Configurazione di una regola di superamento in un sistema Cisco Firepower

Sommario

Introduzione

In questo documento viene descritta una regola di accesso, viene spiegato come crearla e come attivarla in un criterio di intrusione.

Èpossibile creare regole di superamento per impedire che i pacchetti che soddisfano i criteri definiti nella regola di superamento attivino la regola di avviso in situazioni specifiche anziché disattivarla. Per impostazione predefinita, le regole di superamento sostituiscono le regole di avviso. Un sistema Firepower confronta i pacchetti con le condizioni specificate in ciascuna regola e, 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.

Ad esempio, è possibile che si desideri mantenere attiva una regola che cerca i tentativi di accesso a un server FTP come utente "anonimo". Se tuttavia la rete dispone di uno o più server FTP anonimi legittimi, è possibile scrivere e attivare una regola di accesso che specifichi che, per tali server specifici, gli utenti anonimi non attivano la regola originale.

> **Attenzione:** Quando una regola originale su cui si basa la regola di superamento riceve una revisione, la regola di superamento non viene aggiornata automaticamente. Pertanto, potrebbe essere difficile mantenere le regole di accettazione.

> **Nota:** Se attivate la funzione di soppressione per una regola, vengono eliminate le notifiche degli eventi per tale regola. Tuttavia, la regola viene ancora valutata. Ad esempio, se si sopprime una regola di rilascio, i pacchetti che corrispondono alla regola vengono eliminati automaticamente.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

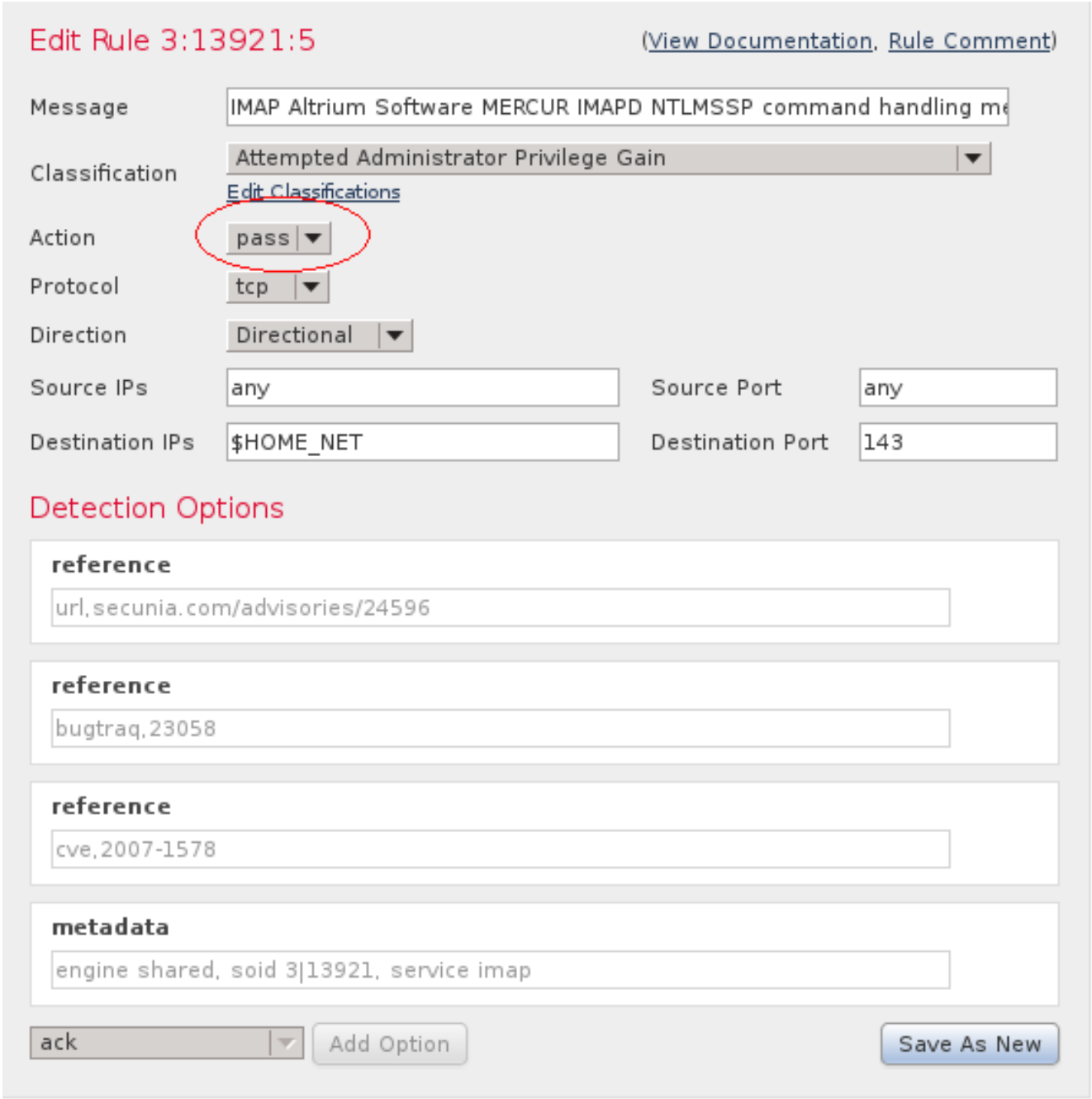
Il documento può essere consultato per tutte le versioni software o hardware.

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.

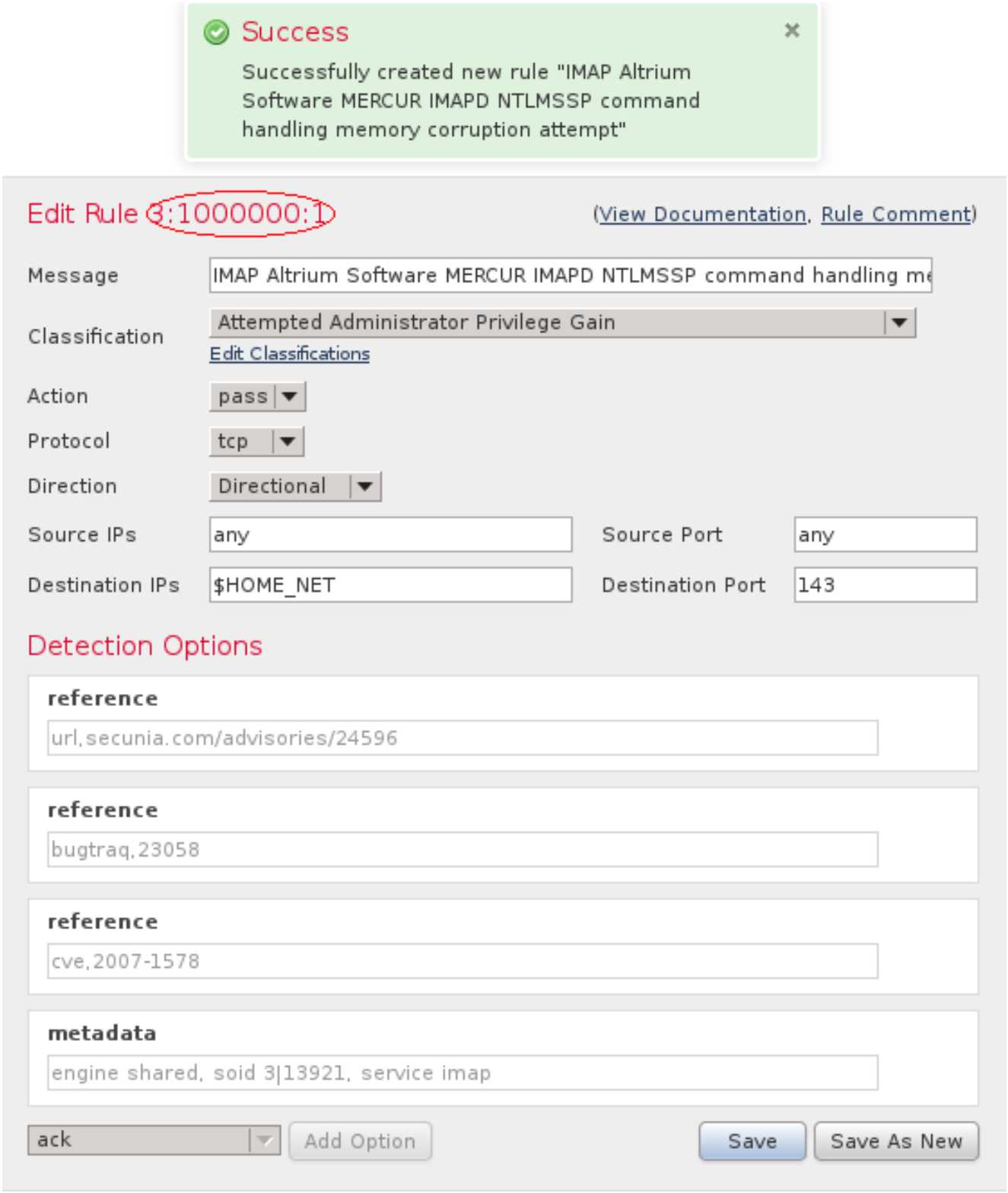
Configurazione

Crea regola di superamento

1. Selezionare **Oggetti > Regole intrusione**. Viene visualizzato l'elenco delle categorie di regole.
2. Individuare la categoria associata alla regola che si desidera filtrare. Utilizzare l'icona a forma di freccia per espandere la categoria della regola dagli elenchi delle categorie e trovare la regola per la quale si desidera creare una regola di accettazione. In alternativa, è possibile utilizzare la casella di ricerca delle regole.
3. Una volta trovata la regola desiderata, fare clic sull'icona della matita accanto ad essa per modificare la regola.
4. Quando si modifica una regola, effettuare le seguenti operazioni: Fare clic sul pulsante **Modifica** corrispondente alla regola.Nell'elenco a discesa Azione, scegliere **passa**.Modificare i campi IP di origine e IP di destinazione in host o reti per i quali non si desidera che la regola attivi un avviso.Fare clic su **Salva come nuovo**.



5. Prendere nota del numero ID della nuova regola. Ad esempio, 1000000.



Abilita regola di superamento

Ènecessario abilitare la nuova regola nei criteri per le intrusioni appropriati per consentire il passaggio del traffico sugli indirizzi di origine o di destinazione specificati. Per abilitare una regola di superamento, eseguire la procedura seguente:

1. Modificare il criterio di intrusione attivo: Selezionare **Policy > Controllo accesso > Intrusione**.Fare clic su **Modifica** accanto al criterio di intrusione attivo.
2. Aggiungere la nuova regola all'elenco delle regole: Fare clic su **Regole** nel riquadro a sinistra.Immettere l'ID regola annotato in precedenza nella casella del filtro.Selezionare la

casella di controllo Regole e modificare lo stato della regola in **Genera eventi**.Fare clic su **Informazioni criteri** nel riquadro a sinistra. Fare clic su **Commit modifiche**.

3. Fare clic su **Deploy** per distribuire le modifiche nel dispositivo.

Verifica

Èconsigliabile monitorare i nuovi eventi per un certo periodo di tempo per verificare che non vengano generati eventi per questa regola specifica per l'indirizzo IP di origine o di destinazione definito.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.