Zusätzliche Snort 3-Regelaktionen auf FMC konfigurieren

Inhalt

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.

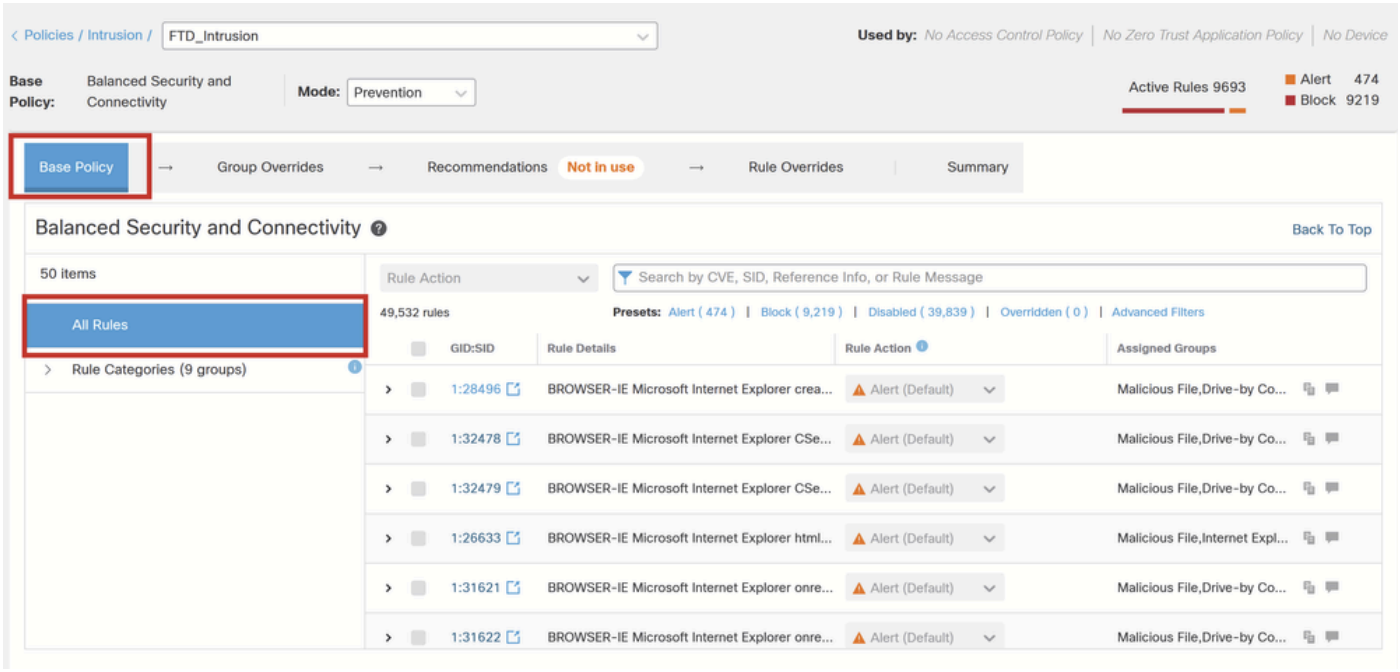
Umschreiben: Generiert Ereignis und überschreibt Paketinhalt basierend auf der Ersetzungsoption in der Regel.

FMC-Einführung

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

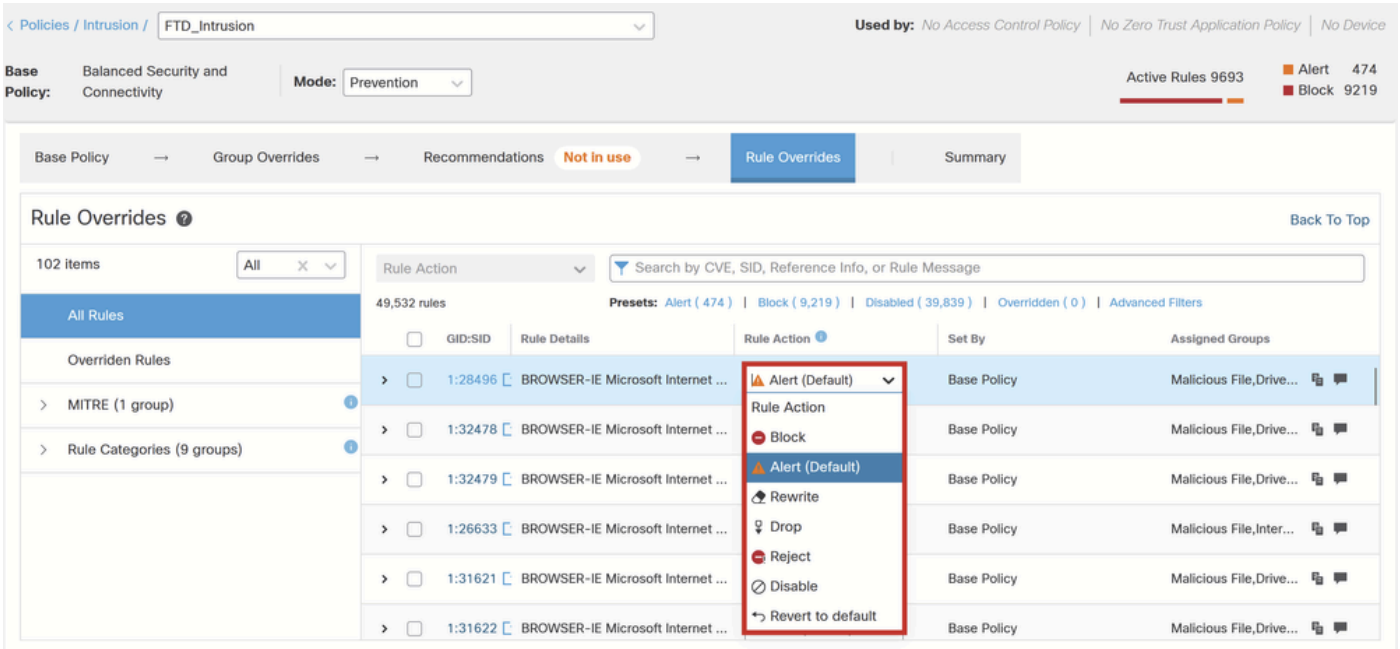
Snort 3-Version

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

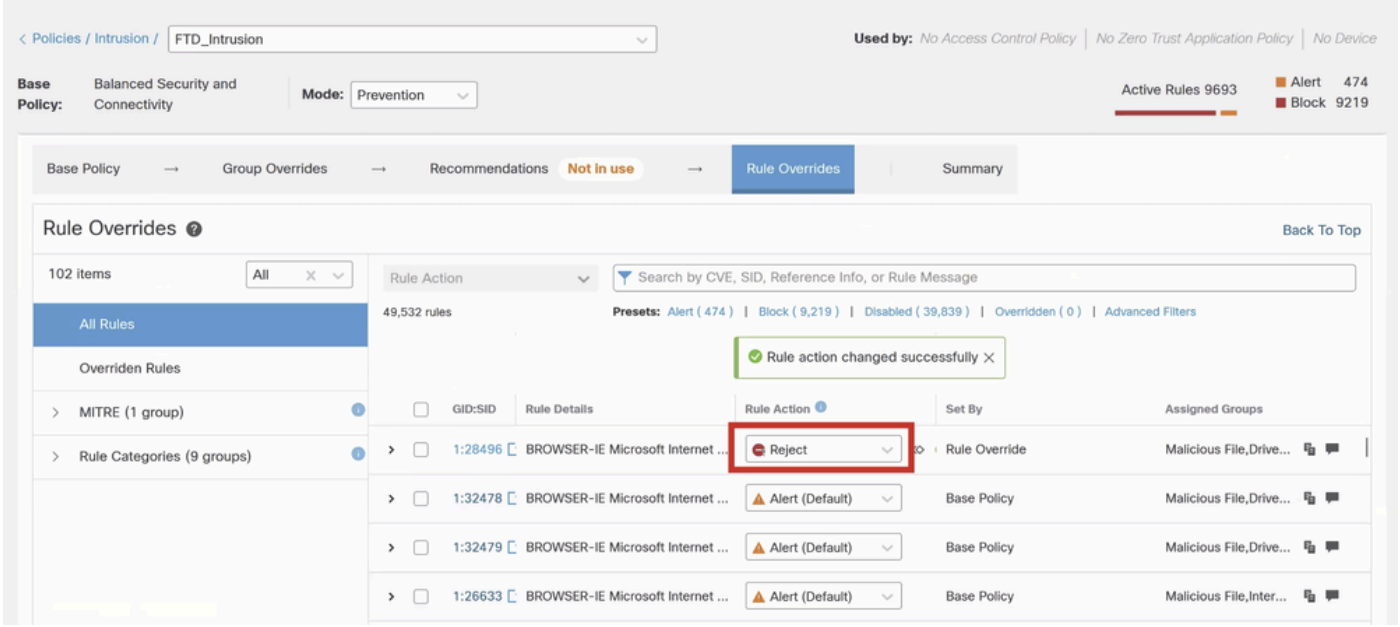


Basisrichtlinie

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.

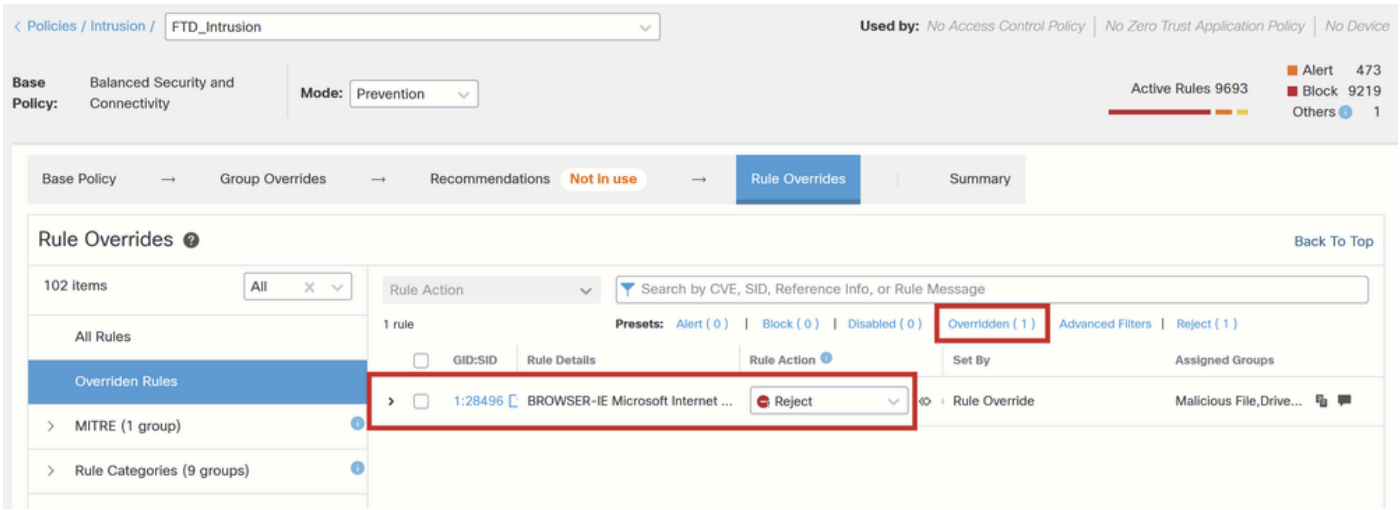


Zusätzliche Regelaktionen



Ändern der Regelaktion

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



Außerkraftsetzte 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.