Configura azioni aggiuntive delle regole dello script 3 in FMC

Sommario

Introduzione

In questo documento viene descritto il supporto di Firepower Management Center (FMC) per la funzionalità aggiuntiva di Snort 3 rule actions aggiunta nella versione 7.1.

Premesse

Sebbene Firepower Threat Defense (FTD) supporti sette azioni delle regole per le intrusioni Alert/Disable/Block/Reject/Pass/Drop in 7.0, FMC ha supportato solo tre azioni delle regole Snort 3: "Alert", "Disable" e "Block".

Da Firepower 7.1.0, FMC supporta la configurazione di nuove azioni regola.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:
· Conoscenza di Snort open-source
· Firepower Management Center (FMC) 7.1.0+
· Firepower Threat Defense (FTD) 7.0.0+

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:
· Questo documento è relativo a tutte le piattaforme Firepower che eseguono lo Snort 3
· Cisco Firepower Threat Defense Virtual (FTD) con software versione 7.4.2
· Firepower Management Center Virtual (FMC) con software versione 7.4.2

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.

Dettagli funzionalità

Le nuove azioni della regola Snort 3 aggiunte e le relative descrizioni sono le seguenti:

Superato: Nessun evento generato, consente il passaggio del pacchetto senza un'ulteriore valutazione da parte delle successive regole Snort.

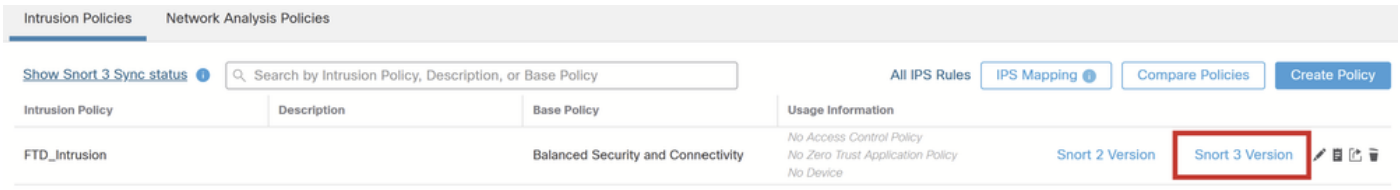
Drop: Genera un evento, scarta il pacchetto corrispondente e non blocca ulteriore traffico in questa connessione.

Rifiuta: Genera un evento, scarta il pacchetto corrispondente, blocca l'ulteriore traffico in questa connessione e invia agli host di origine e di destinazione il comando TCP reset o la porta ICMP non raggiungibile.

Riscrivi: Genera l'evento e sovrascrive il contenuto del pacchetto in base all'opzione di sostituzione nella regola.

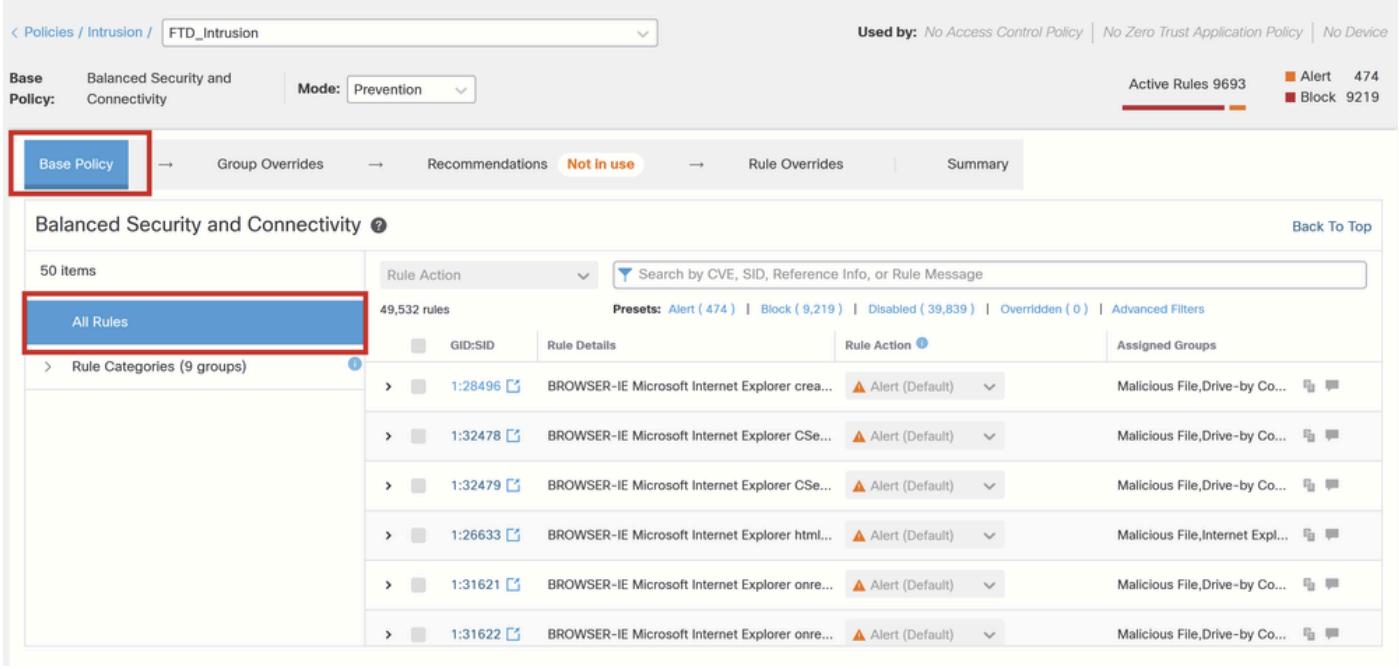
Scenario di FMC

Per visualizzare le regole Snort 3 in un criterio di intrusione, passare allaFMC Policies > Access Control > Intrusion,successiva opzione Snort 3 Version nell'angolo superiore destro del criterio, come mostrato nell'immagine:



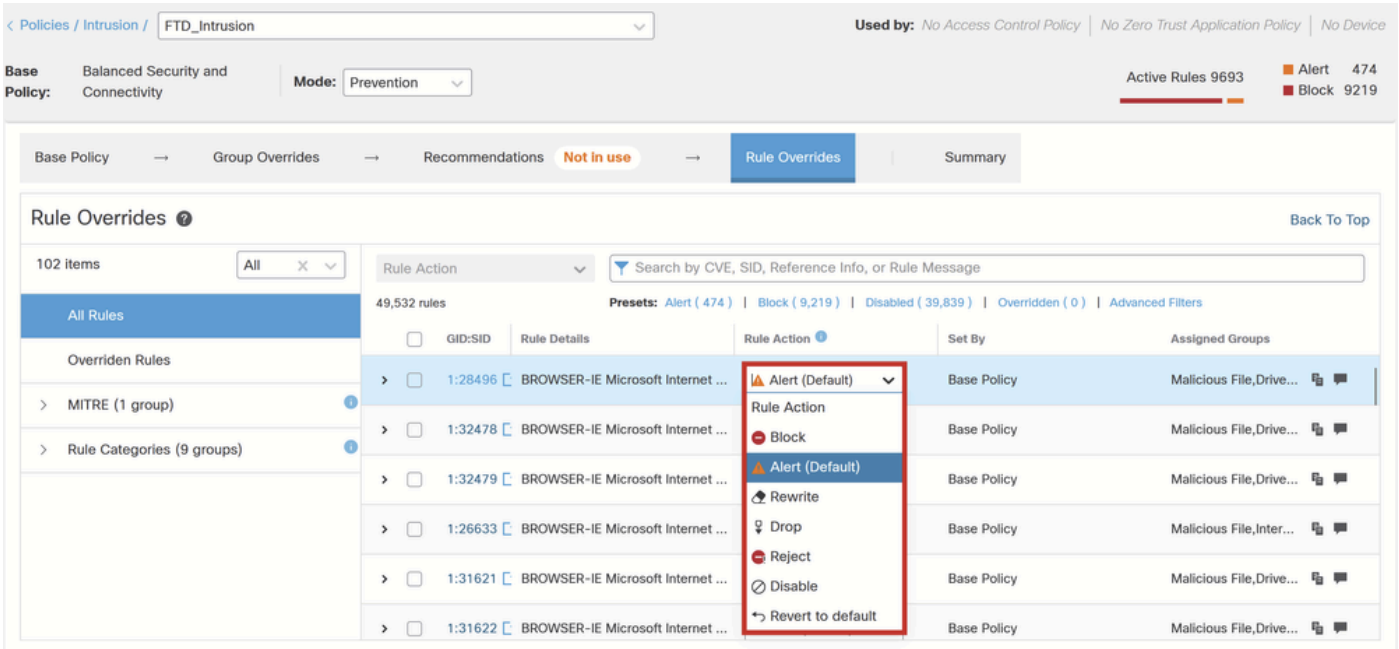
Versione Snort 3

Fare clic su Criteri di base > Tutte le regole per visualizzare le azioni predefinite di tutte le regole Snort 3 definite dal sistema.

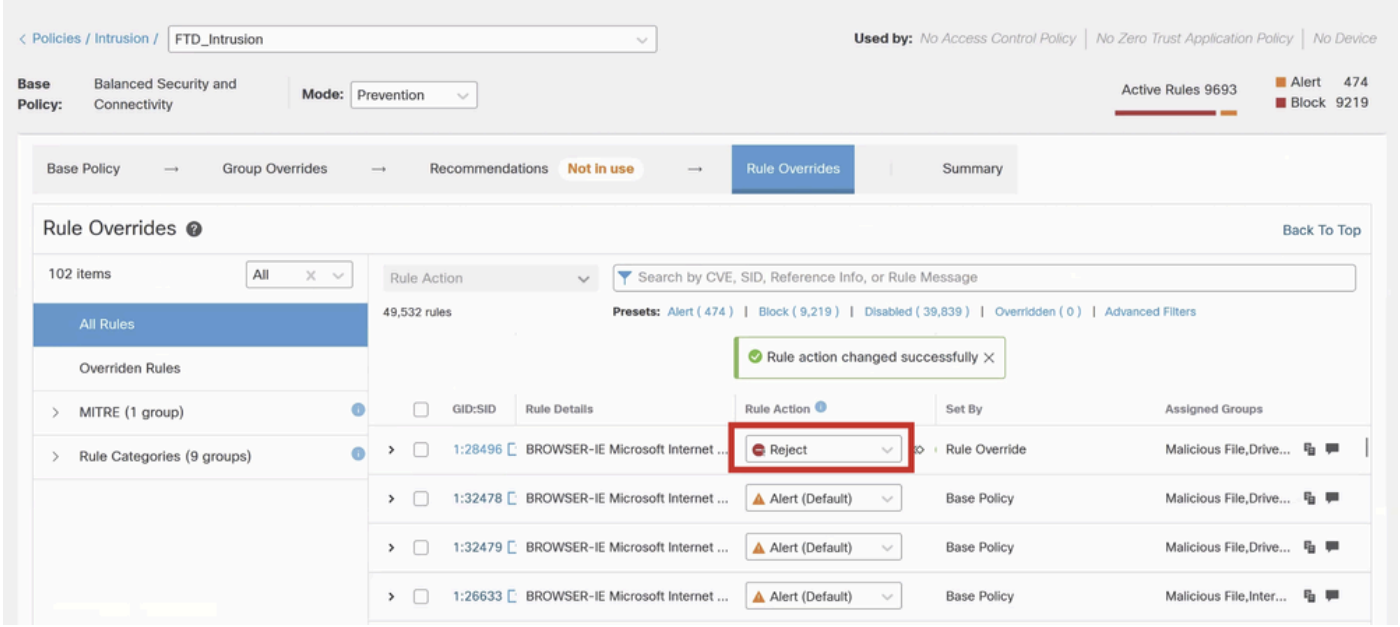


Criteri di base

Per modificare l'azione della regola in una delle nuove azioni della regola, passare a Sostituzioni regole > Tutte le regole e selezionare l'azione della regola dall'elenco a discesa della regola selezionata.

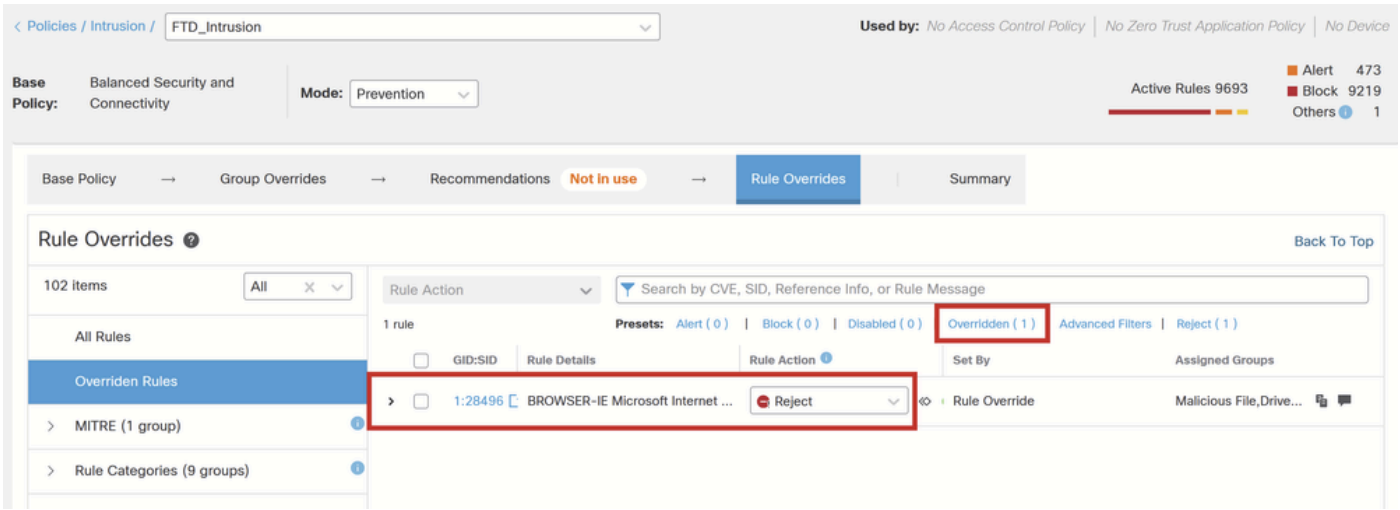


Azioni regola aggiuntive



Modifica dell'azione regola

Le regole sostituite sono disponibili in Sostituzioni regole > Regole sostituite.



Regole sostituite

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).