

Zusätzliche Snort 3-Regelaktionen auf FMC konfigurieren

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Funktionsdetails](#)

[FMC-Einführung](#)

Einleitung

In diesem Dokument wird die Unterstützung von FirePOWER Management Center (FMC) für zusätzliche Snort 3-Regelaktionen beschrieben, die in Version 7.1 hinzugefügt wurden.

Hintergrundinformationen

Obwohl die FirePOWER Threat Defense (FTD) in 7.0 sieben Intrusion Policy-Regelaktionen Alert/Disable/Block/Reject/Rewrite/Pass/Drop unterstützt, unterstützte FMC nur drei Snort 3-Regelaktionen: "Alert" (Warnen), "Disable" (Deaktivieren) und "Block" (Blockieren).

Ab Firepower 7.1.0 unterstützt FMC die Konfiguration neuer Regelaktionen.

Voraussetzungen

Anforderungen

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

- Kenntnisse von Open-Source Snort
- FirePOWER Management Center (FMC) 7.1.0+
- Firepower Threat Defense (FTD) 7.0.0+

Verwendete Komponenten

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

- Dieses Dokument gilt für alle Firepower-Plattformen mit Snort 3
- Cisco Firepower Threat Defense Virtual (FTD) mit der Softwareversion 7.4.2
- FirePOWER Management Center Virtual (FMC) mit der Softwareversion 7.4.2

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.

Funktionsdetails

Die neu hinzugefügten Snort 3-Regelaktionen und ihre Beschreibungen sind wie folgt:

Bestanden: Es wird kein Ereignis generiert. Das Paket kann ohne weitere Evaluierung durch nachfolgende Snort-Regeln weitergeleitet werden.

Verwerfen: Generiert Ereignis, verwirft passendes Paket und blockiert keinen weiteren Datenverkehr in dieser Verbindung.

Ablehnen: Generiert Ereignis, verwirft passendes Paket, blockiert weiteren Datenverkehr in dieser Verbindung und sendet TCP-Reset oder ICMP-Port unerreichbar an Quell- und Ziel-Hosts.

Umschreiben: Generiert Ereignis und überschreibt Paketinhalt basierend auf der Ersetzungsoption in der Regel.

FMC-Einführung

Um die Snort 3-Regeln in einer Richtlinie für Sicherheitsrisiken anzuzeigen, navigieren Sie **FMC Policies > Access Control > Intrusion**, anschließend zur Option **Snort 3 Version** in der oberen rechten Ecke der Richtlinie, wie im Bild gezeigt:



Snort 3-Version

Klicken Sie auf **Basisrichtlinie > Alle Regeln**, um die Standardaktionen aller vom System definierten Snort 3-Regeln anzuzeigen.

< Policies / Intrusion / FTD_Intrusion

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

Base Policy: Balanced Security and Connectivity Mode: Prevention

Active Rules 9693 Alert 474 Block 9219

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

Balanced Security and Connectivity

50 items

All Rules

49,532 rules

Presets: Alert (474) | Block (9,219) | Disabled (39,839) | Overridden (0) | Advanced Filters

GID:SID	Rule Details	Rule Action	Assigned Groups
1:28496	BROWSER-IE Microsoft Internet Explorer crea...	Alert (Default)	Malicious File,Drive-by Co...
1:32478	BROWSER-IE Microsoft Internet Explorer CSe...	Alert (Default)	Malicious File,Drive-by Co...
1:32479	BROWSER-IE Microsoft Internet Explorer CSe...	Alert (Default)	Malicious File,Drive-by Co...
1:26633	BROWSER-IE Microsoft Internet Explorer html...	Alert (Default)	Malicious File,Internet Expl...
1:31621	BROWSER-IE Microsoft Internet Explorer onre...	Alert (Default)	Malicious File,Drive-by Co...
1:31622	BROWSER-IE Microsoft Internet Explorer onre...	Alert (Default)	Malicious File,Drive-by Co...

Basisrichtlinie

Um die Regelaktion in eine dieser neuen Regelaktionen zu ändern, navigieren Sie zu Regelüberschreibungen > Alle Regeln, und wählen Sie die Regelaktion aus dem Dropdown-Menü für die ausgewählte Regel aus.

< Policies / Intrusion / FTD_Intrusion

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

Base Policy: Balanced Security and Connectivity Mode: Prevention

Active Rules 9693 Alert 474 Block 9219

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

Rule Overrides

102 items

All Rules

49,532 rules

Presets: Alert (474) | Block (9,219) | Disabled (39,839) | Overridden (0) | Advanced Filters

GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
1:28496	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File,Drive...
1:32478	BROWSER-IE Microsoft Internet ...	Block	Base Policy	Malicious File,Drive...
1:32479	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File,Drive...
1:26633	BROWSER-IE Microsoft Internet ...	Rewrite	Base Policy	Malicious File,Inter...
1:31621	BROWSER-IE Microsoft Internet ...	Drop	Base Policy	Malicious File,Drive...
1:31622	BROWSER-IE Microsoft Internet ...	Reject	Base Policy	Malicious File,Drive...
1:31622	BROWSER-IE Microsoft Internet ...	Disable	Base Policy	Malicious File,Drive...
1:31622	BROWSER-IE Microsoft Internet ...	Revert to default	Base Policy	Malicious File,Drive...

Zusätzliche Regelaktionen

< Policies / Intrusion / FTD_Intrusion Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity Mode: Prevention Active Rules 9693 Alert 474 Block 9219

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

Rule Overrides Back To Top

102 items All x v Rule Action v Search by CVE, SID, Reference Info, or Rule Message

49,532 rules Presets: Alert (474) | Block (9,219) | Disabled (39,839) | Overridden (0) | Advanced Filters

✔ Rule action changed successfully x

	GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
<input type="checkbox"/>	1:28496	BROWSER-IE Microsoft Internet ...	Reject v	Rule Override	Malicious File, Drive... 🔗 🗨
<input type="checkbox"/>	1:32478	BROWSER-IE Microsoft Internet ...	Alert (Default) v	Base Policy	Malicious File, Drive... 🔗 🗨
<input type="checkbox"/>	1:32479	BROWSER-IE Microsoft Internet ...	Alert (Default) v	Base Policy	Malicious File, Drive... 🔗 🗨
<input type="checkbox"/>	1:26633	BROWSER-IE Microsoft Internet ...	Alert (Default) v	Base Policy	Malicious File, Inter... 🔗 🗨

Ändern der Regelaktion

Die überschriebenen Regeln finden Sie unter Rule Overrides > Overridden Rules.

< Policies / Intrusion / FTD_Intrusion Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity Mode: Prevention Active Rules 9693 Alert 473 Block 9219 Others 1

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

Rule Overrides Back To Top

102 items All x v Rule Action v Search by CVE, SID, Reference Info, or Rule Message

1 rule Presets: Alert (0) | Block (0) | Disabled (0) | **Overridden (1)** | Advanced Filters | Reject (1)

	GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
<input type="checkbox"/>	1:28496	BROWSER-IE Microsoft Internet ...	Reject v	Rule Override	Malicious File, Drive... 🔗 🗨

Außerkräftsetzte Regeln

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.