admin 🔒 Cisco SECURE

Snort 2 All Rules **Snort 3 All Rules**

< Intrusion Policy Back To Top

**All Rules**

All rules assigned to current intrusion policy irrespective of rule group

Rule Actions Search by CVE, SID, Reference Info, or Rule Message Tasks

50,094 rules

<input type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups
> <input type="checkbox"/>	148:2	(cip) CIP data is non-conforming to ODVA standard	Disable (Default)	Builtins
> <input type="checkbox"/>	133:3	(dce_smb) SMB - bad SMB message type	Disable (Default)	Builtins

Upload Snort 3 rules  
**Convert Snort 2 rules and import**  
Convert Snort 2 rules and download  
Add Rule Groups

Importa regola personalizzata per snort 3

Controllare il messaggio di avviso e fare clic su OK.

## Convert Snort 2 rules and import ?

The Snort 2 local rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. This action will convert all Snort 2 local rules to Snort 3 rules. All the enabled rules per the Snort 2 version of the policy will be added into different groups and enabled in the corresponding Snort 3 version of the policy.

Cancel 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.

Firewall Management Center  
Objects / Intrusion Rules / Snort 3 All Rules

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ admin 🔒 Cisco SECURE

Snort 2 All Rules **Snort 3 All Rules**

< Intrusion Policy Back To Top

**All Rules**

Local Rules (1 group)

**All Snort 2 Converted Global**

MITRE (1 group)

Rule Categories (9 groups)

**Local Rules / All Snort 2 Converted Global**

Description Group created for custom rules enabled in snort 2 version

Rule Actions Search by CVE, SID, Reference Info, or Rule Message Tasks

1 rule

The custom rules were successfully imported

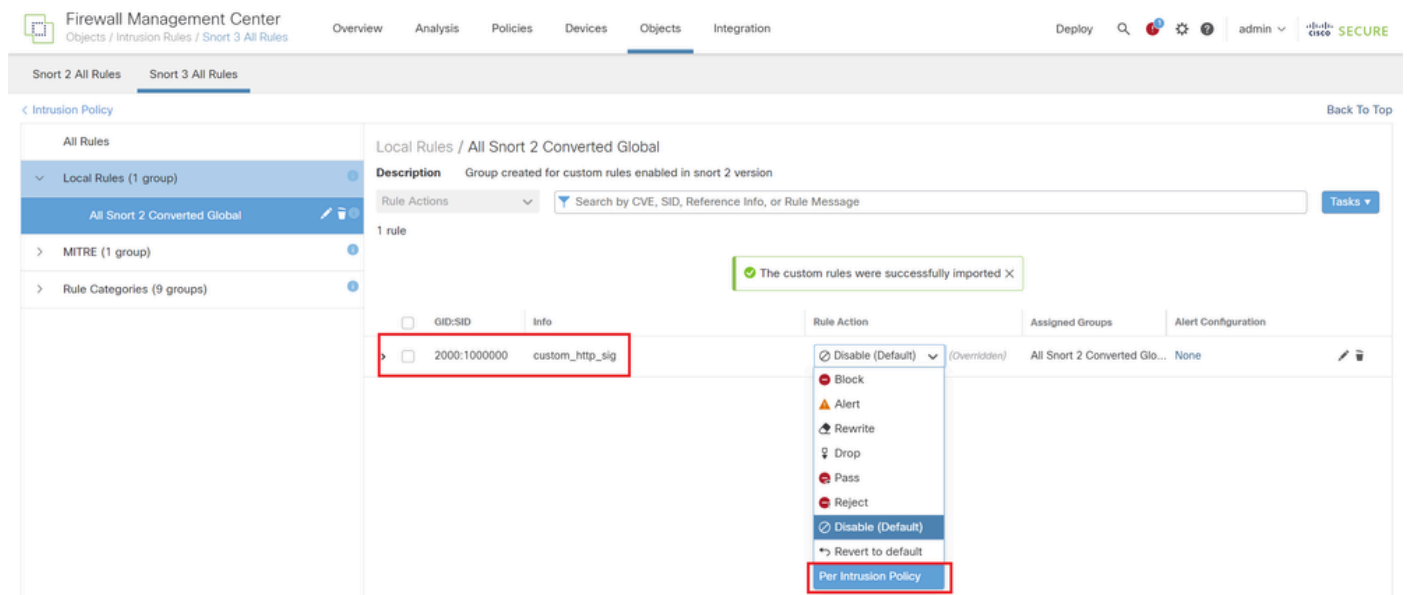
<input type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups	Alert Configuration
> <input type="checkbox"/>	2000:1000000	custom_http_sig	Disable (Default)	All Snort 2 Converted Glo...	None

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.

2000:100... | custom\_http\_sig

All Policies  Per Intrusion Policy

Policy: snort\_test Rule Action: BLOCK

Add Another

Comments (optional): Provide a reason to change if applicable

Cancel Save

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.

Firewall Management Center

Policies / Access Control / Intrusion / Intrusion Policies

Overview Analysis Policies Devices Objects Integration Deploy

Intrusion Policies Network Analysis Policies

Hide Snort 3 Sync status Search by Intrusion Policy, Description, or Base Policy All IPS Rules IPS Mapping Compare Policies Create Policy

Intrusion Policy	Description	Base Policy	Usage Information
snort_test → Snort 3 is in sync with Snort 2. 2024-01-12		Balanced Security and Connectivity	1 Access Control Policy No Zero Trust Application Policy 1 Device

Snort 2 Version Snort 3 Version

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.

Firewall Management Center  
Policies / Access Control / Intrusion / Intrusion Policies

Overview Analysis Policies Devices Objects Integration Deploy

Used by: 1 Access Control Policy | No Zero Trust Application Policy | 1 Device

Base Policy: Balanced Security and Connectivity | Mode: Prevention

Active Rules 9811 | Alert 478 | Block 9333

Base Policy → Group Overrides → Recommendations **Not in use** → **Rule Overrides** → Summary

Rule Overrides (103 items)

Local Rules / All Snort 2 Converted Global

Description: Group created for custom rules enabled in snort 2 version

Rule Action: Search by CVE, SID, Reference Info, or Rule Message

1 rule

GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
2000:10...	custom_http_sig	Block	Rule Override	All Snort 2 Converte...

alert tcp any any <> any any ( sid:1000000; gid:2000; flow:established,to\_client; raw\_data; content:"username"; msg:"custom\_http\_sig"; classtype:unknown; rev:3; )

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.

1 Editing Rule ftd\_acp

Name: ftd\_acp

Action: Allow

Logging: ON

Time Range: None

Rule Enabled: ON

Intrusion Policy: snort\_test

Default-Set: [ ]

File Policy: None

Zones (2): inside\_zone, outside\_zone

Selected Sources: 1 (inside\_zone)

Selected Destinations and Applications: 1 (outside\_zone)

Associa a regola ACP

Passaggio 7. Distribuisci modifiche

Distribuire le modifiche in FTD.

Firewall Management Center  
Policies / Access Control / Policy Editor

Overview Analysis Policies Devices Objects Integration

Return to Access Control Policy Management

acp-rule

Packets → Prefilter Rules → Decryption → Security Intelligence → Identity → Access Control

Deploy

Advanced Deploy | Ignore warnings | Deploy All

FPR2120\_FTD | Ready for Deployment | 1 device

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.

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Objects' tab is active, and the 'Snort 3 All Rules' sub-tab is selected. The main content area is titled 'All Rules' and shows a list of rules. A 'Tasks' dropdown menu is open, displaying options such as 'Upload Snort 3 rules', 'Convert Snort 2 rules and import', 'Convert Snort 2 rules and download', and 'Add Rule Groups'. The table below shows the following rules:

Rule Actions	Info	Rule Action	Assigned Groups
50,094 rules			
<input type="checkbox"/>	GID:SID		
<input type="checkbox"/>	148:2	(cip) CIP data is non-conforming to ODVA standard	Disable (Default)
<input type="checkbox"/>	133:3	(dce_smb) SMB - bad SMB message type	Disable (Default)

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.

Add Custom Rules

Drag and drop a file here or click to browse  
.rules and .txt files are supported

File Name  
custom-rules.txt | Replace File

Associate Rules to Rule Groups 1 Selected

Search

All Snort 2 Converted Global

Create New Custom Rule Group

Choose the appropriate action.

Merge Rules  
Merges any extra rules with the existing rules in the rule group.

Replace all rules in the group with file contents  
Replaces the rules which are already present in a custom intrusion rule group with the new rules

Cancel OK

Cancel Next

Aggiungi regola personalizzata

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

Add Custom Rules

### Summary

✓ 1 new rule

2000:1000000

Download the summary file.

Back Finish

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.

Firewall Management Center  
Objects / Intrusion Rules / Snort 3 All Rules

Overview Analysis Policies Devices Objects Integration Deploy Search Settings Help admin

Snort 2 All Rules Snort 3 All Rules

< Intrusion Policy Back To Top

All Rules

- Local Rules (1 group)
  - All Snort 2 Converted Global
- MITRE (1 group)
- ATT&CK Framework (1 group)
- Enterprise (13 groups)
- Rule Categories (9 groups)

Local Rules / All Snort 2 Converted Global

Description Group created for custom rules enabled in snort 2 version

Rule Actions Search by CVE, SID, Reference Info, or Rule Message Tasks

1 rule

Rule	GID:SID	Info	Rule Action	Assigned Groups	Alert Configuration
2000:1000000	custom_http_sig		Disable (Default)	All Snort 2 Converted Glo...	None

alert tcp any any <-> any any ( sid:1000000; gid:2000; flow:established,to\_client; raw\_data; content:'username'; msg:'custom\_http\_sig'; classtype:unknown; rev:3; )

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. Distribuisce 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.

192.168.20.1

192.168.20.1/test.txt



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.

Firewall Management Center  
Analysis / Intrusions / Events

Overview **Analysis** Policies Devices Objects Integration

Deploy 🔍 ⚙️ 🌐 admin 🔒 **SECURE**

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

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

No Search Constraints [\(Edit Search\)](#)

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

Jump to...

	Time X	Priority X	Impact X	Inline Result X	Reason X	Source IP X	Source Country X	Destination IP X	Destination Country X	Source Port / ICMP Type X	Destination Port / ICMP Code X	SSL Status X	VLAN ID X	Message X	Classification X	Generat
▼	2024-04-06 14:30:48	low	Unknown	<b>Block</b>		192.168.20.1		192.168.10.1		80 (http) / tcp	50103 / tcp			<b>custom_http_sig (2000:1000000:3)</b>	Unknown Traffic	Standar

Evento Intrusion

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

Firewall Management Center  
Analysis / Intrusions / Events

Overview **Analysis** Policies Devices Objects Integration

Deploy 🔍 ⚙️ 🌐 admin 🔒 **SECURE**

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

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

No Search Constraints [\(Edit Search\)](#)

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

Event Information

Message **custom\_http\_sig (2000:1000000:3)**

Time 2024-04-06 14:31:26

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 50103 / 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:1000000; gid:2000; flowestablished,to\_client; raw\_data; content:"usernaa"; asg:"custoa\_http\_sig"; classtype:unknown; rev:3; )

Actions

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).