Configurazione della policy di intrusione e della configurazione delle firme in Firepower Module (gestione integrata)

Sommario

Introduzione

In questo documento viene descritta la funzionalità IPS (Intrusion Prevention System)/IDS (Intrusion Detection System) del modulo FirePOWER e vari elementi della policy di intrusione che creano una policy di rilevamento nel modulo FirePOWER.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

* Conoscenza del firewall di Adaptive Security Appliance (ASA), Adaptive Security Device Manager (ASDM).

* Conoscenza dell'appliance FirePOWER.

Componenti usati

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

Moduli ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) con software versione 5.4.1 e successive.

Modulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) con software versione 6.0.0 e successive.

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

FirePOWER IDS/IPS è progettato per esaminare il traffico di rete e identificare eventuali modelli dannosi (o firme) che indicano un attacco alla rete o al sistema. Il modulo FirePOWER funziona in modalità IDS se la policy dei servizi dell'ASA è configurata in modo specifico in modalità monitor (promiscua), altrimenti funziona in modalità Inline.

FirePOWER IPS/IDS è un approccio di rilevamento basato su firma. Il modulo FirePOWER in modalità IDS genera un avviso quando la firma corrisponde al traffico dannoso, mentre il modulo FirePOWER in modalità IPS genera un avviso e blocca il traffico dannoso.

> **Nota**: Verificare che il modulo FirePOWER disponga della licenza **Protect** per configurare questa funzionalità. Per verificare la licenza, selezionare **Configurazione > ASA FirePOWER Configuration > Licenza.**

Configurazione

Passaggio 1. Configurare i criteri per le intrusioni

Passaggio 1.1. Creazione di una policy di intrusione

Per configurare la policy sulle intrusioni, accedere a Adaptive Security Device Manager (ASDM) e completare i seguenti passaggi:

Passaggio 1. Passare a **Configurazione > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy**.

Passaggio 2. Fare clic su **Crea criterio**.

Passaggio 3. Inserire il **nome** della policy di intrusione.

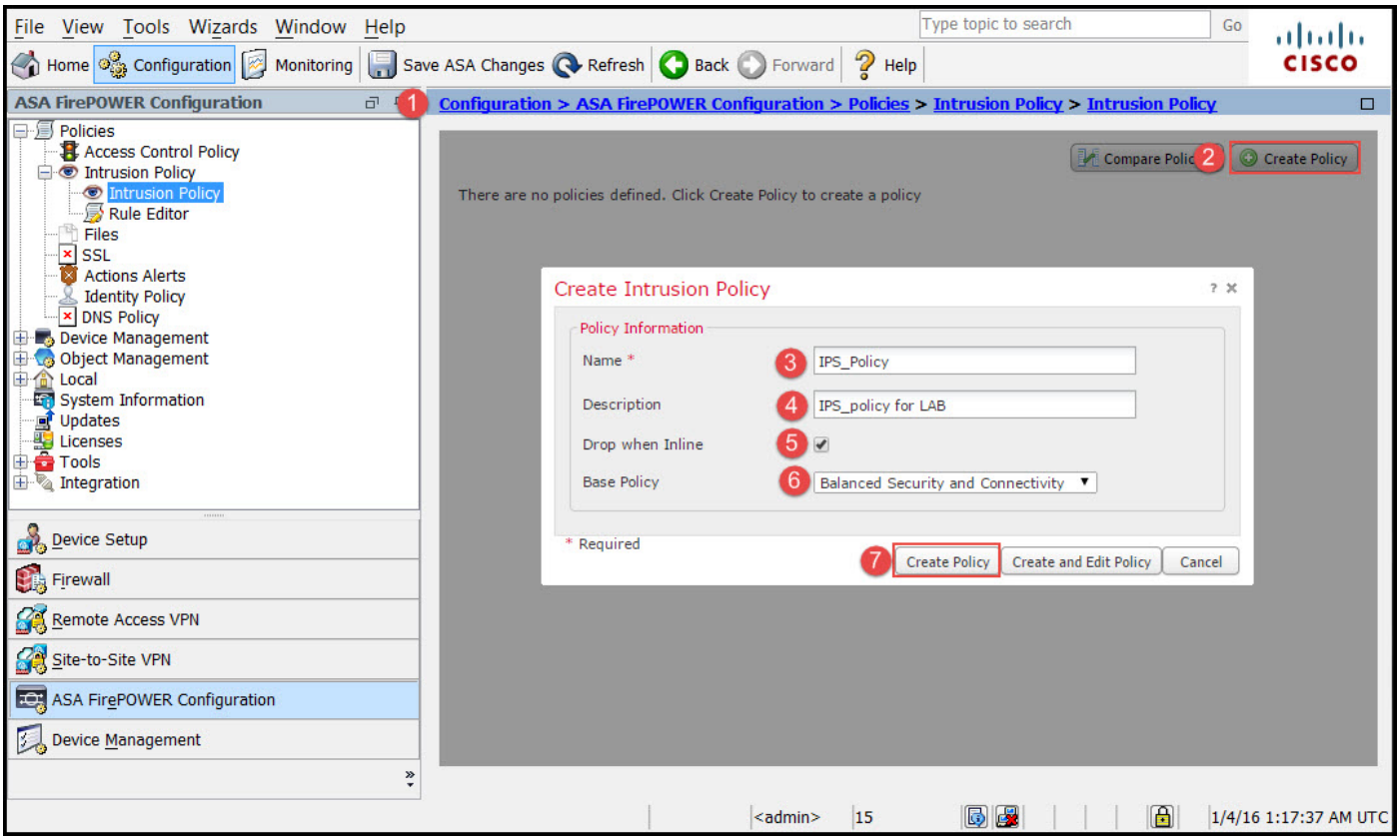
Passaggio 4. Inserire la **descrizione** della politica sulle intrusioni (facoltativo).

Passaggio 5. Specificare l'opzione **Elimina quando in linea**.

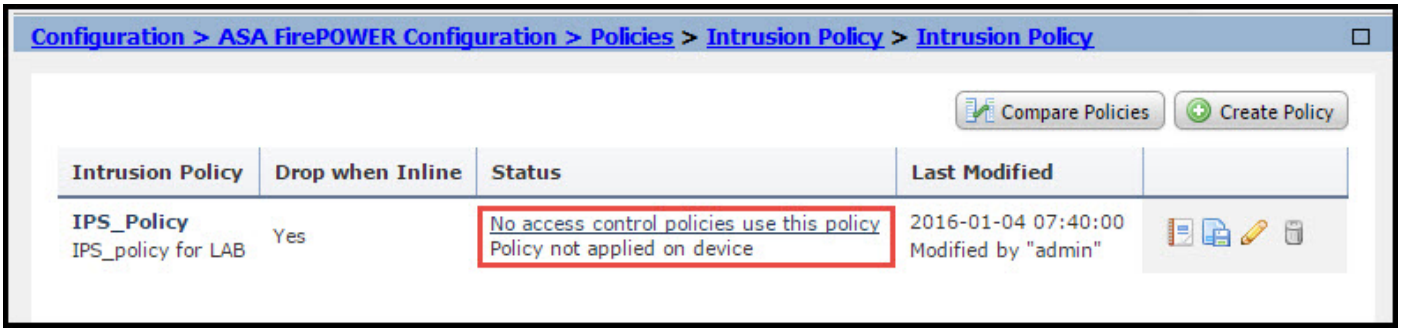
Passaggio 6. Selezionare il **criterio di base** dall'elenco a discesa.

Passaggio 7. Fare clic su **Crea criterio** per completare la creazione dei criteri di intrusione.

> **Suggerimento**: l'opzione Rilascia quando inline è fondamentale in alcuni scenari quando il sensore è configurato in modalità inline ed è richiesto di non rilasciare il traffico anche se corrisponde a una firma che ha un'azione di rilascio.

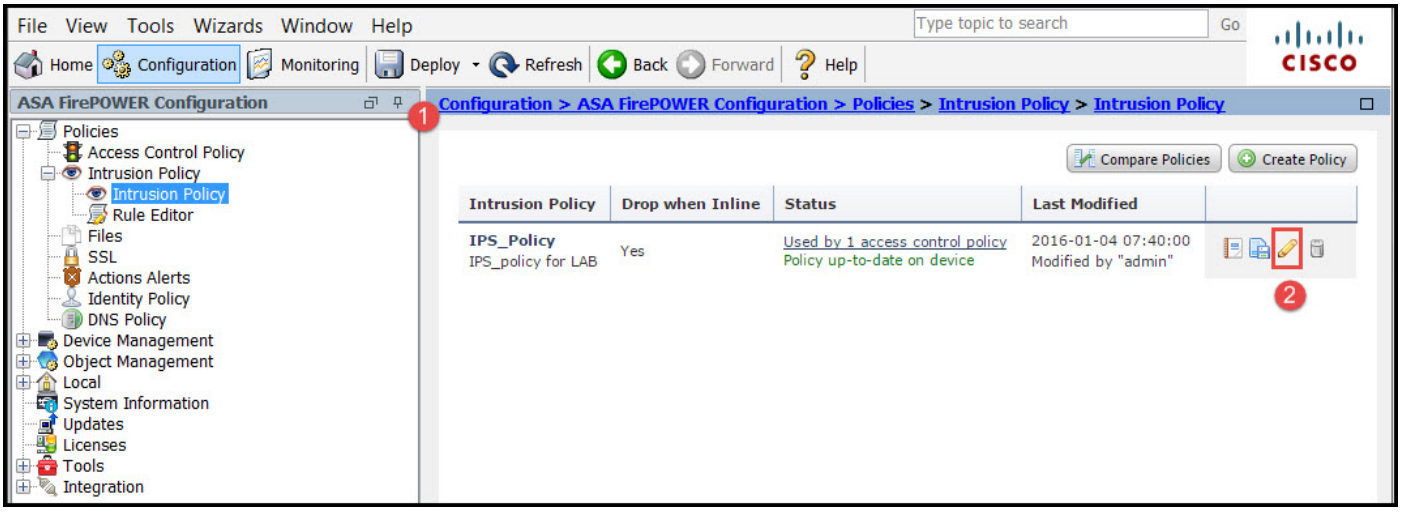


Èpossibile notare che il criterio è configurato, ma non viene applicato ad alcun dispositivo.



Passaggio 1.2. Modifica criteri intrusioni

Per modificare la policy di intrusione, selezionare **Configurazione > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy** (Configurazione ASA FirePOWER > Criteri di intrusione), quindi selezionare l'opzione **Edit** (Modifica).

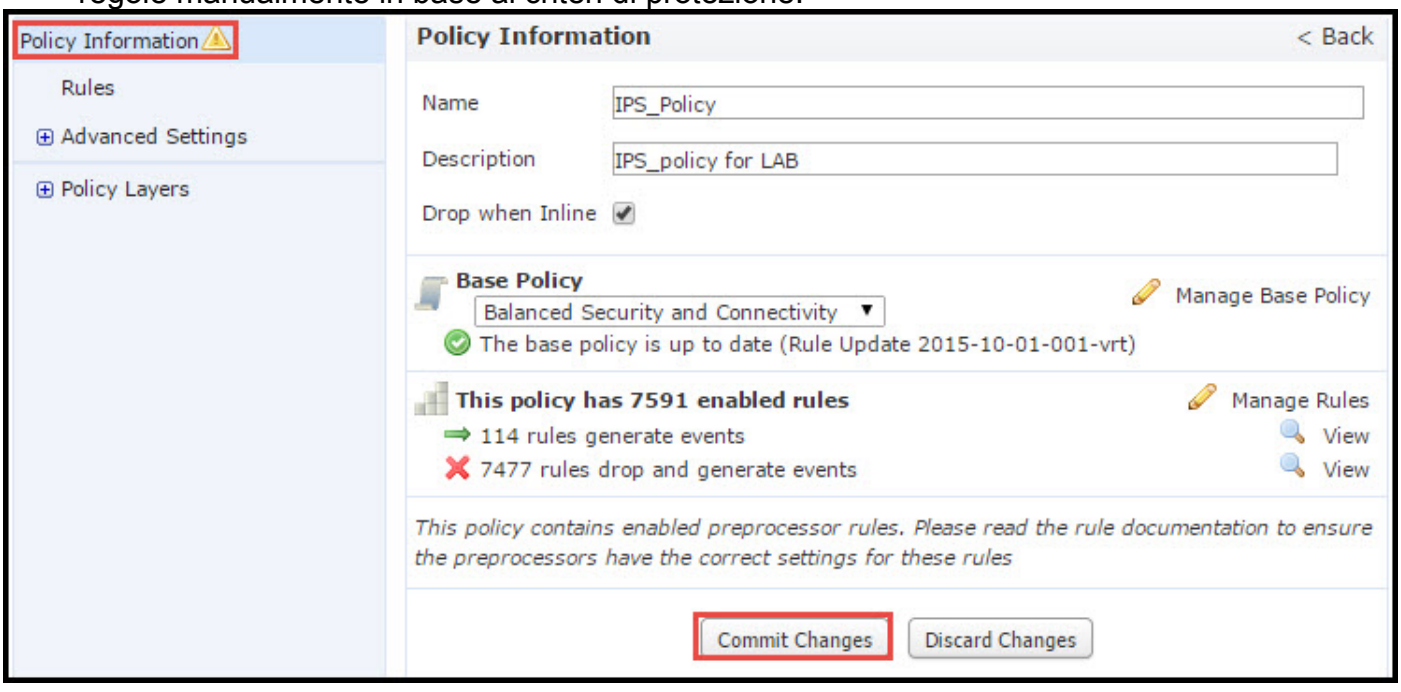


Passaggio 1.3. Modifica criteri di base

La pagina Gestione dei criteri per le intrusioni consente di modificare l'opzione Criteri di base/Elimina in linea/Salva e Elimina.

I criteri di base contengono alcuni criteri forniti dal sistema, ovvero criteri incorporati.

1. Sicurezza e connettività equilibrate: è una politica ottimale in termini di sicurezza e connettività. Questa politica ha attivato circa 7500 regole, alcune delle quali generano solo eventi, mentre altre generano eventi e scaricano il traffico.
2. Protezione rispetto alla connettività: se si preferisce la protezione, è possibile scegliere la protezione rispetto al criterio di connettività, che aumenta il numero di regole abilitate.
3. Connettività anziché sicurezza: se la preferenza è la connettività anziché la sicurezza, è possibile scegliere la connettività anziché i criteri di sicurezza che ridurranno il numero di regole abilitate.
4. Rilevamento massimo: selezionare questo criterio per ottenere il rilevamento massimo.
5. Nessuna regola attiva: questa opzione disattiva tutte le regole. È necessario attivare le regole manualmente in base ai criteri di protezione.



Passaggio 1.4. Filtro della firma con l'opzione della barra Filtro

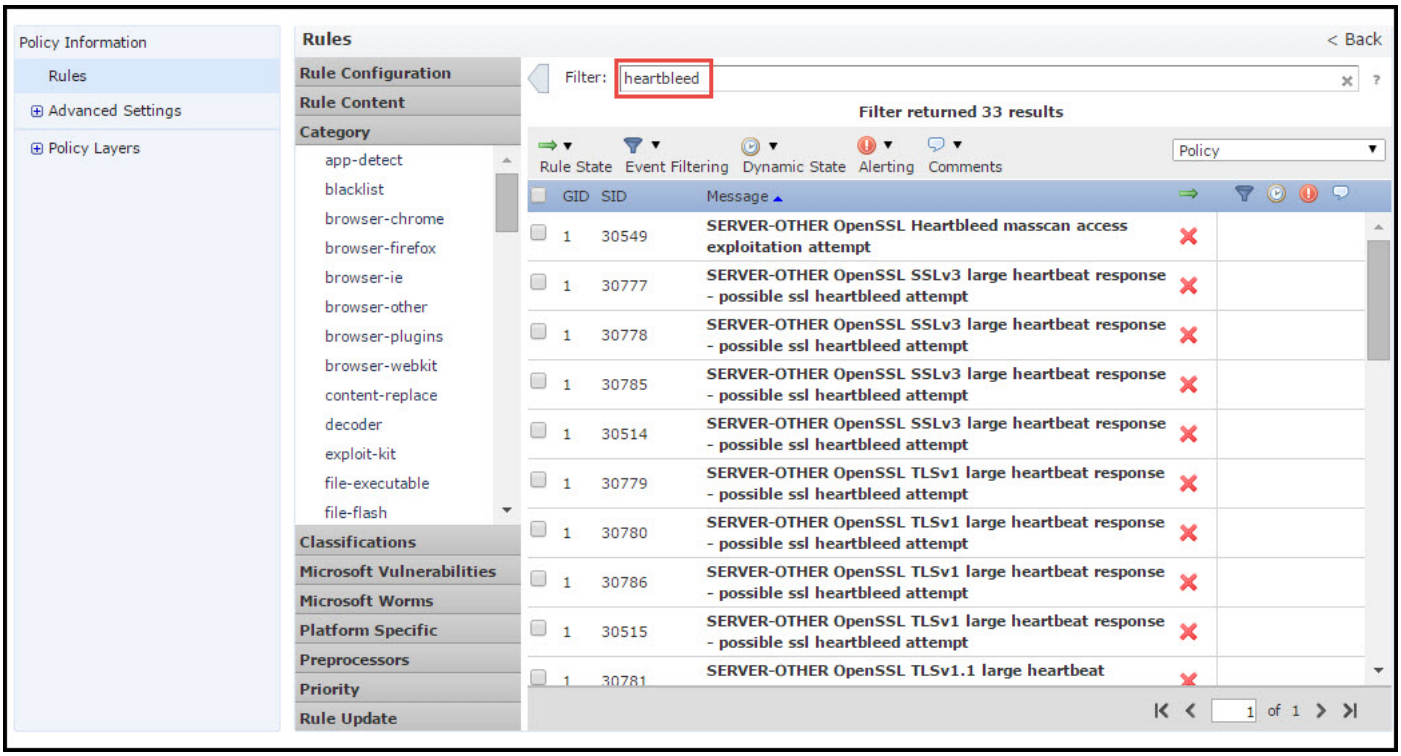
Passare all'opzione **Regole** nel pannello di navigazione e viene visualizzata la pagina Gestione regole. Nel database delle regole sono presenti migliaia di regole. La barra dei filtri fornisce un'opzione valida per il motore di ricerca per eseguire ricerche efficaci nella regola.

Èpossibile inserire qualsiasi parola chiave nella barra Filtro e il sistema acquisisce automaticamente i risultati. Se è necessario trovare la firma per la vulnerabilità heartbleed SSL (Secure Sockets Layer), è possibile cercare la parola chiave heartbleed nella barra del filtro e recupererà la firma per la vulnerabilità heartbleed.

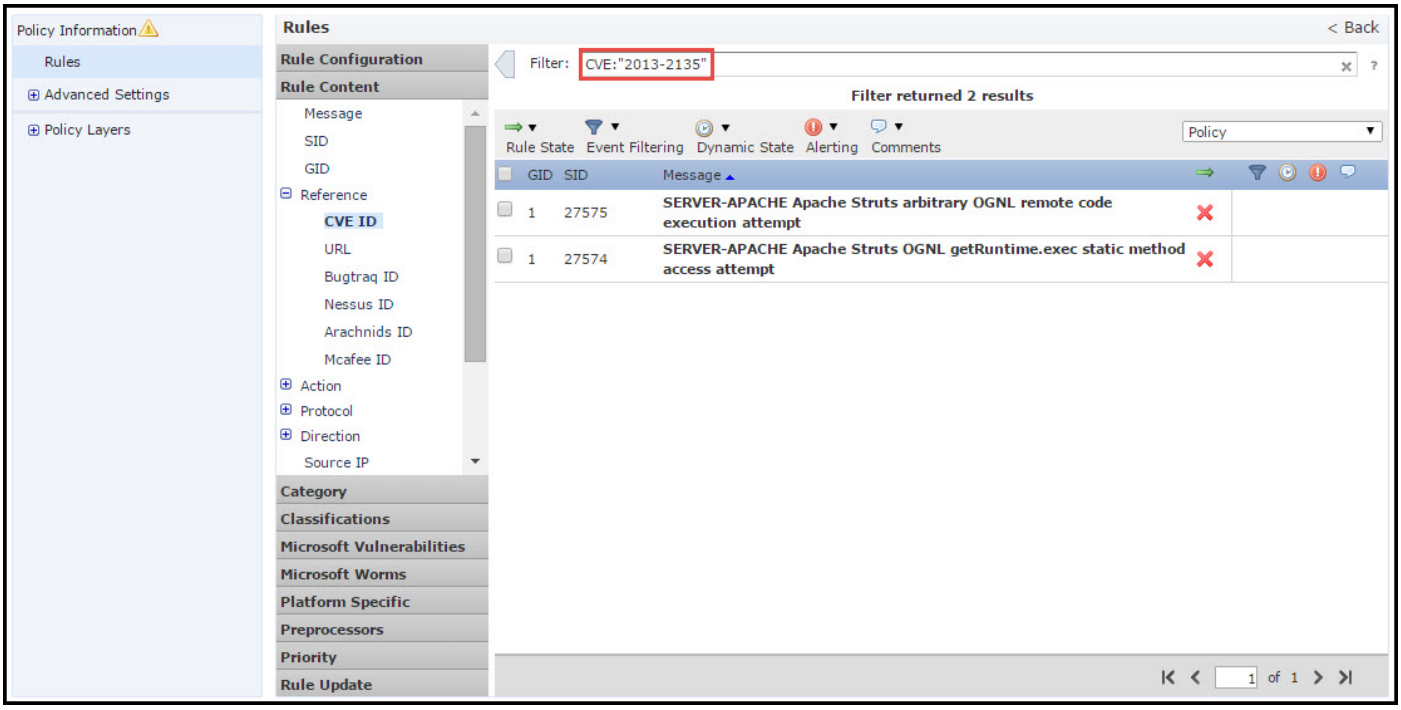
> **Suggerimento**: se nella barra Filtro vengono utilizzate più parole chiave, il sistema le combina utilizzando la logica AND per creare una ricerca composta.

Èinoltre possibile cercare le regole utilizzando Signature ID (SID), Generator ID (GID), Category: dos ecc.

Le regole sono effettivamente suddivise in più modi, ad esempio in base a categoria/classificazioni/vulnerabilità Microsoft/Microsoft Worm/specifiche della piattaforma. Tale associazione di regole consente al cliente di ottenere la firma corretta in modo semplice e aiuta il cliente a ottimizzare efficacemente le firme.



Èinoltre possibile eseguire ricerche con il numero CVE per trovare le regole che li riguardano. È possibile utilizzare la sintassi **CVE: <numero-cve>.**



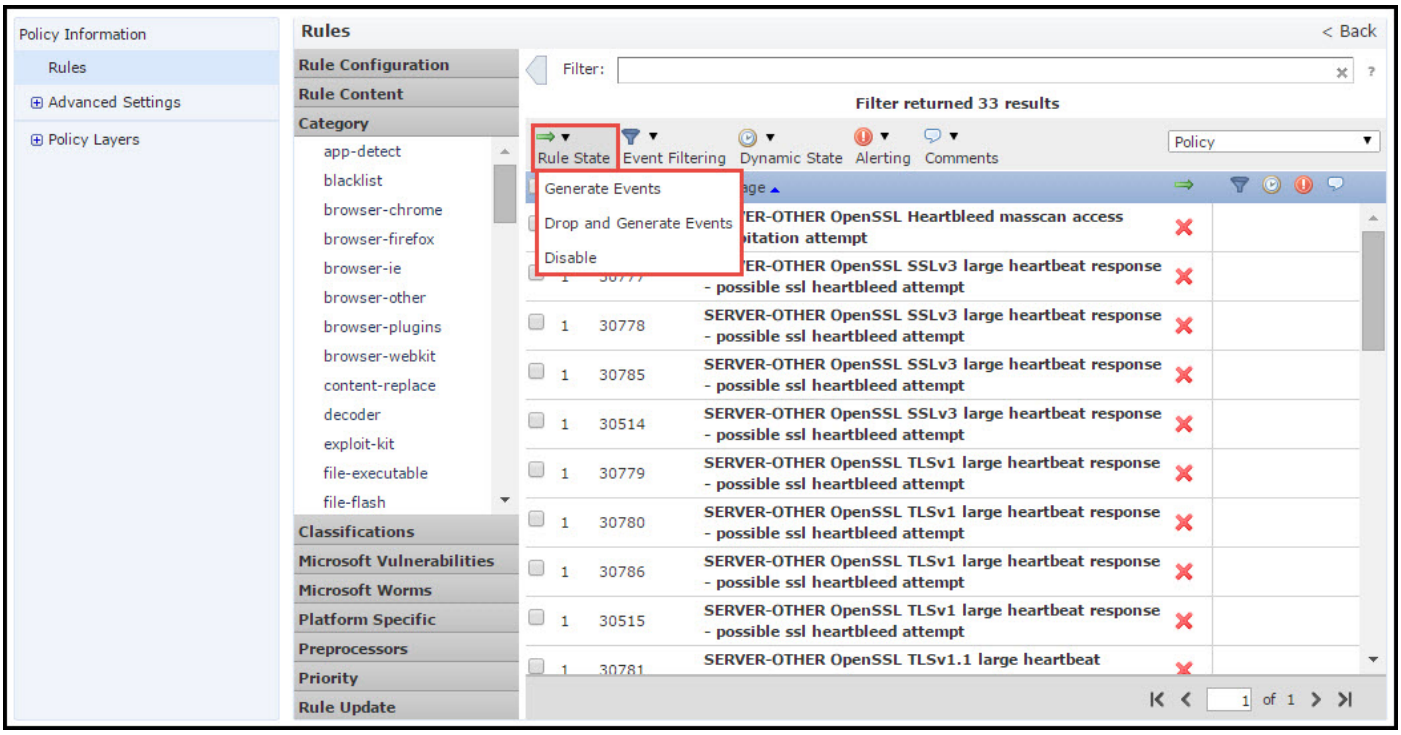
Passaggio 1.5. Configurazione dello stato della regola

Passa a **Regole** nel pannello di navigazione e viene visualizzata la pagina Gestione regole. Selezionare le regole e scegliere l'opzione **Stato regola** per configurare lo stato delle regole. È possibile configurare tre stati per una regola:

1. **Genera eventi:** Questa opzione genera eventi quando la regola corrisponde al traffico.

2. **Elimina e genera eventi:** questa opzione genera eventi e rilascia traffico quando la regola corrisponde al traffico.

3. **Disabilitazione:** Questa opzione disattiva la regola.



Passaggio 1.6. Configurazione del filtro eventi

L'importanza di un evento di intrusione può essere basata sulla frequenza dell'evento oppure sull'indirizzo IP di origine o di destinazione. In alcuni casi è possibile che un evento non sia rilevante fino a quando non si è verificato un determinato numero di volte. È possibile, ad esempio, che il problema non si verifichi se un utente tenta di accedere a un server fino a quando il tentativo non riesce per un determinato numero di volte. In altri casi, potrebbe essere necessario visualizzare solo alcune occorrenze della regola per verificare se il problema è molto diffuso.

A tale scopo, è possibile procedere in due modi:

1. Soglia evento.

2. Eliminazione degli eventi.

Soglia evento

Èpossibile impostare soglie che determinano la frequenza di visualizzazione di un evento, in base al numero di occorrenze. È possibile configurare la soglia per evento e per criterio.

Passaggi per la configurazione della soglia eventi:

Passaggio 1. Selezionare le **regole** per le quali si desidera configurare la soglia evento.

Passaggio 2. Fare clic su **Filtro eventi**.

Passaggio 3. Fare clic su **Soglia**.

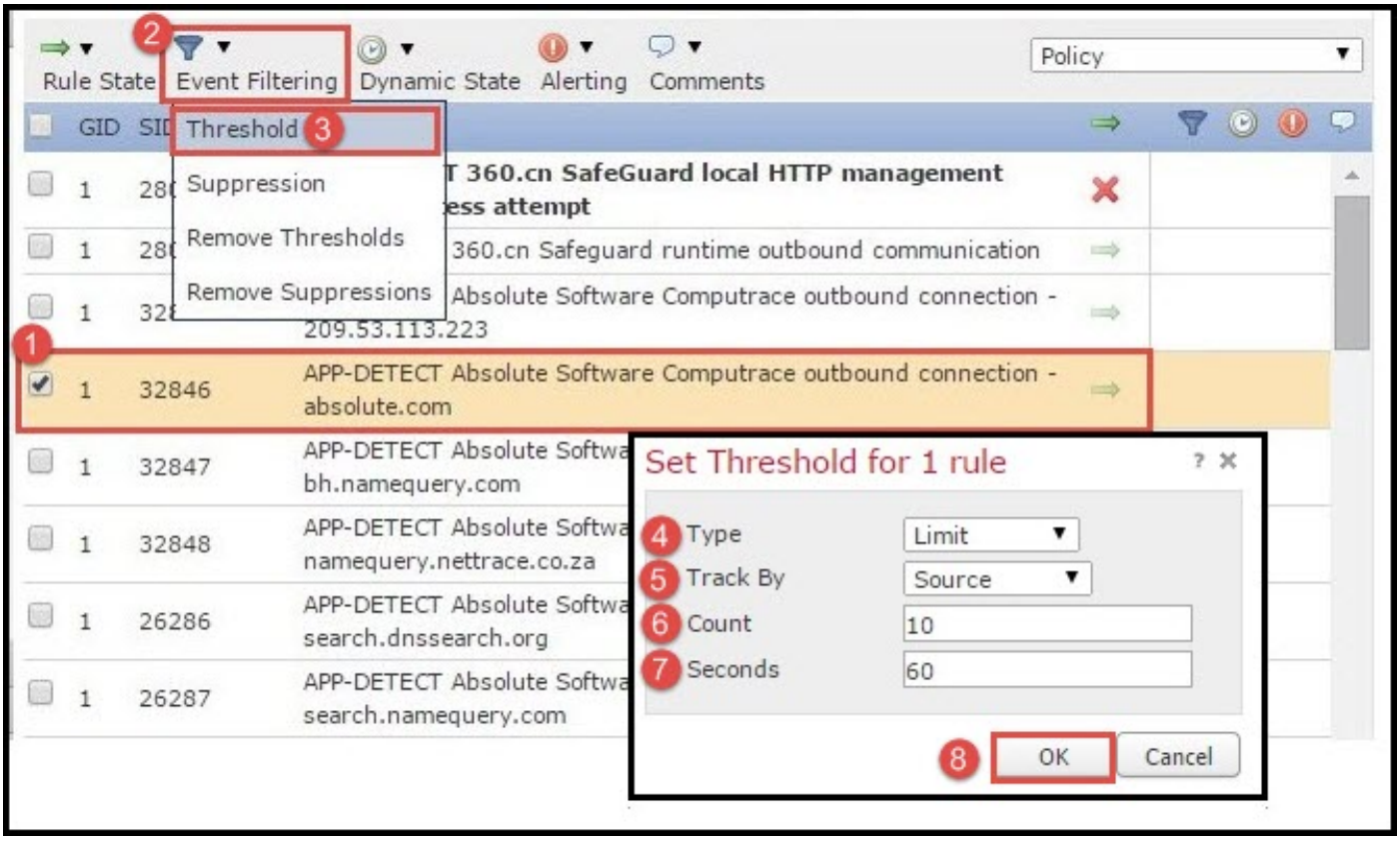
Passaggio 4. Selezionare il **Tipo** dall'elenco a discesa. (Limite o Soglia o Entrambi).

Passaggio 5. Selezionare la modalità di registrazione dalla casella di riepilogo **Traccia per**. (Origine o Destinazione).

Passaggio 6. Inserire il **conteggio** degli eventi per raggiungere la soglia.

Passaggio 7. Inserire i **secondi** che devono trascorrere prima della reimpostazione dell'inventario.

Passaggio 8. Fare clic su **OK** per completare l'operazione.



Dopo l'aggiunta di un filtro di eventi a una regola, dovrebbe essere possibile visualizzare un'icona di filtro accanto all'indicazione della regola, che indica che per la regola è abilitato il filtro di eventi.

Eliminazione eventi

Le notifiche degli eventi specificati possono essere eliminate in base all'indirizzo IP di origine/destinazione o in base a una regola.

Nota: Quando si aggiunge l'eliminazione di eventi per una regola. L'ispezione della firma funziona normalmente ma il sistema non genera gli eventi se il traffico corrisponde alla firma. Se si specifica un'origine o una destinazione specifica, gli eventi non vengono visualizzati solo per l'origine o la destinazione specifica per questa regola. Se si sceglie di sopprimere la regola completa, il sistema non genera alcun evento per questa regola.

Passaggi per la configurazione della soglia eventi:

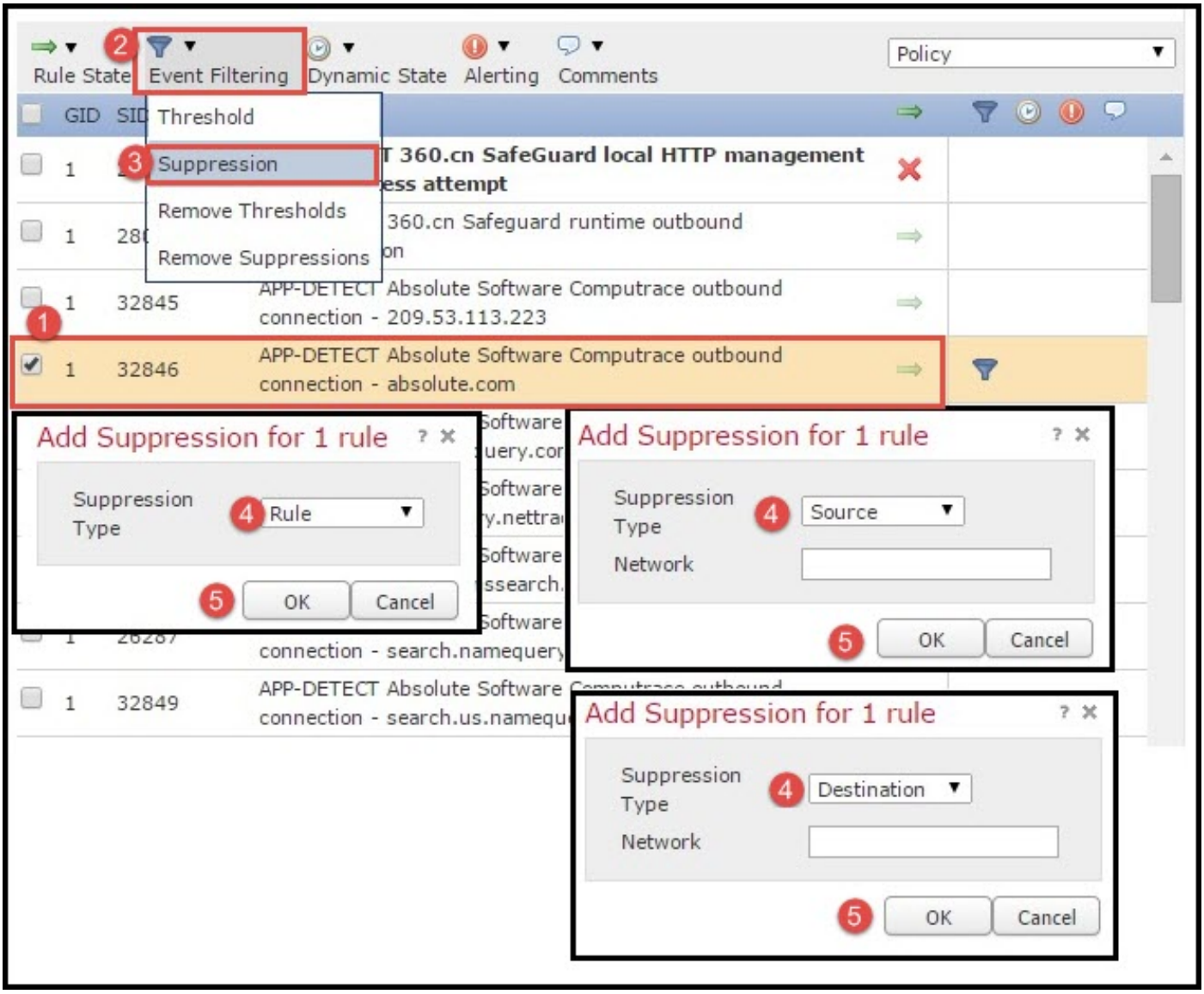
Passaggio 1. Selezionare le **regole** per le quali si desidera configurare la soglia evento.

Passaggio 2. Fare clic su **Filtro eventi**.

Passaggio 3. Fare clic su **Soppressione.**

Passaggio 4. Selezionare **Tipo di soppressione** dall'elenco a discesa**.** (Regola, Origine o Destinazione).

Passaggio 5. Fare clic su **OK** per completare l'operazione.



Dopo aver aggiunto il filtro eventi a questa regola, dovrebbe essere possibile visualizzare un'icona di filtro con il conteggio due accanto all'indicazione della regola, che indica che sono disponibili due filtri eventi abilitati per questa regola.

Passaggio 1.7. Configurazione dello stato dinamico

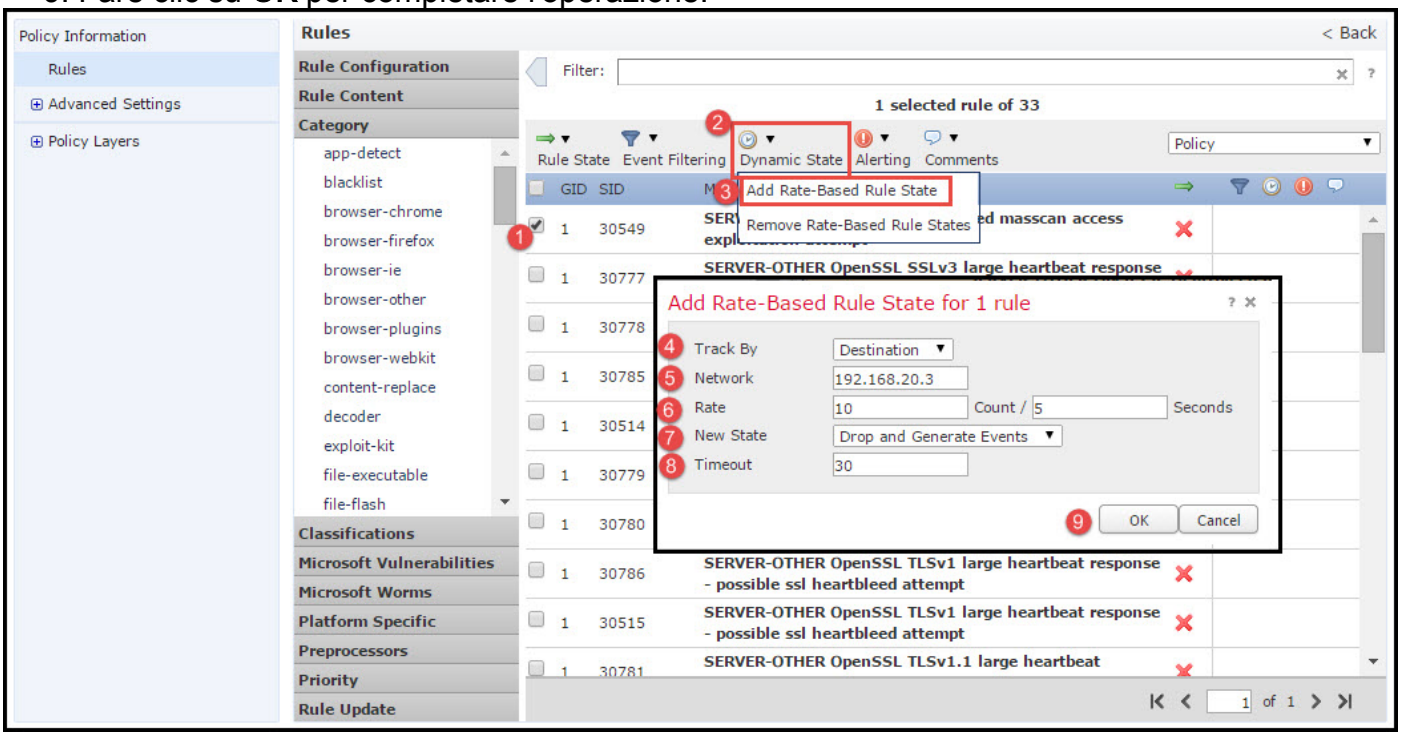
Si tratta di una funzionalità che consente di modificare lo stato di una regola se la condizione specificata corrisponde.

Si supponga di avere uno scenario di attacco di forza bruta per violare la password. Se una firma rileva un tentativo di errore della password e l'azione della regola consiste nel generare un evento. Il sistema continua a generare l'avviso per il tentativo di mancato superamento della password. In questo caso, potete utilizzare lo **stato Dinamico** in cui un'azione di **Genera eventi** (Generate Events) può essere modificata in **Elimina (Drop) e Genera eventi (Generate Events)** per bloccare l'attacco di forza bruta.

Passa a **Regole** nel pannello di navigazione e viene visualizzata la pagina Gestione regole. Selezionare la regola per la quale si desidera abilitare lo stato Dinamico e scegliere le opzioni **Stato dinamico > Aggiungi uno stato regola base tasso.**

Per configurare lo stato della regola basata sulla velocità:

1. Selezionare le **regole** per le quali si desidera configurare la soglia evento.
2. Fare clic su **Stato dinamico**.
3. Fare clic su **Aggiungi stato regola basata su tasso**.
4. Selezionare come si desidera tenere traccia dello stato della regola dalla casella di riepilogo **Rileva per**. (**regola, origine o destinazione**).
5. Accedere alla **rete**. È possibile specificare un singolo indirizzo IP, un blocco di indirizzi, una variabile o un elenco separato da virgole costituito da una combinazione di questi elementi.
6. Immettere il **conteggio** degli eventi e il timestamp in secondi.
7. Selezionare il **Nuovo stato** che si desidera definire per la regola.
8. Immettere il **timeout** dopo il quale lo stato della regola viene ripristinato.
9. Fare clic su **OK** per completare l'operazione.



Passaggio 2. Configurare i set di variabili e criteri di analisi della rete (facoltativo)

Configura criteri di analisi della rete

I criteri di accesso alla rete sono noti anche come preprocessori. Il preprocessore riassembla il pacchetto e normalizza il traffico. Aiuta a identificare le anomalie del protocollo del livello di rete e del livello di trasporto nell'identificazione di opzioni di intestazione inappropriate.

Protezione accesso alla rete esegue la deframmentazione dei datagrammi IP, fornisce l'ispezione con conservazione dello stato TCP e il riassemblaggio dei flussi e la convalida dei checksum. Il preprocessore normalizza il traffico, convalida e verifica lo standard del protocollo.

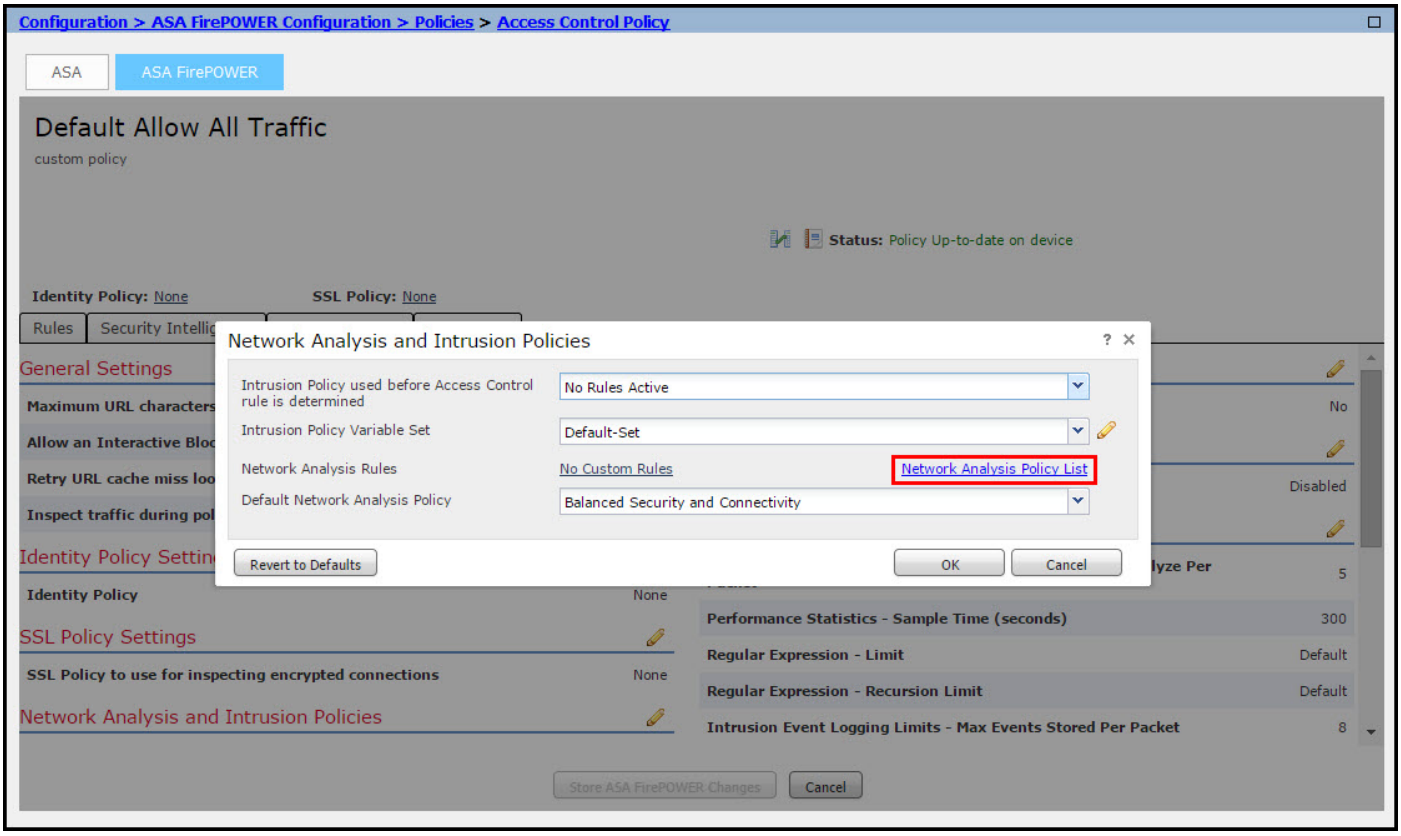
Ogni preprocessore dispone di un proprio numero GID. Indica il preprocessore attivato dal pacchetto.

Per configurare i criteri di analisi della rete, selezionare **Configurazione > ASA FirePOWER Configuration > Policy > Access Control Policy > Advanced > Network Analysis and Intrusion Policy**

Il criterio di analisi della rete predefinito è Protezione e connettività bilanciate, il criterio consigliato

ottimale. Esistono altri tre criteri di Protezione accesso alla rete forniti dal sistema che è possibile selezionare dall'elenco a discesa.

Selezionare l'opzione **Network Analysis Policy** List per creare un criterio di Protezione accesso alla rete personalizzato.



Configura set di variabili

I set di variabili vengono utilizzati nelle regole di intrusione per identificare le porte e gli indirizzi di origine e di destinazione. Le regole sono più efficaci quando le variabili riflettono l'ambiente di rete in modo più accurato. La variabile svolge un ruolo importante nel tuning delle prestazioni.

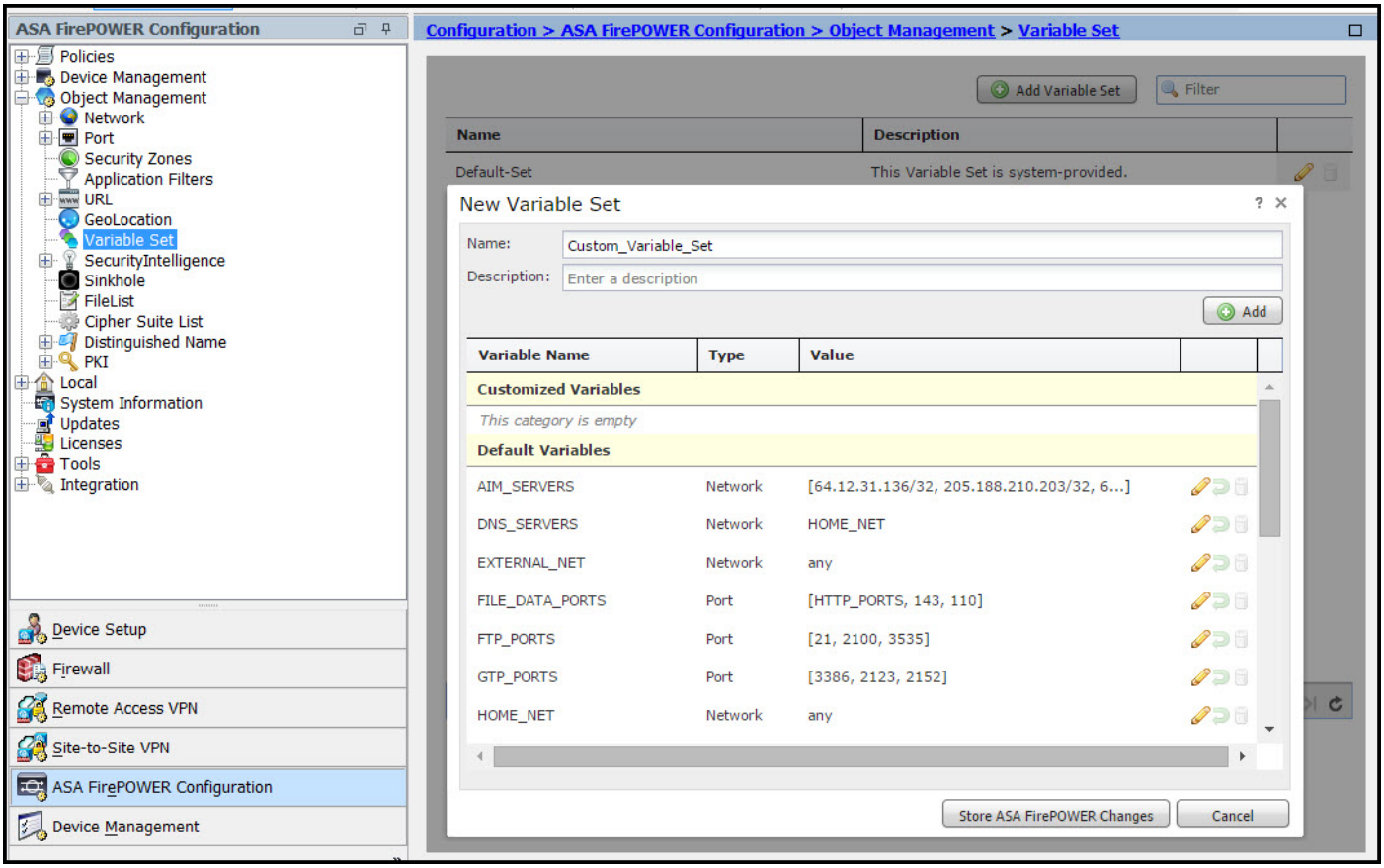
I set di variabili sono già stati configurati con l'opzione predefinita (Rete/Porta). Aggiungere nuovi set di variabili se si desidera modificare la configurazione predefinita.

Per configurare i set di variabili, selezionare **Configurazione > ASA Firepower Configuration > Object Management > Set di variabili**. Selezionare l'opzione **Add Variable Set** (Aggiungi set di variabili) per aggiungere nuovi set di variabili. Immettere il **nome** degli insiemi di variabili e specificare la **descrizione.**

Se un'applicazione personalizzata funziona su una porta specifica, definire il numero di porta nel campo Numero porta. Configurare il parametro network.

$Home_NET specifica la rete interna.

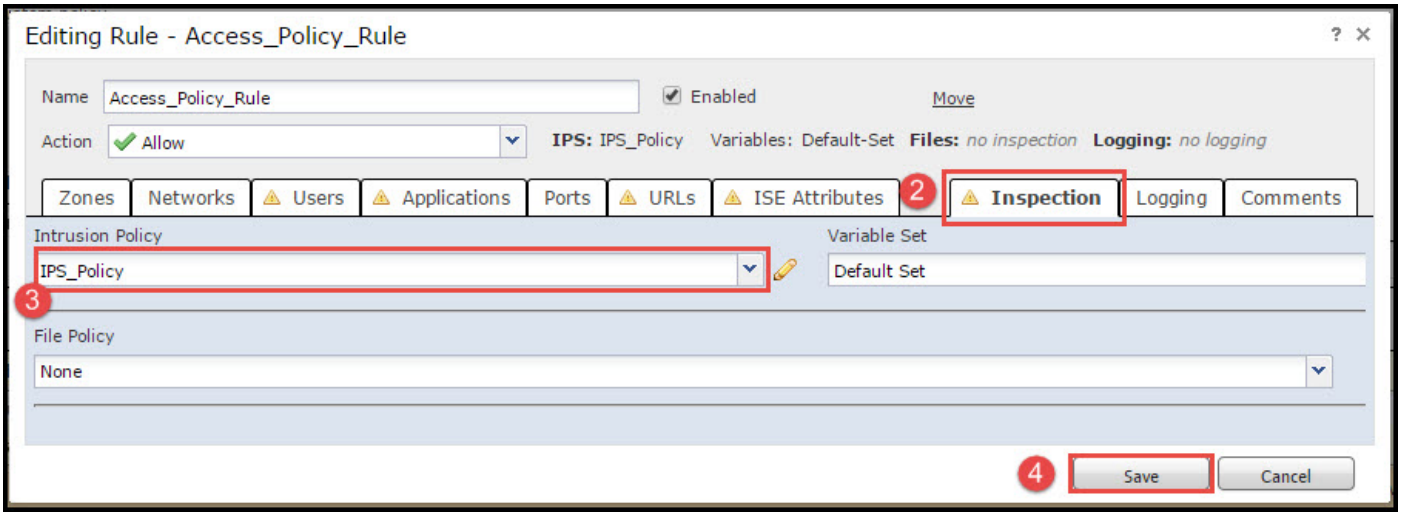
$External_NET specifica la rete esterna.



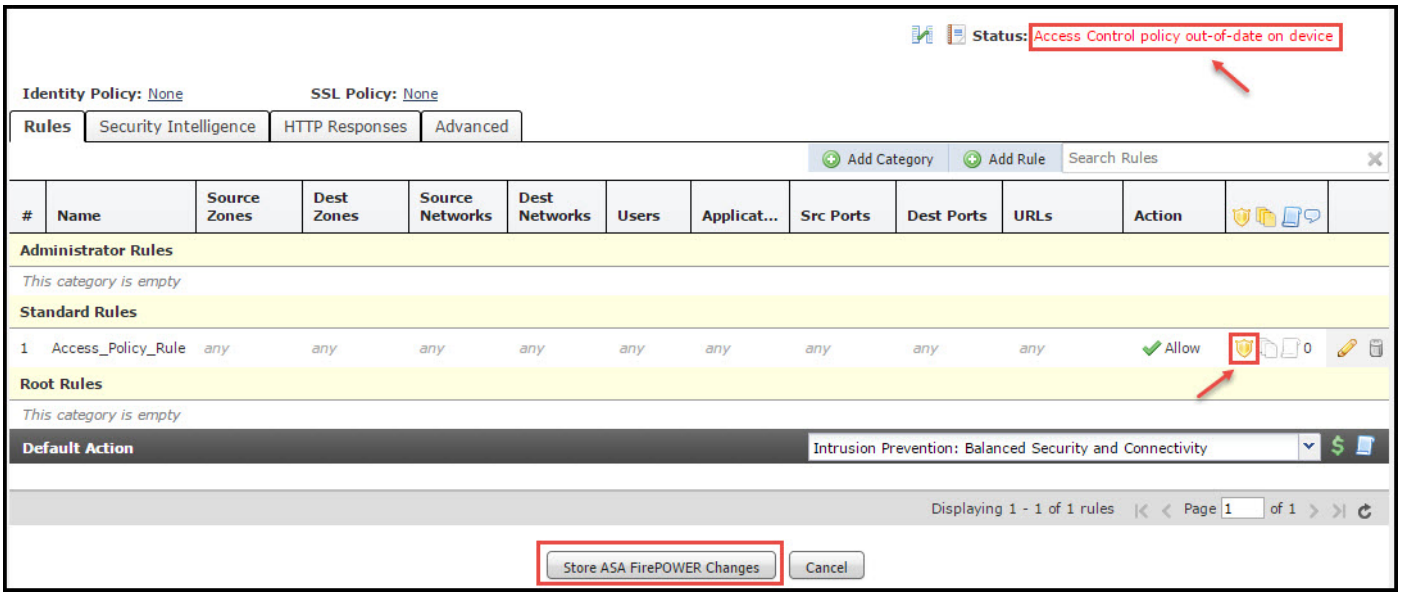
Passaggio 3: Configurare il controllo di accesso per includere i set di criteri/variabili di Protezione accesso alla rete per le intrusioni

Selezionare **Configuration > ASA Firepower Configuration > Policies > Access Control Policy (Configurazione di ASA Firepower > Criteri > Policy di controllo dell'accesso).** Eseguire i seguenti passaggi:

1. Modificare la regola dei criteri di accesso a cui si desidera assegnare i criteri per le intrusioni.
2. Scegliere la scheda **Ispezione.**
3. Selezionare il **criterio** di **intrusione** dall'elenco a discesa e scegliere **Set di variabili** dall'elenco a discesa
4. Fare clic su **Salva**.



Poiché a questa regola dei criteri di accesso è stato aggiunto un criterio di intrusione. È possibile vedere l'icona a forma di scudo in Colore dorato che indica che la policy sulle intrusioni è attivata.

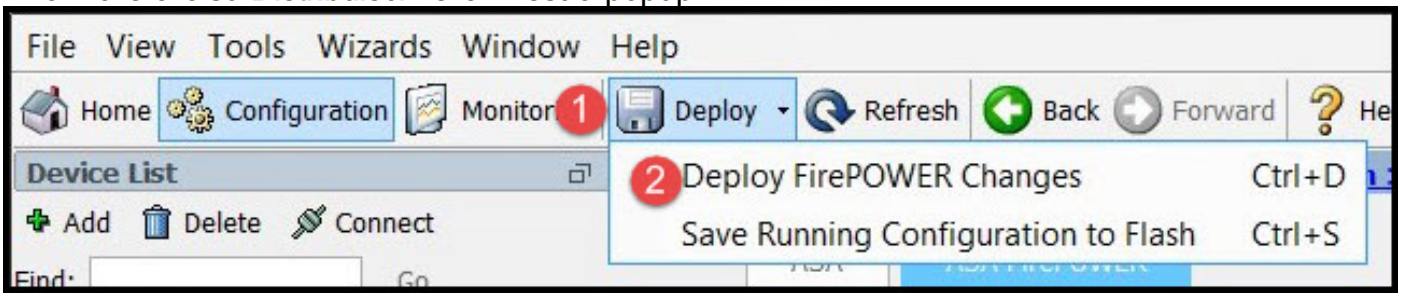


Fare clic su **Store ASA FirePOWER changes** per salvare le modifiche.

Passaggio 4. Distribuire i criteri di controllo di accesso

A questo punto è necessario distribuire i criteri di controllo di accesso. Prima di applicare il criterio, nel dispositivo verrà visualizzata un'indicazione relativa ai criteri di controllo di accesso non aggiornata. Per distribuire le modifiche al sensore:

1. Fare clic su **Distribuisci**.
2. Fare clic su **Distribuisci modifiche FirePOWER**.
3. Fare clic su **Distribuisci** nella finestra popup.

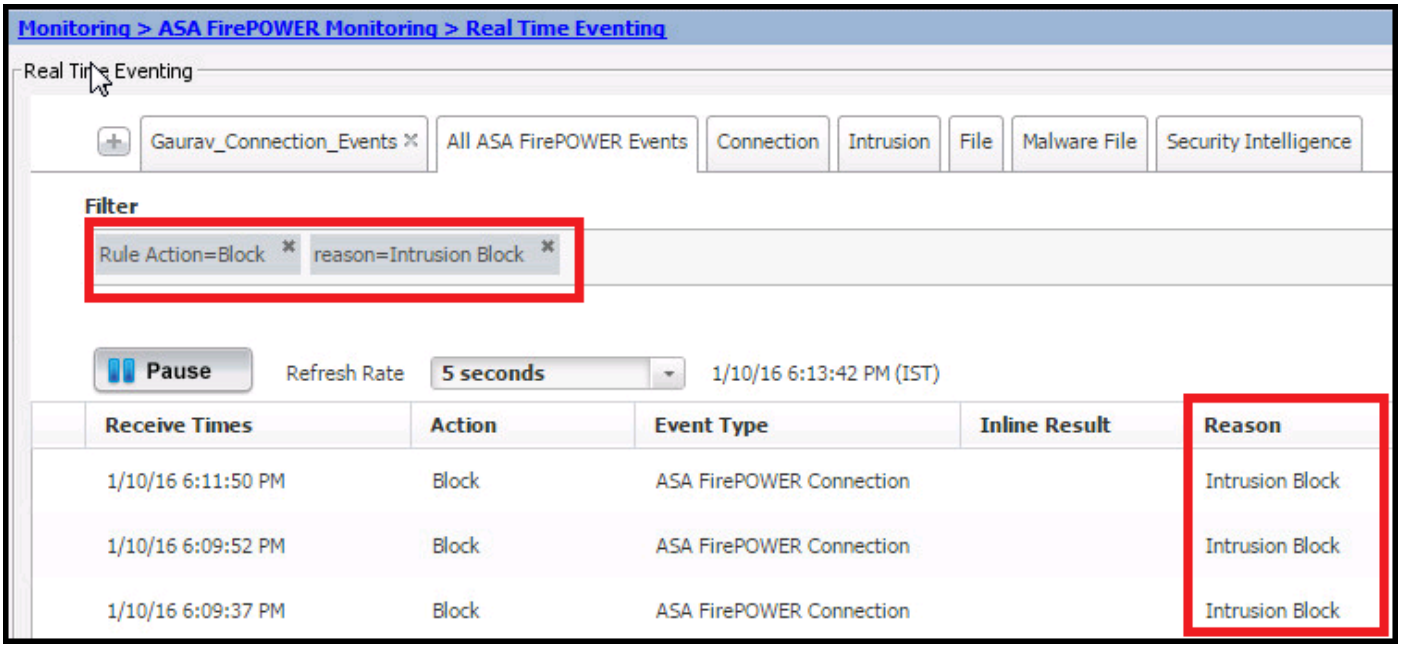


Nota: Nella versione 5.4.x, per applicare la policy di accesso al sensore, è necessario fare clic su Apply ASA FirePOWER Changes (Applica modifiche FirePOWER ASA)

Nota: Passare a **Monitoraggio > Monitoraggio ASA Firepower > Stato task. Per** applicare la modifica alla configurazione, verificare che il task debba essere completato.

Passaggio 5. Monitoraggio degli eventi di intrusione

Per visualizzare gli eventi Intrusion generati dal modulo FirePOWER, passare a **Monitoraggio > ASA FirePOWER Monitoring > Eventi in tempo reale.**



Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Passaggio 1. Verificare che lo stato delle regole sia configurato correttamente.

Passaggio 2. Verificare che nelle regole di accesso sia stato incluso il criterio IPS corretto.

Passaggio 3. Verificare che i set di variabili siano configurati correttamente. Se i set di variabili non sono configurati correttamente, le firme non corrisponderanno al traffico.

Passaggio 4. Verificare che la distribuzione dei criteri di controllo di accesso venga completata correttamente.

Passaggio 5. Monitorare gli eventi di connessione e gli eventi di intrusione per verificare se il flusso di traffico sta violando la regola corretta.

Informazioni correlate

- **Guida introduttiva al modulo Cisco ASA FirePOWER**
- **Documentazione e supporto tecnico – Cisco Systems**