Configurazione di un sistema FireSIGHT per l'invio di avvisi a un server Syslog esterno

Sommario

Introduzione

Mentre un sistema FireSIGHT fornisce diverse viste degli eventi all'interno dell'interfaccia web, è possibile configurare la notifica degli eventi esterni per facilitare il monitoraggio costante dei sistemi critici. È possibile configurare un sistema FireSIGHT in modo da generare avvisi che inviano una notifica via e-mail, trap SNMP o syslog quando viene generata una delle seguenti condizioni. In questo articolo viene descritto come configurare un centro di gestione FireSIGHT per l'invio di avvisi su un server Syslog esterno.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Syslog e FireSIGHT Management Center. Inoltre, la porta syslog (l'impostazione predefinita è 514) deve essere consentita nel firewall.

Componenti usati

Le informazioni fornite in questo documento si basano sul software versione 5.2 o successive.

> **Attenzione:** Le informazioni discusse in questo documento fanno riferimento a un accessorio installato in uno specifico ambiente di emulazione e la configurazione iniziale è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Invio di avvisi di intrusione

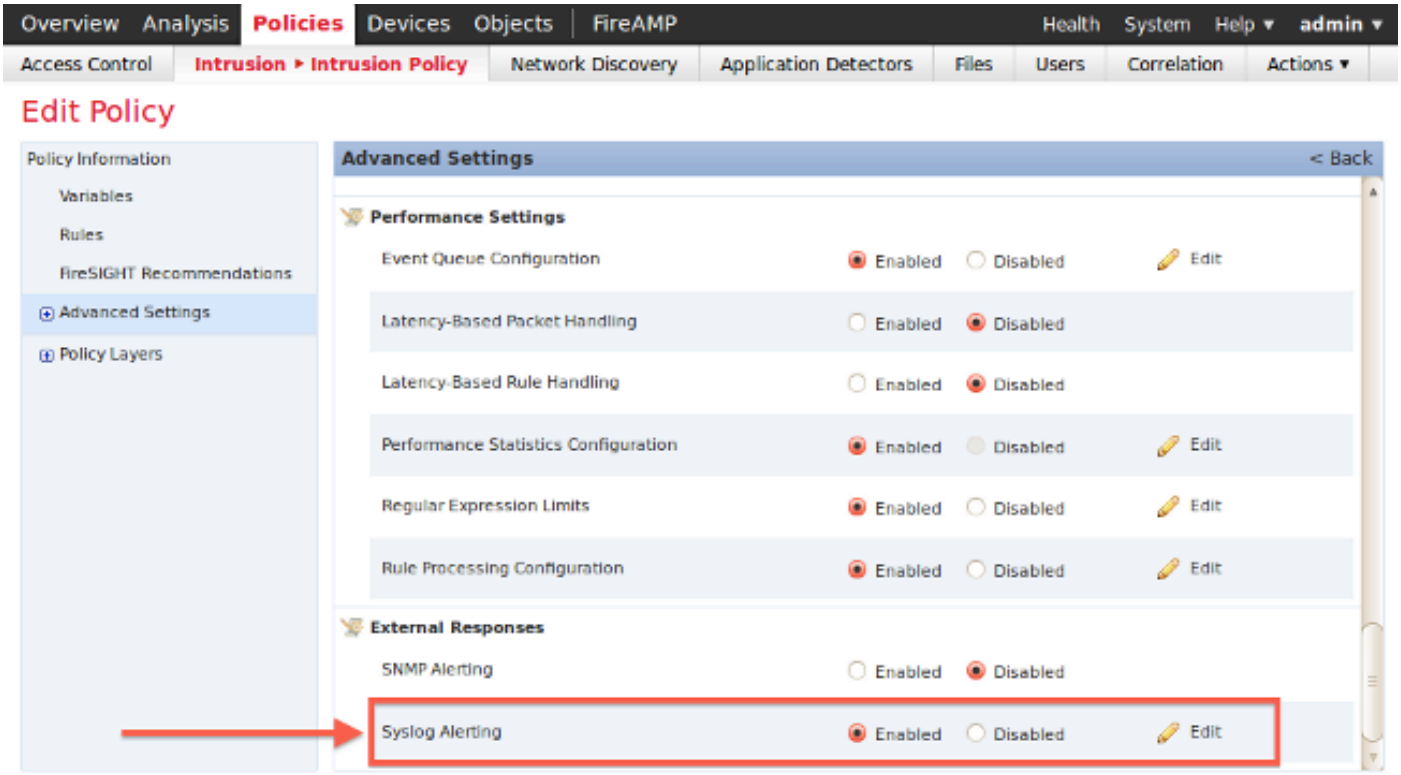
1. Accedere all'interfaccia utente Web del centro di gestione FireSIGHT.

2. Passare a **Criteri** > **Intrusione** > **Criteri intrusione**.

3. Fare clic su **Modifica** accanto al criterio che si desidera applicare.

4. Fare clic su **Advanced Settings** (Impostazioni avanzate).

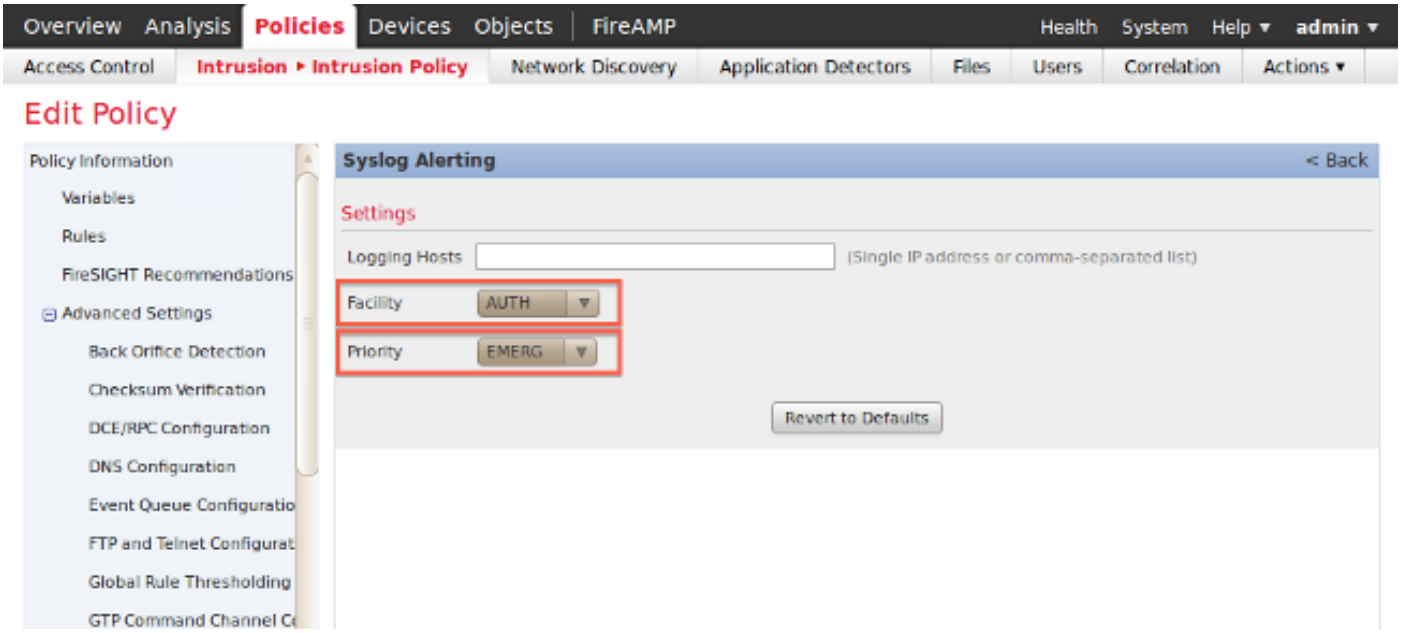
5. Individuare **Syslog Alerting** nell'elenco e impostarlo su **Enabled**.



6. Fare clic su **Modifica** a destra di **Syslog Alerting**.

7. Digitare l'indirizzo IP del server syslog nel campo **Host di registrazione**.

8. Scegliere una **struttura** e una **gravità** appropriate dal menu a discesa. A meno che un server syslog non sia configurato per accettare gli avvisi per una determinata struttura o gravità, è possibile lasciare questi valori ai valori predefiniti.



9. Fai clic su **Informazioni** sul **criterio** in alto a sinistra in questa schermata.

10. Fare clic sul pulsante **Conferma modifiche**.

11. Riapplicare la policy antintrusione.

> **Nota:** Per generare gli avvisi, utilizzare questo criterio di intrusione nella regola di controllo di accesso. Se non è stata configurata alcuna regola di controllo d'accesso, impostare il criterio di intrusione da utilizzare come azione predefinita del criterio di controllo d'accesso e riapplicare il criterio di controllo d'accesso.

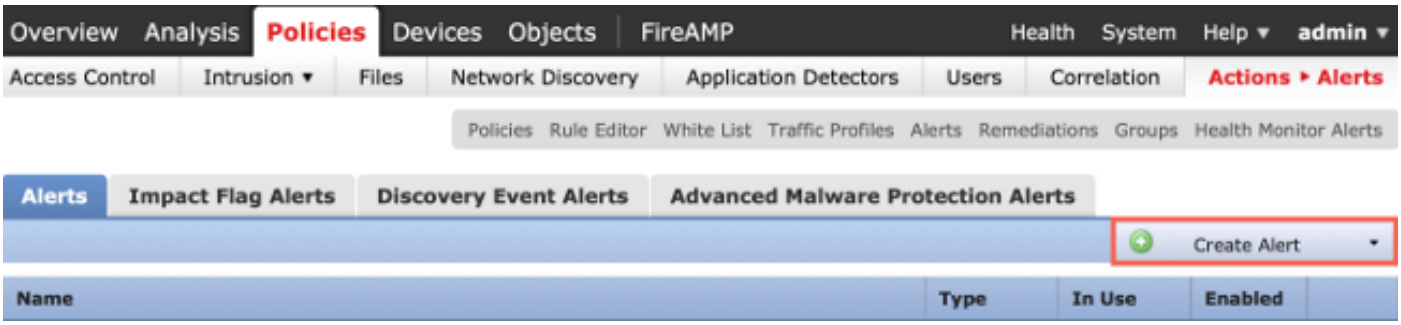
Ora, se un evento di intrusione viene attivato su tale criterio, verrà inviato un avviso anche al server syslog configurato sul criterio di intrusione.

Invio di avvisi sullo stato

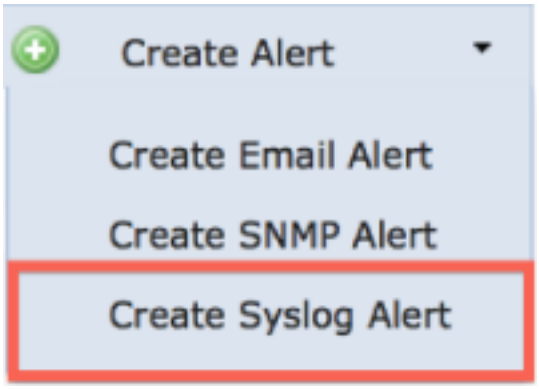
Parte 1: Creazione di un avviso di syslog

1. Accedere all'interfaccia utente Web del centro di gestione FireSIGHT.

2. Passare a **Criteri > Azioni > Alert**.



3. Selezionare **Crea avviso**, che si trova sul lato destro dell'interfaccia Web.



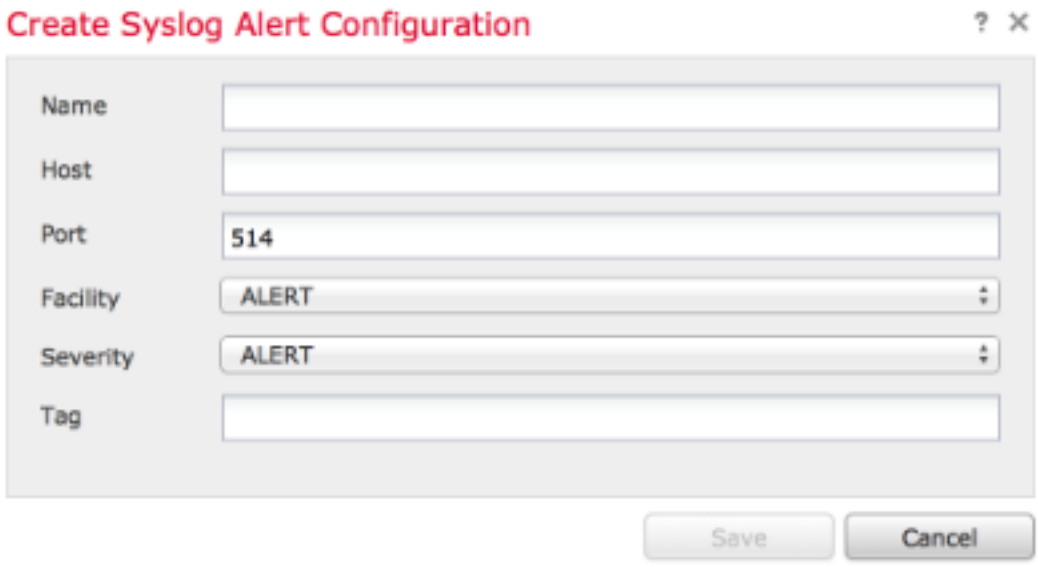
4. Fare clic su **Crea avviso syslog**. Viene visualizzata una finestra popup di configurazione.

5. Specificare un nome per l'avviso.

6. Inserire l'indirizzo IP del server syslog nel campo **Host**.

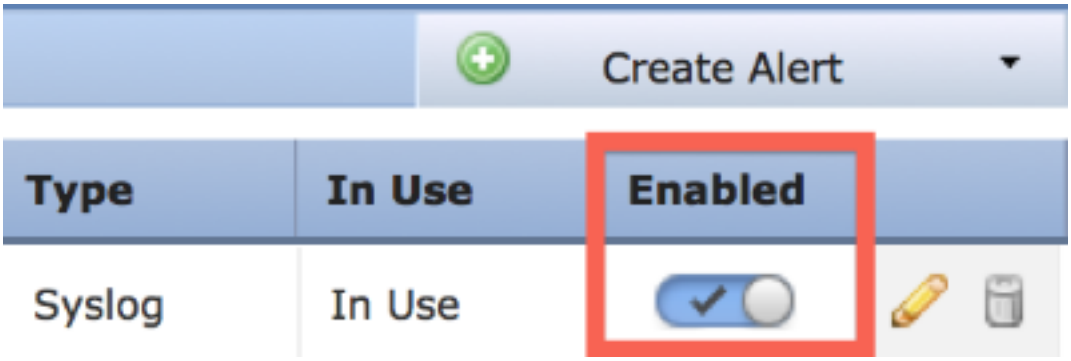
7. Cambiare la porta se necessario per il server syslog (la porta predefinita è 514).

8. Selezionare una **struttura** e una **gravità** appropriate.



9. Fare clic sul pulsante **Salva**. Si tornerà alla pagina **Criteri > Azioni > Alert**.

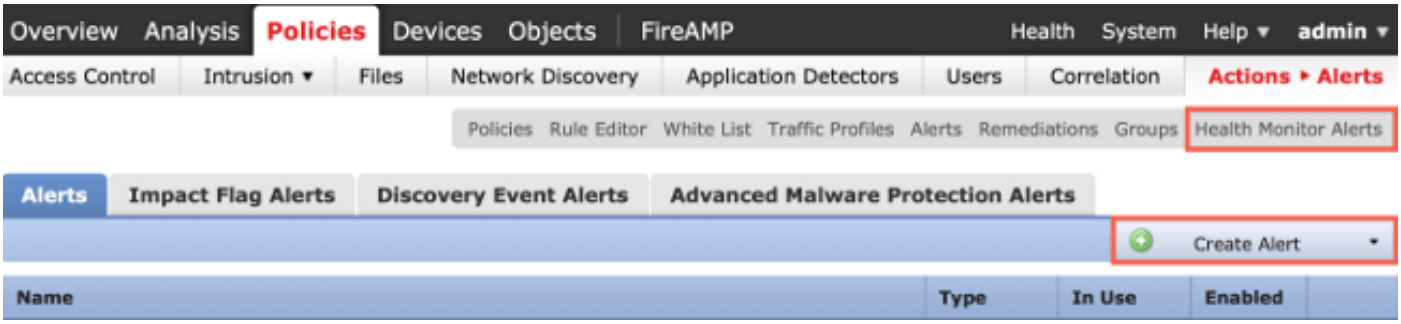
10. Abilitare la configurazione Syslog.



Parte 2: Creazione di avvisi di Health Monitor

La seguente istruzione descrive i passaggi per configurare **gli avvisi di Health Monitor** che utilizzano l'avviso syslog appena creato (nella sezione precedente):

1. Andare alla pagina **Criteri > Azioni > Alert** e scegliere **Alert di Health Monitor**, che si trova nella parte superiore della pagina.



2. Assegnare un nome all'avviso di stato.

3. Scegliere un tipo di **severità** (è possibile selezionare più tipi di severità tenendo premuto il tasto CTRL mentre si fa clic).

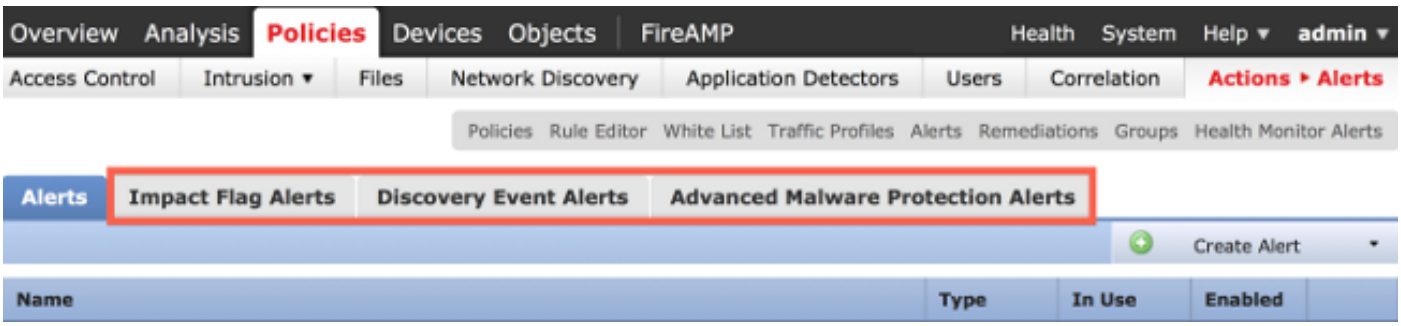
4. Dalla colonna **Modulo** scegliere i moduli di stato per i quali si desidera inviare gli avvisi al server syslog (ad esempio, Uso del disco).

5. Selezionare l'alert di syslog creato in precedenza dalla colonna **Alert**.

6. Fare clic sul pulsante **Salva**.

Invio di flag di impatto, avvisi di rilevamento eventi e malware

Èinoltre possibile configurare un centro di gestione FireSIGHT per inviare avvisi syslog per eventi con un flag di impatto specifico, un tipo specifico di eventi di rilevamento ed eventi malware. A tale scopo, è necessario eseguire la Parte 1: Creare un avviso di syslog e quindi configurare il tipo di eventi che si desidera inviare al server syslog. A tale scopo, passare alla pagina **Criteri > Azioni > Alert** e quindi selezionare una scheda per il tipo di alert desiderato.



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).