Verifica di un elenco SID personalizzato dai sensori Firepower tramite l'interfaccia CLI e FMC

Introduzione

In questo documento viene descritto come ottenere un elenco SID personalizzato da Firepower Threat Defense (FTD) o dal modulo FirePOWER utilizzando la CLI e la GUI di FMC. Le informazioni SID sono disponibili nella GUI di FMC selezionando ***Oggetti > Regole intrusione***. In alcuni casi, è necessario ottenere un elenco di SID disponibili dalla CLI.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Firepower Threat Defense (FTD)
- Cisco ASA con servizi FirePOWER
- Cisco Firepower Management Center (FMC)
- Conoscenze base di Linux

Componenti usati

Le informazioni di questo documento si basano sulla seguente versione del software:

- Firepower Management Center 6.6.0
- Firepower Threat Defense 6.4.0.9
- Modulo FirePOWER 6.2.3.2

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.

Premesse

Una ***regola di intrusione*** è un insieme di parole chiave e argomenti che il sistema utilizza per rilevare i tentativi di sfruttare le vulnerabilità della rete. Quando il sistema analizza il traffico di rete, confronta i pacchetti con le condizioni specificate in ciascuna regola. Se i dati del pacchetto soddisfano tutte le condizioni specificate in una regola, la regola viene attivata. Se una regola è una regola di avviso, genera un evento intrusione. Se è una regola di accesso, ignora il traffico. Per una regola di eliminazione in una distribuzione inline, il sistema scarta il pacchetto e genera un evento. È possibile visualizzare e valutare gli eventi di intrusione dalla console Web di Firepower Management Center.

Il sistema Firepower fornisce due tipi di regole di intrusione: ***regole per gli oggetti condivisi*** e ***regole per il testo standard***. Il Cisco Talos Security Intelligence and Research Group (Talos) può

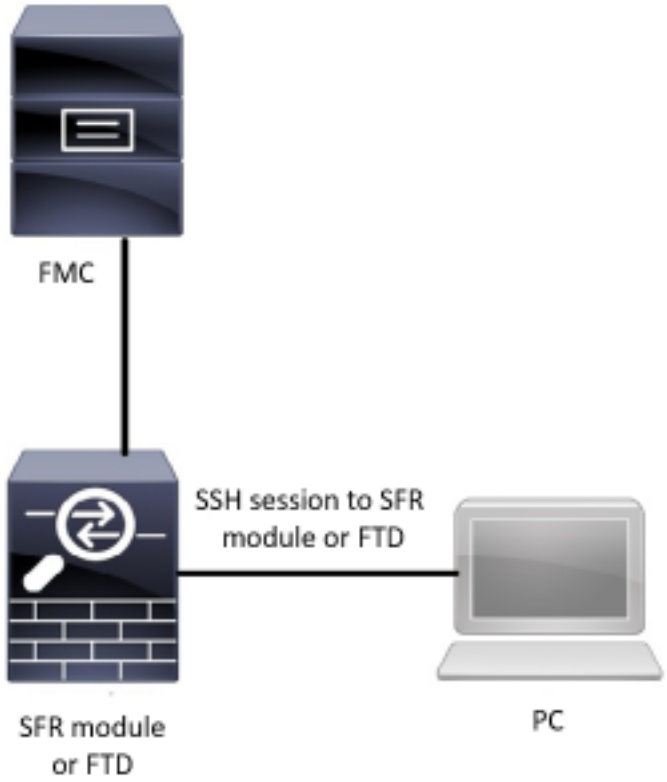
utilizzare regole di oggetto condiviso per rilevare attacchi alle vulnerabilità in modi diversi dalle tradizionali regole di testo standard. Non è possibile creare regole per oggetti condivisi. Quando le regole di intrusione vengono scritte da sole, è necessario creare regole di testo standard. Regole di testo standard personalizzate per ottimizzare i tipi di eventi che è possibile visualizzare. Scrivere regole e specificare il messaggio di evento della regola consente di identificare più facilmente il traffico che indica attacchi ed evasioni delle policy.

Quando si abilita una regola di testo standard personalizzata in un criterio per le intrusioni personalizzato, tenere presente che alcune parole chiave e alcuni argomenti della regola richiedono che il traffico venga prima decodificato o pre-elaborato in un determinato modo.

Una *regola locale personalizzata* su un sistema Firepower è una regola standard personalizzata Snort che viene importata in un formato di file di testo ASCII da un computer locale. Un sistema Firepower 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.

> Avviso: Prima di utilizzare le regole in un ambiente di produzione, accertarsi di utilizzare un ambiente di rete controllato per verificare le regole di intrusione scritte. Regole inadeguate in materia di intrusione possono compromettere gravemente le prestazioni del sistema

Esempio di rete



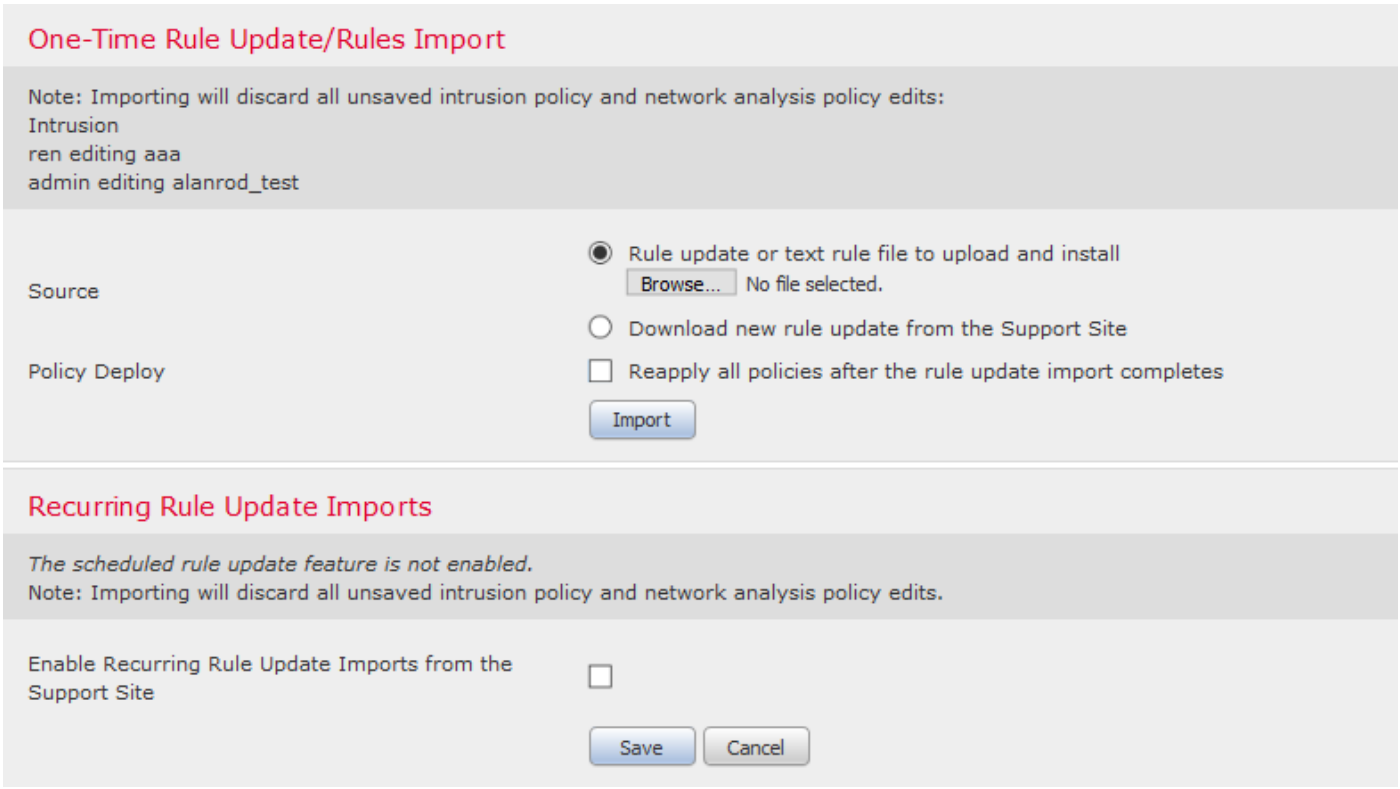
Configurazione

Importa regole locali

Prima di iniziare, è necessario verificare che le regole elencate nel file personalizzato non

contengano caratteri speciali. L'utilità di importazione delle regole richiede che tutte le regole personalizzate vengano importate utilizzando la codifica ASCII o UTF-8. La procedura riportata di seguito spiega come importare le regole di testo standard locali da un computer locale.

Passo 1. Accedere alla scheda **Importa regole** passando a **Oggetti > Regole intrusione > Importa regole. La pagina Aggiornamenti regole** viene visualizzata come illustrato nell'immagine seguente:



Passaggio 2. Selezionare **Aggiornamento regole o file di regole di testo da caricare e installare** e fare clic su **Sfoglia** per selezionare il file di regole personalizzato

> **Nota:** Tutte le regole caricate vengono salvate nella categoria **delle regole locali**

Passaggio 3. Fare clic su **Import**. Il file delle regole viene importato

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

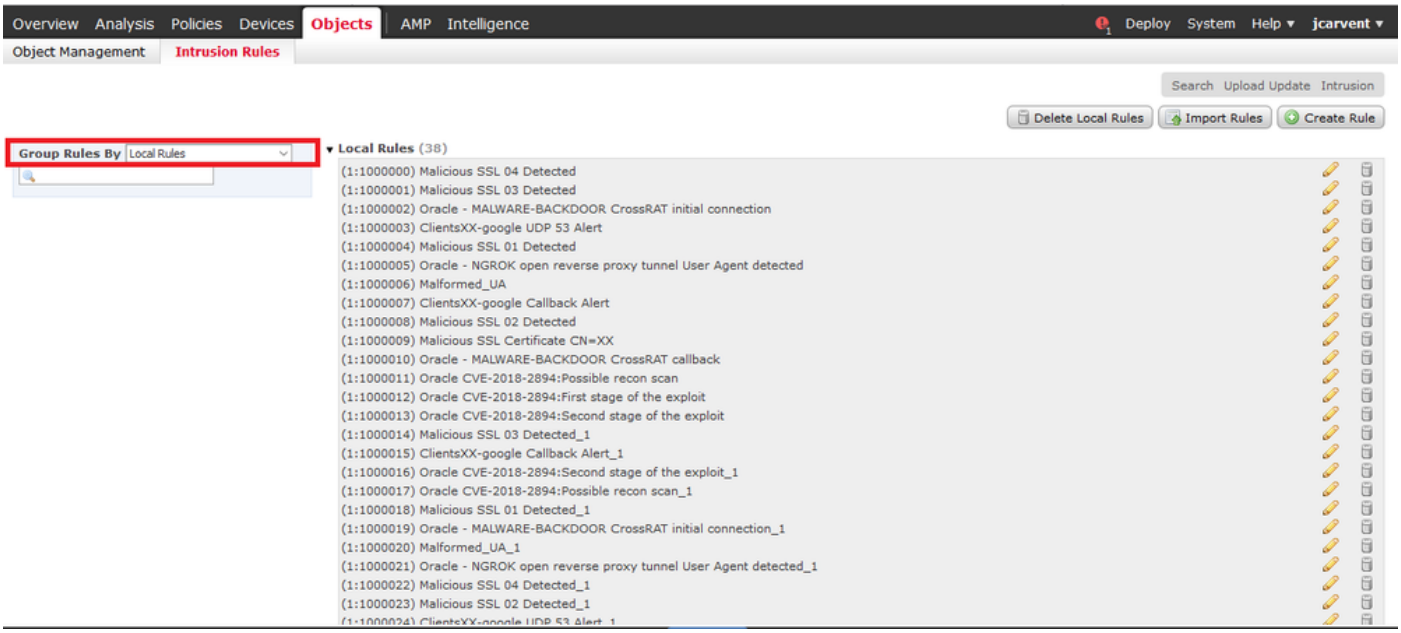
Verifica

Dalla GUI FMC

1. Visualizzare le regole locali importate dall'interfaccia utente di FMC

Passaggio 1. Passare a **Oggetti > Regole intrusione**

Passaggio 2. Selezionare **Regole locali** da **Regole gruppo**



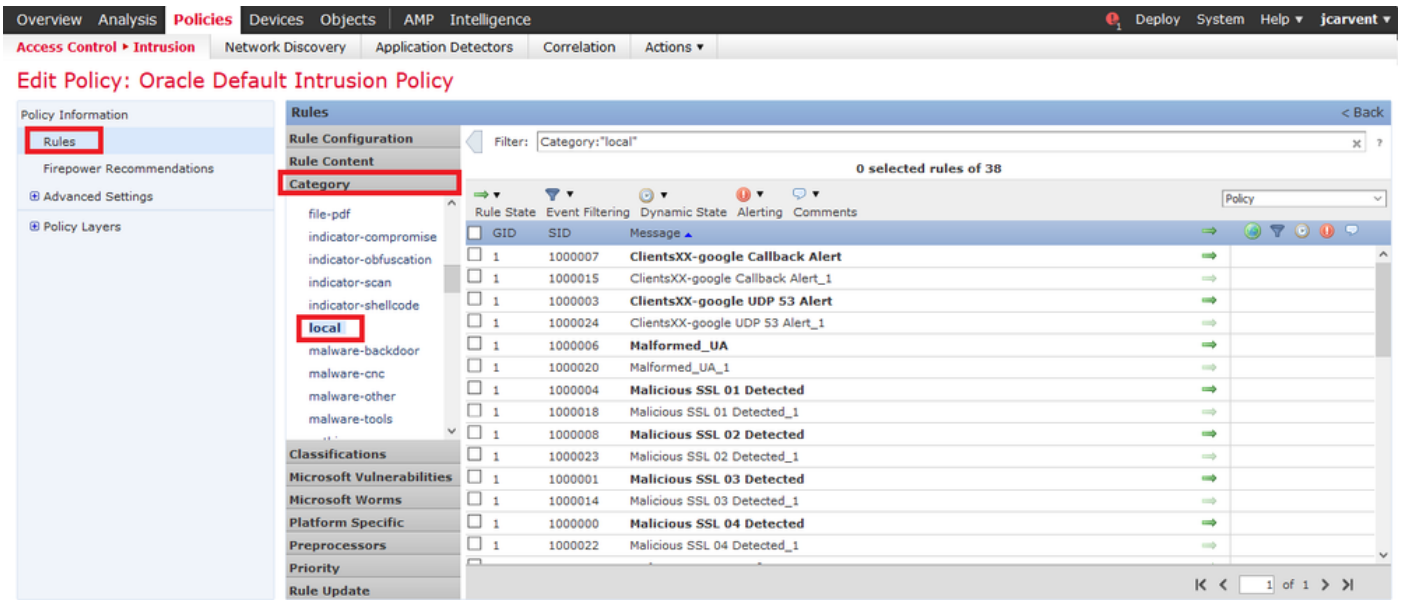
Per impostazione predefinita, il sistema Firepower imposta le regole locali in uno stato disabilitato. Queste regole locali devono impostare manualmente lo stato delle regole locali prima di poterle utilizzare nei criteri per le intrusioni.

2. Abilitare una regola locale da Criteri intrusione

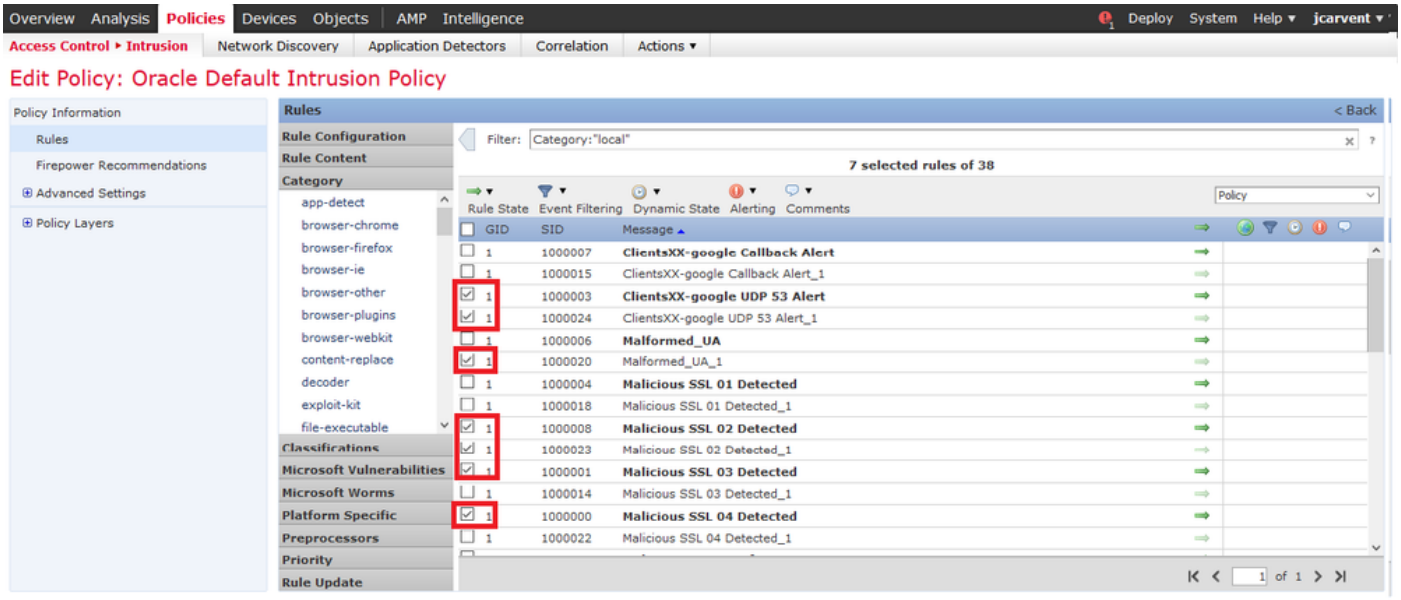
Passaggio 1. Passare alla pagina Editor dei criteri in **Criteri > Intrusione > Criteri di intrusione**

Passaggio 2. Selezionare **Regole** nel pannello sinistro

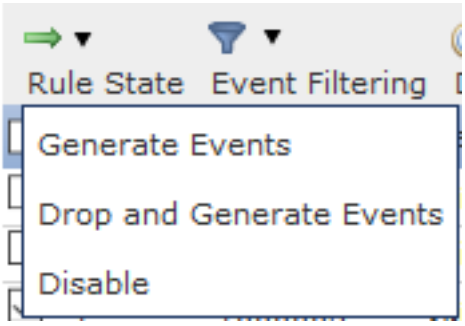
Passaggio 3. Sotto la **categoria**, selezionare **locale.** Tutte le regole locali dovrebbero essere visualizzate se disponibili:



Passaggio 4. Selezionare le regole locali desiderate:



Passaggio 5. Dopo aver selezionato le regole locali desiderate, selezionare uno stato da **Stato regola**



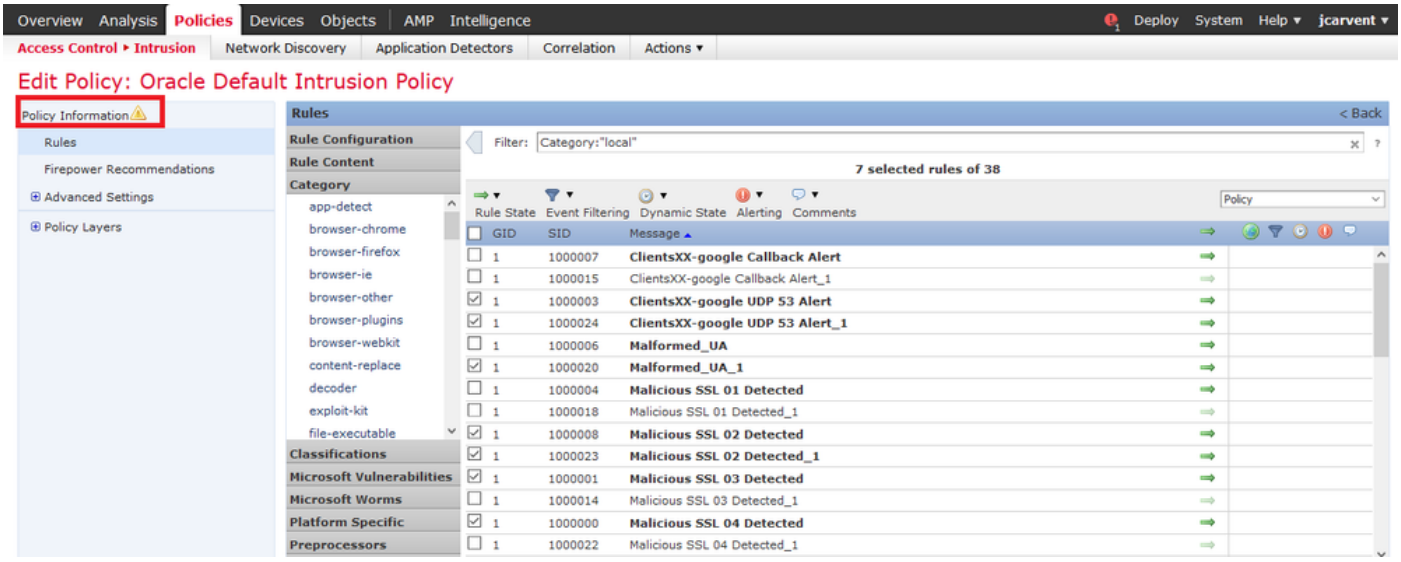
Sono disponibili le seguenti opzioni:

- **Genera eventi:** Attiva la regola e genera un evento

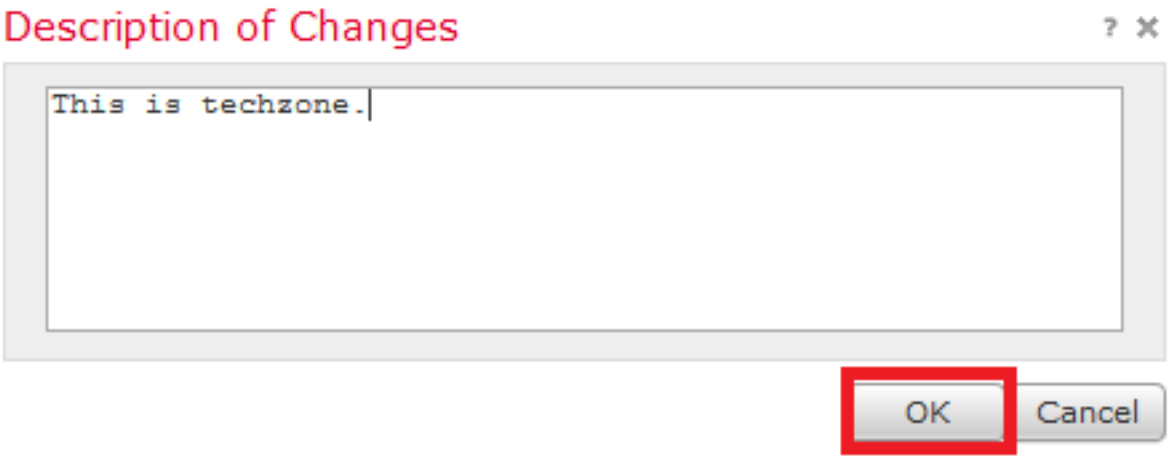
- **Elimina e genera eventi:** Abilitare la regola, eliminare il traffico e generare un evento

- **Disabilita:** Non attivare la regola, non attivare eventi

Passaggio 6. Una volta selezionato lo stato della regola, fare clic su Opzione **Informazioni criterio** nel pannello sinistro



Passaggio 7. Selezionare il pulsante **Commit modifiche** e fornire una breve descrizione delle modifiche. Fare clic su **OK** successivamente. 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.

Passaggio 8. Distribuire le modifiche

Dalla CLI del modulo FTD o SFR

1. Visualizzare le regole locali importate dalla CLI del modulo FTD o SFR

Passaggio 1. Stabilire una sessione SSH o CLI dal modulo SFR o FTD

Passaggio 2. Passare alla modalità Expert

```
> expert
admin@firepower:~$
```

Passaggio 3. Ottenere i privilegi di amministratore

```
admin@firepower:~$ sudo su -
```

Passaggio 4. Digitare la password

```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
```

Passaggio 5. Passare a **/ngfw/var/sf/detection_engine/UUID/intrusion/**

```
root@firepower:/home/admin# cd /ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-
2369c038cbc9/intrusion/
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
```

> **Nota:** Se si utilizza il modulo SFR, non utilizzare /ngfw/var/sf/detection_engine/*/intrusion path. Utilizzo preferenziale **/var/sf/detection_engine/*/intrusion**

Passaggio 6. Introdurre il seguente comando

```
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
```

Fare riferimento all'immagine seguente come esempio di funzionamento:

```
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
sid:1000008
sid:1000023
sid:1000007
sid:1000035
sid:1000004
sid:1000000
...
```

Elenca l'elenco SID del cliente abilitato dal modulo FTD o SFR.

Risoluzione dei problemi

Passaggio 1. Assicurarsi che la sessione SSH sia stabilita sul modulo SFR o FTD, dal FMC detection_engine non è elencato

Passaggio 2. Il comando grep -Eo "sid:*([0-9]{1,8})" */*local.rules funziona solo nella directory di intrusione, il comando non può essere usato da un'altra directory

Passaggio 3. Utilizzare il comando grep -Eo "sid:*([0-9]{1,8})" */*.rules per ottenere un elenco completo dei SID da tutte le categorie

Procedure consigliate per l'importazione delle regole locali per le intrusioni

Durante l'importazione di un file di regole locale, attenersi alle istruzioni riportate di seguito.

- L'utilità di importazione delle regole richiede che tutte le regole personalizzate vengano

importate in un file di testo normale codificato in ASCII o UTF-8
- Il nome del file di testo può includere caratteri alfanumerici, spazi e nessun carattere speciale ad eccezione del carattere di sottolineatura (_), del punto (.) e del trattino (-)
- Il sistema importa le regole locali precedute da un carattere di cancelletto (#), ma sono contrassegnate come eliminate
- Il sistema importa le regole locali precedute da un carattere di cancelletto singolo (#) e non importa le regole locali precedute da caratteri di due libbre (##)
- Le regole non possono contenere caratteri di escape
- Non è necessario specificare un ID generatore (GID) durante l'importazione di una regola locale. In tal caso, specificare solo GID 1 per una regola di testo standard
- Quando si importa una regola per la prima volta, eseguire le operazioni seguenti: *non* specificare ID snort (SID) o numero di revisione. In questo modo si evitano collisioni con SID di altre regole, incluse quelle eliminate. Il sistema assegnerà automaticamente alla regola il successivo SID disponibile della regola personalizzata pari a 1000000 o superiore e un numero di revisione pari a 1
- Se è necessario importare regole con SID, i SID devono essere numeri univoci compresi tra 1.000.000 e 9.999.999
- In una distribuzione multidominio, il sistema assegna i SID alle regole importate da un pool condiviso utilizzato da tutti i domini del Firepower Management Center. Se più amministratori stanno importando contemporaneamente regole locali, i SID all'interno di un singolo dominio potrebbero apparire non sequenziali, perché il sistema ha assegnato i numeri intermedi nella sequenza a un altro dominio
- Quando si importa una versione aggiornata di una regola locale importata in precedenza o quando si ripristina una regola locale eliminata, è ***necessario*** includere il SID assegnato dal sistema e un numero di revisione maggiore del numero di revisione corrente. È possibile determinare il numero di revisione per una regola corrente o eliminata modificando la regola

  Nota: quando eliminate una regola locale, il sistema incrementa automaticamente il numero di revisione. si tratta di un dispositivo che consente di ripristinare le regole locali. Tutte le regole locali eliminate vengono spostate dalla categoria delle regole locali alla categoria delle regole eliminate.

- Importare le regole locali nel centro Firepower Management primario in una coppia ad alta disponibilità per evitare problemi di numerazione SID
- L'importazione non riesce se una regola contiene uno dei seguenti elementi:Un SID è maggiore di 2147483647Elenco di porte di origine o di destinazione più lunghe di 64 caratteri
- La convalida dei criteri ha esito negativo se si abilita una regola locale importata che utilizza la parola chiave ***threshold*** deprecata in combinazione con la funzione di soglia degli eventi di intrusione in un criterio di intrusione
- Tutte le regole locali importate vengono salvate automaticamente nella categoria delle regole locali
- Le regole locali importate vengono sempre impostate sullo stato delle regole disattivato. È necessario impostare manualmente lo stato delle regole locali prima di poterle utilizzare nei criteri per le intrusioni

Informazioni correlate

Di seguito sono riportati alcuni documenti di riferimento relativi a Snort SID:

Aggiorna regole di intrusione

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/System_Software_Updates.html#ID-2259-00000356

Editor delle regole di intrusione

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/the_intrusion_rules_editor.html