

Filtern von Snort-Regeln basierend auf der SRU- und LSP-Version von FirePOWER-Geräten, die von FMC verwaltet werden

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Verfahren zum Filtern von Snort-Regeln](#)

Einleitung

In diesem Dokument wird beschrieben, wie Snort-Regeln basierend auf der Cisco Secure Rule Update (SRU)- und Link State Packet (LSP)-Version von Firepower-Geräten gefiltert werden, die vom FirePOWER Management Center (FMC) verwaltet werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse von Open-Source Snort
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Dieser Artikel gilt für alle Firepower-Plattformen.
- Cisco Firepower Threat Defense (FTD) mit der Softwareversion 7.0.0
- FirePOWER Management Center Virtual (FMC) mit der Softwareversion 7.0.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

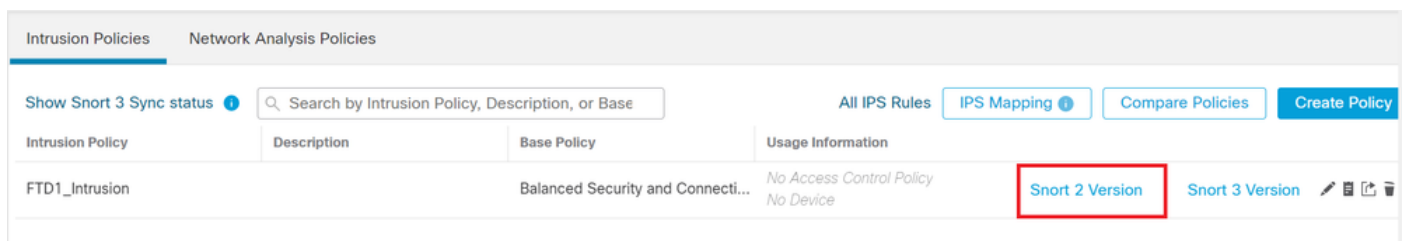
Im Kontext von Intrusion Detection Systemen (IDS) und Intrusion Prevention Systemen (IPS) steht "SID" für "Signature ID" oder "Snort Signature ID".

Eine Snort Signature ID (SID) ist eine eindeutige ID, die jeder Regel oder Signatur innerhalb ihres Regelsatzes zugewiesen wird. Diese Regeln werden verwendet, um bestimmte Muster oder Verhaltensweisen im Netzwerkverkehr zu erkennen, die auf schädliche Aktivitäten oder Sicherheitsbedrohungen hinweisen können. Jede Regel ist mit einer SID verknüpft, um den Zugriff und die Verwaltung zu vereinfachen.

Weitere Informationen zu Open-Source Snort finden Sie auf der [SNORT-Website](#).

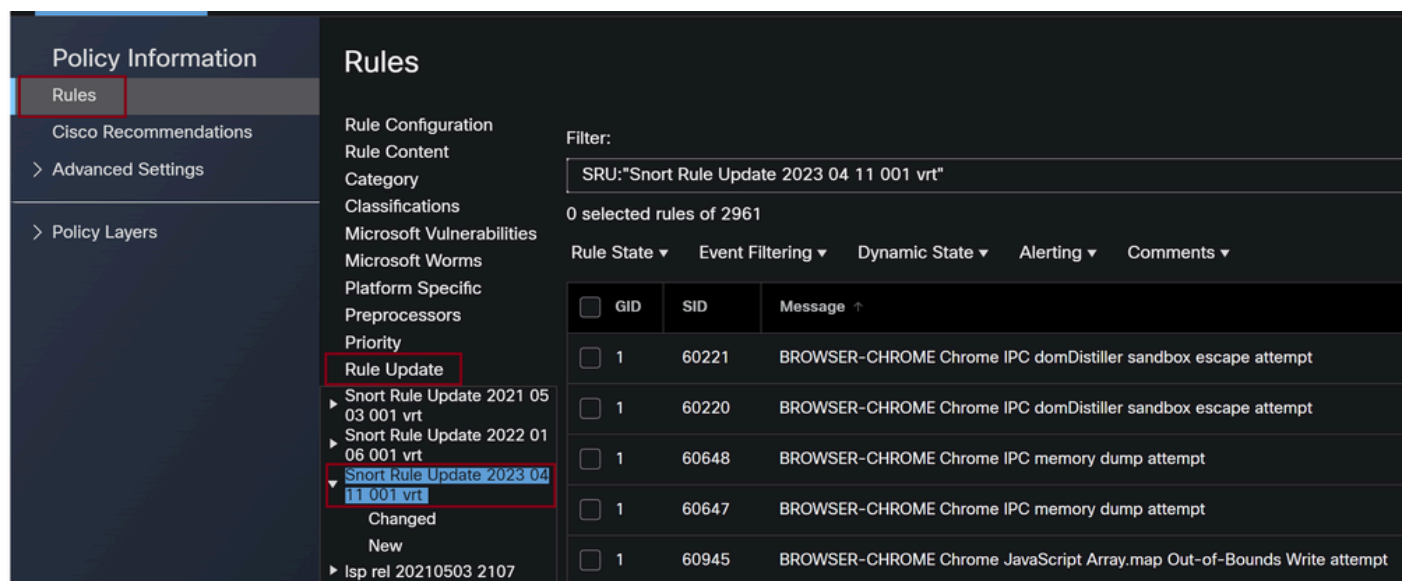
Verfahren zum Filtern von Snort-Regeln

Um die Snort 2-Regel-SIDs anzuzeigen, navigieren Sie zu **FMC Policies > Access Control > Intrusion**, Klicken Sie anschließend auf die **SNORT2-Option** in der rechten oberen Ecke, wie im Bild gezeigt:



Snort 2

Navigieren Sie zu **Rules > Rule Update** und wählen Sie das späteste Datum aus, um die SID zu filtern.



Regelaktualisierung

Rules

Rule Configuration

Rule Content

Category: SRU:"Snort Rule Update 2023 04 11 001 vrt"

Classifications: 0 selected rules of 16

Microsoft Vulnerabilities: Policy

Microsoft Worms

Platform Specific: Rule State, Event Filtering, Dynamic State, Alerting, Comments

Preprocessors

Priority: GID, SID, Message ↑

Rule Update: 04 10 001 vrt, **Snort Rule Update 2023 04 11 001 vrt**

Table:

Rule State	SID	Message
<input type="checkbox"/>	61615	readme file detected
<input type="checkbox"/>	1	OS-WINDOWS Microsoft Windows AFD.sys privilege escalation

Page 1 of 1

Verfügbare Sids gemäß Snort-Regeln

Wählen Sie die gewünschte Option unter **Rule State** wie im Bild dargestellt.

Rules

Rule Configuration

Rule Content

Category: SRU:"Snort Rule Update 2023 04 11 001 vrt"

Classifications: 16 selected rules of 16

Microsoft Vulnerabilities: Policy

Microsoft Worms

Platform Specific: **Rule State**, Event Filtering, Dynamic State, Alerting, Comments

Preprocessors

Priority: Generate Events, Drop and Generate Events, Disable

Rule Update: 04 10 001 vrt, Snort Rule Update 2023 04 11 001 vrt

Table:

Rule State	SID	Message
<input type="checkbox"/>	61615	readme file detected
<input type="checkbox"/>	1	OS-WINDOWS Microsoft Windows AFD.sys privilege escalation

Page 1 of 1

Auswählen von Regelzuständen

Um die Snort 3-Regel-SIDs anzuzeigen, navigieren Sie zu **FMC Policies > Access Control > Intrusion**, klicken Sie anschließend auf die **SNORT3-Option** in der rechten oberen Ecke, wie in der Abbildung dargestellt:

Intrusion Policies | Network Analysis Policies

Show Snort 3 Sync status

Search by Intrusion Policy, Description, or Base

All IPS Rules | IPS Mapping | Compare Policies | Create Policy

Intrusion Policy	Description	Base Policy	Usage Information
FTD1_Intrusion	Balanced Security and Connect...	No Access Control Policy No Device	Snort 2 Version Snort 3 Version

Snort 3

Navigieren Sie zu **Advanced Filters** und wählen Sie das **späteste Datum** aus, um die SID wie im Bild dargestellt zu filtern.

< 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	BROWSER-IE Microsoft Internet Explore...	<input type="text" value="Alert (Default)"/>	Browser/Internet Explo...

Snort 3-Filter

Advanced Filters ?

LSP

Select...

Show Only * New Changed

Classifications

Select...

Microsoft Vulnerabilities

Select...

Cancel

OK

LSP mit erweitertem Filter

Advanced Filters ?

LSP

Show Only * New Changed

Classifications

Microsoft Vulnerabilities

Cancel

LSP-Version

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

Voreingestellter Filter für Sid's

Wählen Sie die gewünschte Option unter **Rule state** wie im Bild dargestellt.

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

Regelaktion

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.