

# Filtrare le regole di ordinamento in base all'SRU e alla versione LSP dei dispositivi Firepower gestiti da FMC

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Procedura per filtrare le regole di tipo Snort](#)

---

## Introduzione

In questo documento viene descritto come filtrare le regole di ordinamento in base alla versione Cisco Secure Rule Update (SRU) e Link State Packet (LSP) di dispositivi firepower gestiti da Firepower Management Center (FMC).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di Snort open-source
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

### Componenti usati

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

- Questo articolo è applicabile a tutte le piattaforme Firepower
- Cisco Firepower Threat Defense (FTD) con software versione 7.0.0
- Firepower Management Center Virtual (FMC) con software versione 7.0.0

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

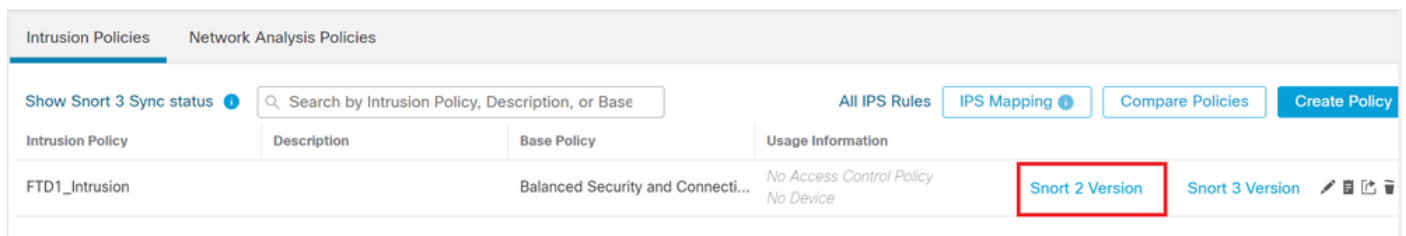
Nel contesto dei sistemi di rilevamento intrusioni (IDS) e dei sistemi di prevenzione delle intrusioni (IPS), "SID" sta per "Signature ID" o "Snort Signature ID".

Il SID (Snort Signature ID) è un identificativo univoco assegnato a ogni regola o firma all'interno del relativo set di regole. Queste regole vengono utilizzate per rilevare modelli o comportamenti specifici nel traffico di rete che possono indicare attività dannose o minacce alla sicurezza. Ogni regola è associata a un SID per semplificare il riferimento e la gestione.

Per informazioni su Snort open-source, visitate il sito Web [SNORT](#).

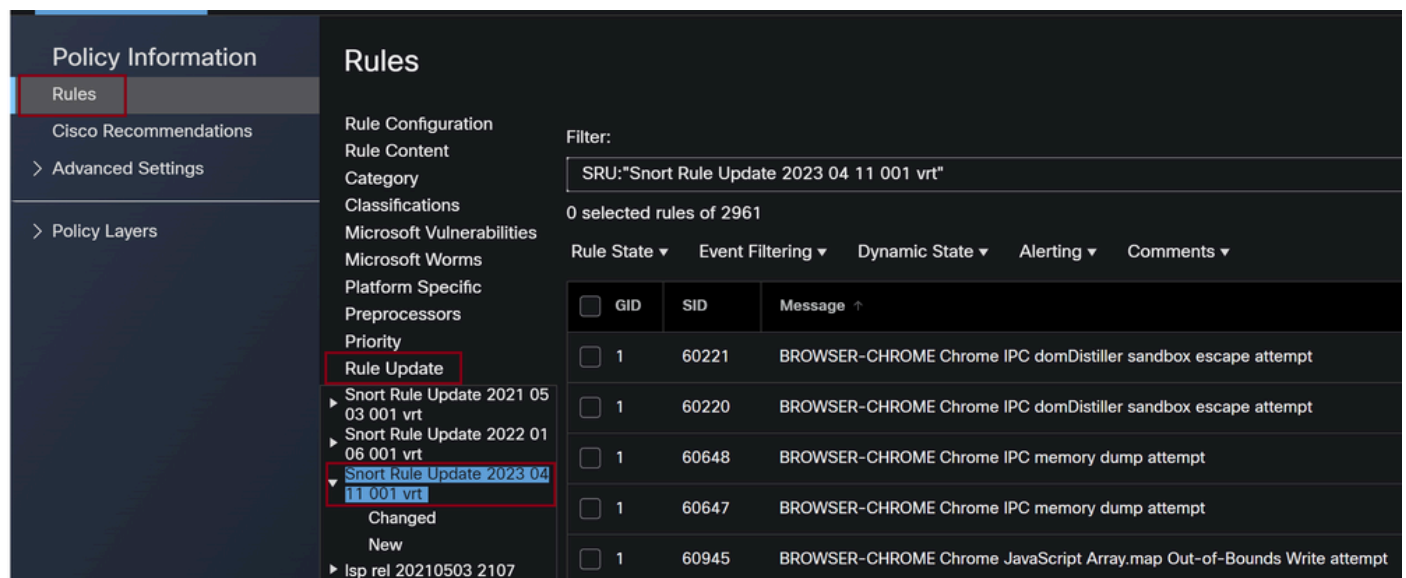
## Procedura per filtrare le regole di tipo Snort

Per visualizzare i SID della regola Snort 2, passare a **FMC Policies > Access Control > Intrusion**, quindi fate clic sull'opzione **SNORT2** nell'angolo superiore destro, come mostrato nell'immagine:

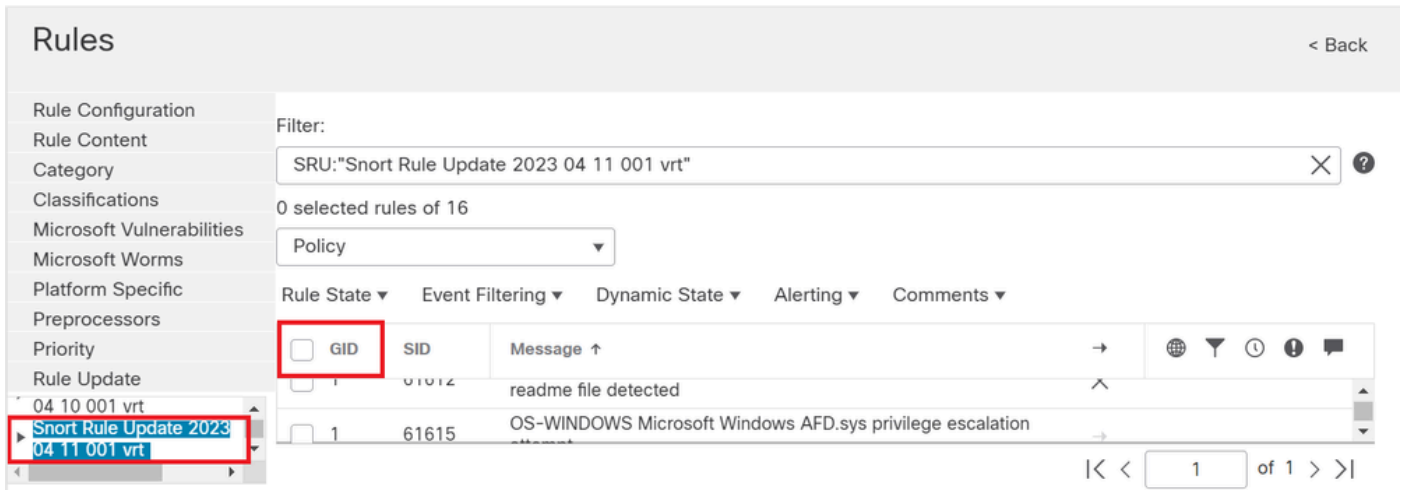


Snort 2

Passa a **Rules > Rule Update** e selezionare l'ultima data utile per filtrare il SID.

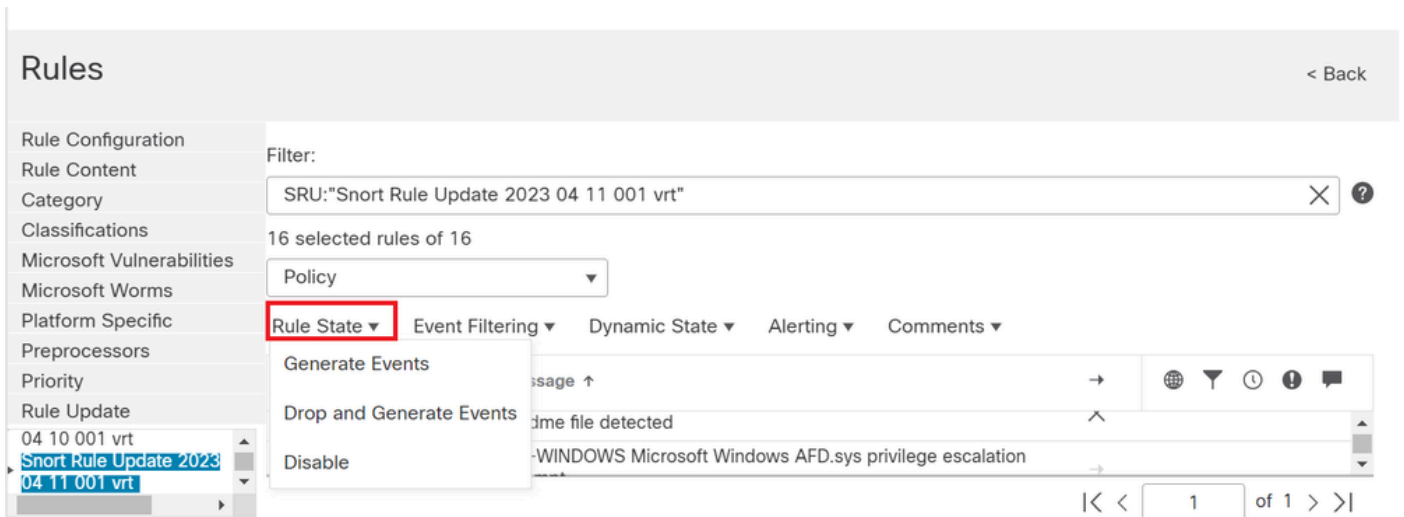


Aggiornamento regola



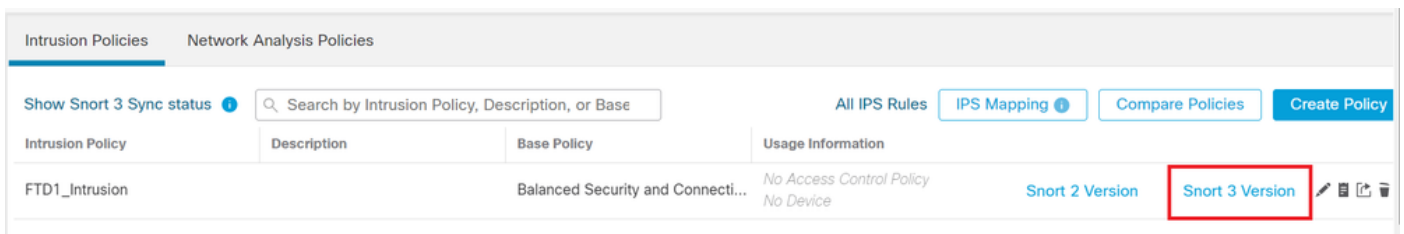
Sid disponibili sotto snort rules

Selezionare un'opzione richiesta in **Rule State** come mostrato nell'immagine.



Selezione degli stati delle regole

Per visualizzare i SID della regola Snort 3, passare a **FMC Policies > Access Control > Intrusion**, quindi fare clic sull'opzione SNORT3 nell'angolo superiore destro, come mostrato nell'immagine:



Snort. 3

Passa a **Advanced Filters** e selezionare la data più recente per filtrare il SID come mostrato nell'immagine.

< Intrusion Policy

Policy Name  Used by: No Access Control Policy | No Device

Mode  Base Policy Balanced Security and Connectivity

Disabled 39249 | Alert 470 | Block 9151 | Overridden 0 | Rewrite 0 | Pass 0 | Drop 0 | Reject 0

Rule Groups Back To Top

50 items  Excluded | Included | Overridden

All Rules Reco

> Browser (6 groups)

> Server (8 groups)

All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action

48,870 rules Preset Filters: 470 Alert rules | 9,151 Block rules | 39,249 Disabled rules | 0 Overridden rules

Advanced Filters

<input type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups
>	<input type="checkbox"/> 1:28496	<a href="#">BROWSER-IE Microsoft Internet Explore...</a>	<input type="text" value="Alert (Default)"/>	Browser/Internet Explo...

Ordina 3 filtri

## Advanced Filters ?

LSP

Select...

Show Only \*  New  Changed

Classifications

Select...

Microsoft

Vulnerabilities

Select...

Cancel

OK

LSP in filtro avanzato

## Advanced Filters ?

LSP

Show Only \*  New  Changed

Classifications

Microsoft Vulnerabilities

Cancel

Versione LSP

### All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action

22 ▾ | 48,870 rules    Preset Filters: 0 Alert rules | **11 Block rules** | 11 Disabled rules | 0 Overridden rules | [Advanced Filters](#)

<input type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups
<input type="checkbox"/>	1:300509	MALWARE-BACKDOOR Win.Backdoor...	Block (Default)	Malware/Backdoor

Filtro preimpostato per SID

Selezionare un'opzione richiesta in `Rule state` come mostrato nell'immagine.

### All Rules

All rules assigned to current intrusion policy irrespective of rule group

Rule Action

22  | 22 ▾ | 48,870 rules    Preset Filters: 0 Alert rules | 11 Block rules | 11 Disabled rules | 0 Overridden rules | [Advanced Filters](#)

<input checked="" type="checkbox"/>	GID:SID	Info	Rule Action	Assigned Groups
<input checked="" type="checkbox"/>	1:300509	MALWARE-BACKDOOR Win.Backdoor...	Block (Default)	Malware/Backdoor

Azione regola

## 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).