L'indirizzo IP è bloccato o inserito nella blacklist dalla Security Intelligence di un sistema Cisco FireSIGHT

Sommario

Introduzione

La funzionalità di intelligence di sicurezza consente di specificare il traffico che può attraversare la rete in base all'indirizzo IP di origine o di destinazione. Questa funzione è particolarmente utile quando si desidera creare una lista nera del traffico da e verso indirizzi IP specifici, prima che il traffico venga analizzato da regole di controllo d'accesso. In questo documento viene descritto come gestire gli scenari in cui un indirizzo IP viene bloccato o messo in blacklist da un sistema Cisco FireSIGHT.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza del Cisco FireSIGHT Management Center.

Componenti usati

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

- Cisco FireSIGHT Management Center
- Appliance Cisco Firepower

- Cisco ASA con modulo Firepower (SFR)
- Software versione 5.2 o 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.

Differenza tra i feed di intelligence e l'elenco di intelligence

Esistono due modi per utilizzare la funzionalità Security Intelligence in un sistema FireSIGHT:

Feed Security Intelligence

Un feed di Security Intelligence è una raccolta dinamica di indirizzi IP che il Centro difesa scarica da un server HTTP o HTTPS. Per facilitare la creazione di liste nere, Cisco fornisce il *feed di Security Intelligence*, che rappresenta gli indirizzi IP di cui il Vulnerability Research Team (VRT) ha determinato la reputazione insufficiente.

Elenco Security Intelligence

Un elenco di Security Intelligence, a differenza di un feed, è un semplice elenco statico di indirizzi IP che vengono caricati manualmente nel centro di gestione FireSIGHT.

L'indirizzo IP legittimo è bloccato o non elencato

Verifica se un indirizzo IP è presente nel feed di Security Intelligence

Se un indirizzo IP viene bloccato dalla lista nera dei feed di Security Intelligence, è possibile eseguire la procedura seguente per verificare questa condizione:

Passaggio 1: Accedere alla CLI dell'appliance Firepower o del modulo di servizio.

Passaggio 2: Eseguire il comando seguente. Sostituire <IP_Address> con l'indirizzo IP da cercare:

```
admin@Firepower:~$ grep
```

Ad esempio, per cercare l'indirizzo IP 198.51.100.1, eseguire il comando seguente:

```
admin@Firepower:~$ grep 198.51.100.1 /var/sf/iprep_download/*.blf
```

Se questo comando restituisce una corrispondenza per l'indirizzo IP fornito, indica che l'indirizzo IP è presente nella blacklist dei feed di Security Intelligence.

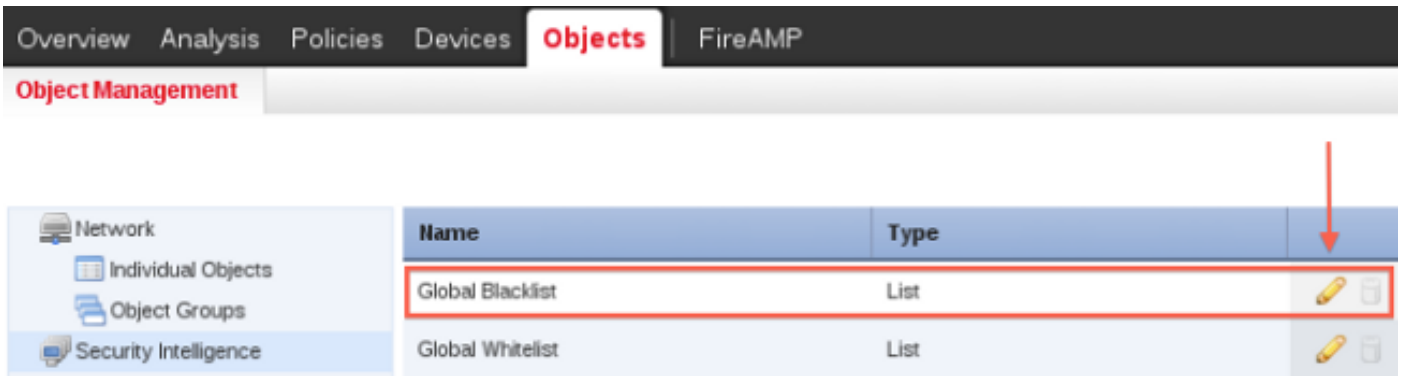
Controlla la lista nera

Per trovare un elenco degli indirizzi IP che potrebbero essere inclusi in una blacklist, procedere come segue:

Passaggio 1: Accesso all'interfaccia Web del centro di gestione FireSIGHT.

Passaggio 2: Passare a **Oggetti > Gestione oggetti > Security Intelligence**.

Passaggio 3: Fare clic sull'icona a forma di *matita* per aprire o modificare la **lista nera globale**. Viene visualizzata una finestra popup con un elenco di indirizzi IP.



Utilizzare un indirizzo IP bloccato o in blacklist

Se un determinato indirizzo IP è bloccato o non elencato dal feed di Security Intelligence, è possibile utilizzare una delle opzioni seguenti per consentirlo.

Opzione 1: Whitelist sulla Security Intelligence

Èpossibile inserire nella lista nera un indirizzo IP inserito dalla Security Intelligence. Una lista bianca sostituisce la sua lista nera. Il sistema FireSIGHT valuta il traffico con un indirizzo IP di origine o di destinazione inserito nella lista nera usando le regole di controllo dell'accesso, anche se un indirizzo IP è presente nella lista nera. È quindi possibile utilizzare una lista nera quando questa è ancora utile, ma ha un ambito troppo ampio e blocca in modo errato il traffico che si desidera ispezionare.

Ad esempio, se un feed attendibile blocca in modo improprio l'accesso a una risorsa fondamentale, ma risulta nel complesso utile per l'organizzazione, è possibile eliminare solo gli indirizzi IP classificati in modo improprio, anziché rimuovere l'intero feed dalla lista nera.

> **Attenzione:** Dopo aver apportato modifiche ai criteri di controllo di accesso, è necessario riapplicarli ai dispositivi gestiti.

Opzione 2: Applica filtro di intelligence di sicurezza per area di sicurezza

Per una maggiore granularità, è possibile applicare il filtro di Security Intelligence a seconda che l'indirizzo IP di origine o di destinazione in una connessione risieda in una determinata area di sicurezza.

Per estendere l'esempio della lista bianca sopra riportato, è possibile rendere bianca la lista degli indirizzi IP classificati in modo non corretto, ma limitare l'oggetto della lista bianca utilizzando un'area di protezione utilizzata da coloro che nell'organizzazione hanno la necessità di accedere a tali indirizzi IP. In questo modo, solo gli utenti con esigenze aziendali possono accedere agli indirizzi IP presenti nelle liste bianche. È inoltre possibile utilizzare un feed di posta indesiderata di terze parti per creare una blacklist del traffico in un'area di sicurezza del server e-mail.

Opzione 3: Monitor, anziché Blacklist

Se non si è certi di voler mettere in blacklist un particolare indirizzo IP o set di indirizzi, è possibile usare un'impostazione "solo monitor", che permette al sistema di passare la connessione corrispondente alle regole di controllo di accesso, ma anche di registrare la corrispondenza nella blacklist. Si noti che non è possibile impostare la lista nera globale come solo controllo

Considerare uno scenario in cui si desidera testare un feed di terze parti prima di implementare il blocco utilizzando tale feed. Quando si imposta il feed come solo monitor, il sistema consente di analizzare ulteriormente le connessioni che sarebbero state bloccate, ma registra anche un record di ognuna di queste connessioni per la valutazione.

Procedura per configurare l'impostazione Security Intelligence con "solo monitor":

1. Nella scheda **Security Intelligence** di un criterio di controllo di accesso fare clic sull'icona di registrazione. Viene visualizzata la finestra di dialogo Opzioni blacklist.
2. Selezionare la casella di controllo **Registra connessioni** per registrare gli eventi di inizio connessione quando il traffico soddisfa le condizioni di Security Intelligence.
3. Specificare dove inviare gli eventi di connessione.
4. Fare clic su **OK** per impostare le opzioni di registrazione. Verrà nuovamente visualizzata la scheda Intelligence per la sicurezza.
5. Fare clic su **Salva**. Per rendere effettive le modifiche, è necessario applicare i criteri di controllo di accesso.

Opzione 4: Contatta il Technical Assistance Center di Cisco

Èsempre possibile contattare il Technical Assistance Center di Cisco nei seguenti casi:

- Hai delle domande con le opzioni 1, 2 o 3 di cui sopra.
- Si desiderano ulteriori ricerche e analisi su un indirizzo IP non presente nella lista nera di Security Intelligence.
- Si desidera una spiegazione del motivo per cui l'indirizzo IP è incluso nella blacklist di Security Intelligence.