Regole personalizzate per lo snort locale su un sistema Cisco FireSIGHT

Sommario

Introduzione

Una regola locale personalizzata in un sistema FireSIGHT è una regola standard personalizzata Snort che viene importata in un formato di file di testo ASCII da un computer locale. Un sistema FireSIGHT consente di importare regole locali utilizzando l'interfaccia Web. La procedura per importare le regole locali è molto semplice. Tuttavia, per scrivere una regola locale ottimale, un utente richiede una conoscenza approfondita dei protocolli Snort e di rete.

Lo scopo di questo documento è quello di fornire alcuni suggerimenti e assistenza per la scrittura di una regola locale personalizzata. Le istruzioni sulla creazione di regole locali sono disponibili nel *Manuale per gli utenti di Snort,* disponibile su snort.org. Cisco consiglia di scaricare e leggere il Manuale dell'utente prima di scrivere una regola locale personalizzata.

> **Nota:** Le regole incluse in un pacchetto Sourcefire Rule Update (SRU) vengono create e testate dal Cisco Talos Security Intelligence and Research Group e sono supportate dal Cisco Technical Assistance Center (TAC). Cisco TAC non fornisce assistenza per la scrittura o l'ottimizzazione di una regola locale personalizzata. Tuttavia, in caso di problemi con la funzionalità di importazione delle regole del sistema FireSIGHT, contattare Cisco TAC.

> **Avviso:** Una regola locale personalizzata scritta in modo inadeguato può influire sulle prestazioni di un sistema FireSIGHT, con conseguente riduzione delle prestazioni dell'intera rete. Se si verificano problemi di prestazioni nella rete e sul sistema FireSIGHT sono abilitate alcune regole locali personalizzate, Cisco consiglia di disabilitarle.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza delle regole Snort e del sistema FireSIGHT.

Componenti usati

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

- Centro di gestione FireSIGHT (noto anche come centro di difesa)
- Software versione 5.2 o successive

Utilizzo delle regole locali personalizzate

Importa regole locali

Prima di iniziare, è necessario verificare che le regole nel file non contengano caratteri di escape. L'utilità di importazione delle regole richiede che tutte le regole personalizzate vengano importate utilizzando la codifica ASCII o UTF-8.

Nella procedura seguente viene illustrato come importare le regole di testo standard locali da un computer locale:

1. Accedere alla pagina **Editor regole** passando a **Criteri > Intrusione > Editor regole**.

2. Fare clic su **Importa regole**. Viene visualizzata la pagina **Aggiornamenti regole**.

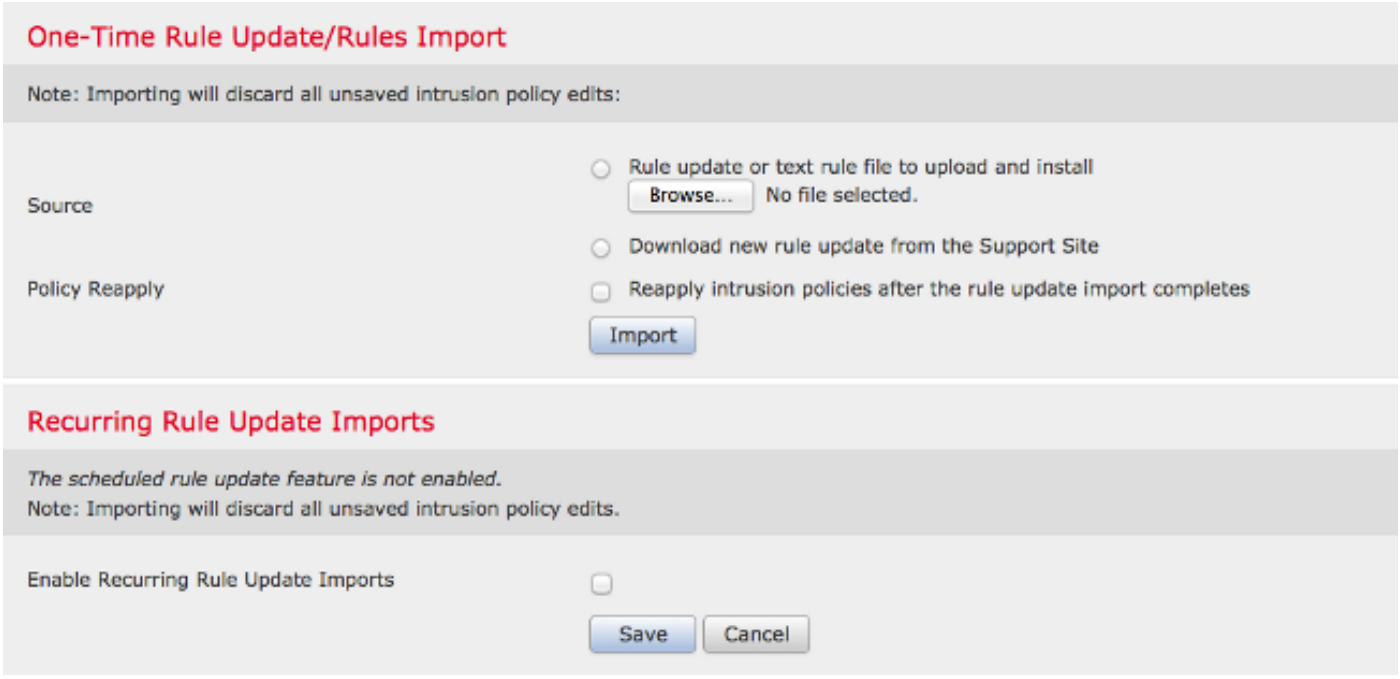


Figura: Schermata della pagina Aggiornamenti regole

3. Selezionare **Aggiornamento regole o file di regole di testo da caricare e installare** e fare clic su **Sfoglia** per selezionare il file di regole.

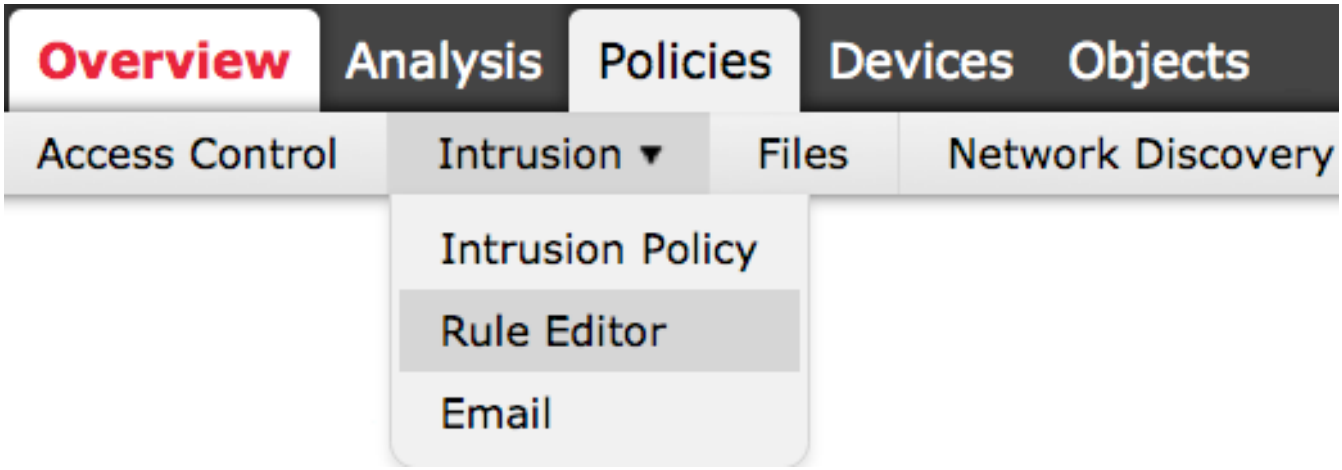
> **Nota:** Tutte le regole caricate vengono salvate nella categoria **regola locale**.

4. Fare clic su **Importa**. Il file delle regole viene importato.

> **Attenzione:** I sistemi FireSIGHT non utilizzano il nuovo set di regole per l'ispezione. Per attivare una regola locale, è necessario attivarla nel criterio intrusione e quindi applicarla.

Visualizza regole locali

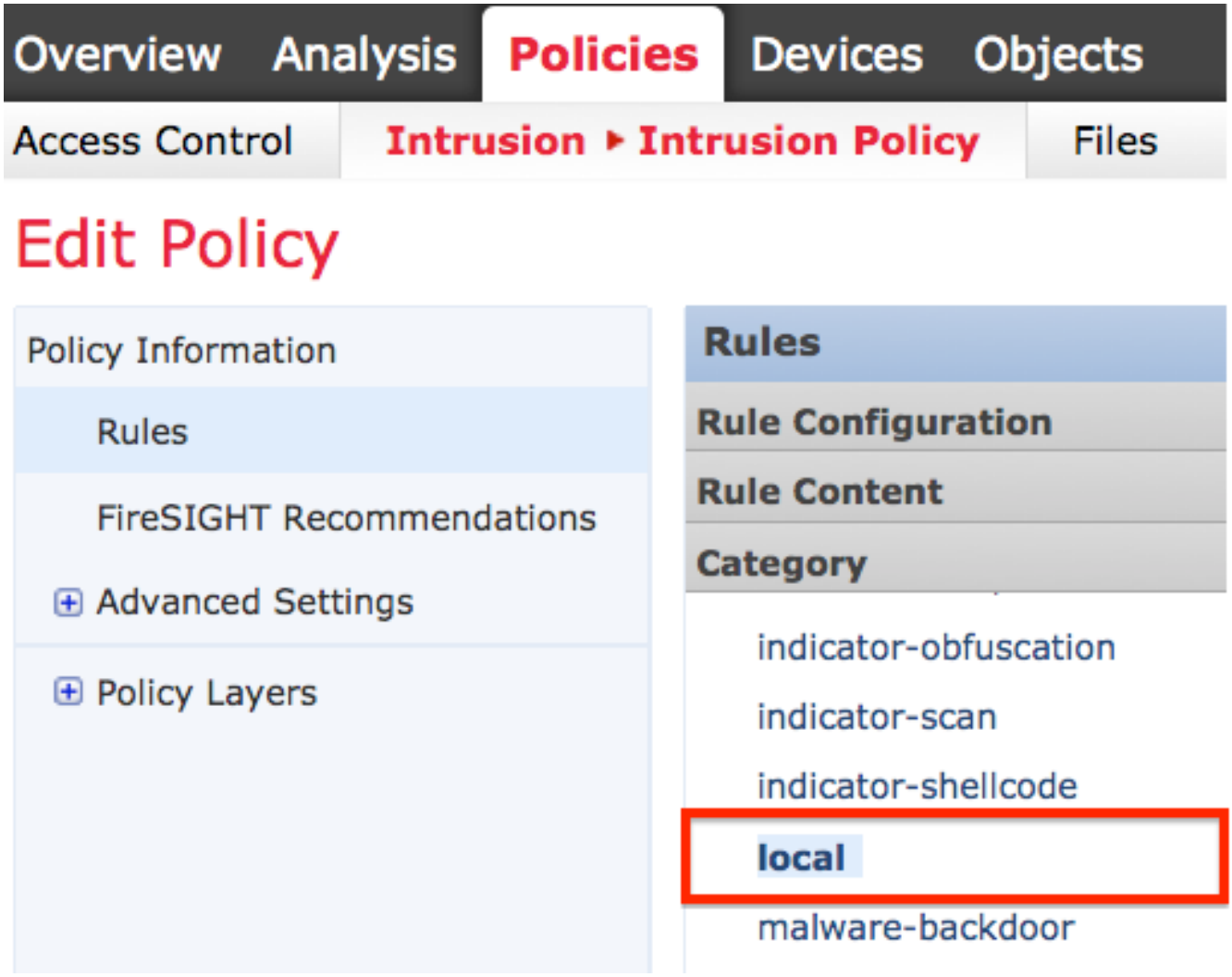
- Per visualizzare il numero di revisione per una regola locale corrente, passare alla pagina **Editor regole** (**Criteri** > **Intrusione** > **Editor regole**).



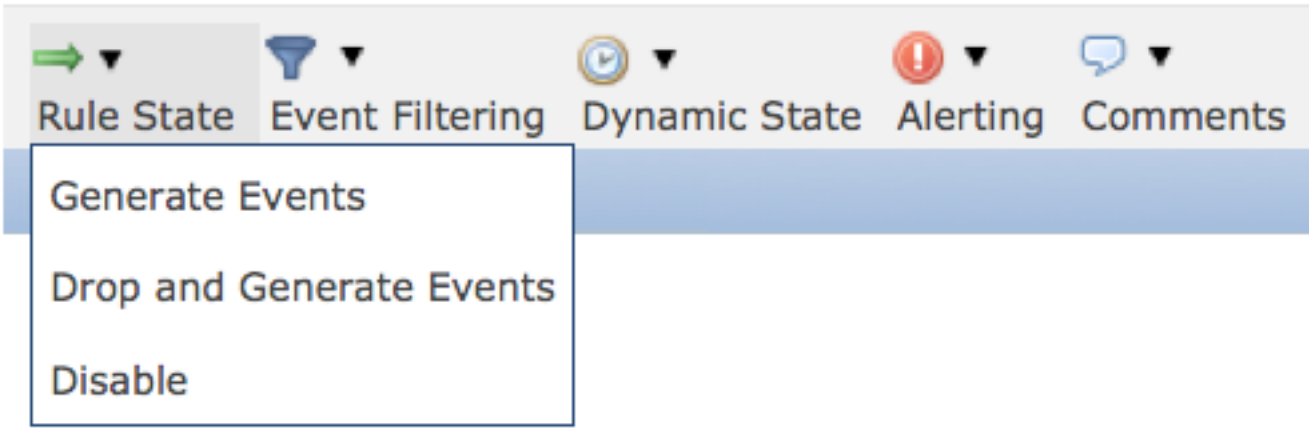
- Nella pagina Editor regole, fare clic sulla categoria **Regola locale** per espandere la cartella, quindi fare clic su **Modifica** accanto alla regola.
- Tutte le regole locali importate vengono salvate automaticamente nella categoria **delle regole locali**.

Abilita regole locali

- Per impostazione predefinita, il sistema FireSIGHT imposta le regole locali in uno stato disabilitato. È necessario impostare manualmente lo stato delle regole locali prima di poterle utilizzare nei criteri per le intrusioni.
- Per abilitare una regola locale, passare alla pagina Editor dei criteri (**Criteri** > **Intrusione** > **Criteri intrusione**). Selezionate **Regole** nel pannello sinistro. In **Categoria**, selezionare **locale**. Verranno visualizzate tutte le regole locali, se disponibili.



- Dopo aver selezionato le regole locali desiderate, selezionare uno stato per le regole.



- Una volta selezionato lo stato della regola, fare clic sull'opzione **Informazioni sui criteri** nel riquadro sinistro. Selezionare il pulsante **Commit modifiche**. Criteri intrusione convalidati.

  Nota: La convalida dei criteri ha esito negativo se si abilita una regola locale importata che utilizza la parola chiave di soglia deprecata in combinazione con la funzione di soglia degli eventi di intrusione in un criterio di intrusione.

Visualizza regole locali eliminate

- Tutte le regole locali eliminate vengono spostate dalla categoria delle regole locali alla categoria delle regole eliminate.
- Per visualizzare il numero di revisione di una regola locale eliminata, andare alla pagina **Editor regole**, fare clic sulla categoria **eliminata** per espandere la cartella, quindi fare clic sull'icona a forma di *matita* per visualizzare i dettagli della regola nella pagina **Editor regole**.

Numerazione delle regole locali

- Non è necessario specificare un Generatore (GID); in tal caso, è possibile specificare solo GID 1 per una regola di testo standard o 138 per una regola di dati riservati.
- Non specificare un ID snort (SID) o un numero di revisione quando si importa una regola per la prima volta. in questo modo si evitano collisioni con SID di altre regole, incluse quelle eliminate.
- Il centro di gestione FireSIGHT assegna automaticamente il successivo SID di regola personalizzata disponibile di 1000000 o superiore e un numero di revisione pari a 1.
- Se si tenta di importare una regola di intrusione con un SID maggiore di 2147483647, si verificherà un errore di convalida.
- Quando si importa una versione aggiornata di una regola locale precedentemente importata, è necessario includere il SID assegnato da IPS e un numero di revisione maggiore del numero di revisione corrente.
- Èpossibile ripristinare una regola locale eliminata importando la regola utilizzando il SID assegnato da IPS e un numero di revisione maggiore del numero di revisione corrente. Notare che il centro di gestione FireSIGHT incrementa automaticamente il numero di revisione quando si elimina una regola locale; si tratta di un dispositivo che consente di ripristinare le regole locali.

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).