Een FireSIGHT-systeem configureren voor het verzenden van meldingen naar een externe systeemserver

Inhoud

Inleiding

Terwijl een FireSIGHT-systeem verschillende weergaven van gebeurtenissen biedt binnen zijn webinterface, kunt u externe gebeurtenismeldingen configureren om constante bewaking van kritieke systemen te vergemakkelijken. U kunt een FireSIGHT-systeem configureren om waarschuwingen te genereren die u via e-mail, SNMP-trap of syslog op de hoogte stellen wanneer een van de volgende bronnen wordt gegenereerd. In dit artikel wordt beschreven hoe u een FireSIGHT Management Center kunt configureren voor het verzenden van meldingen op een externe Syslog-server.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van Syslog en FireSIGHT Management Center. Ook moet de syslog poort (standaard is 514) worden toegestaan in uw firewall.

Gebruikte componenten

De informatie in dit document is gebaseerd op Software versie 5.2 of hoger.

Voorzichtig: De informatie in dit document wordt gemaakt van een apparaat in een

specifieke laboratoriumomgeving en gestart met een gewist (standaard) configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Inbraakmeldingen verzenden

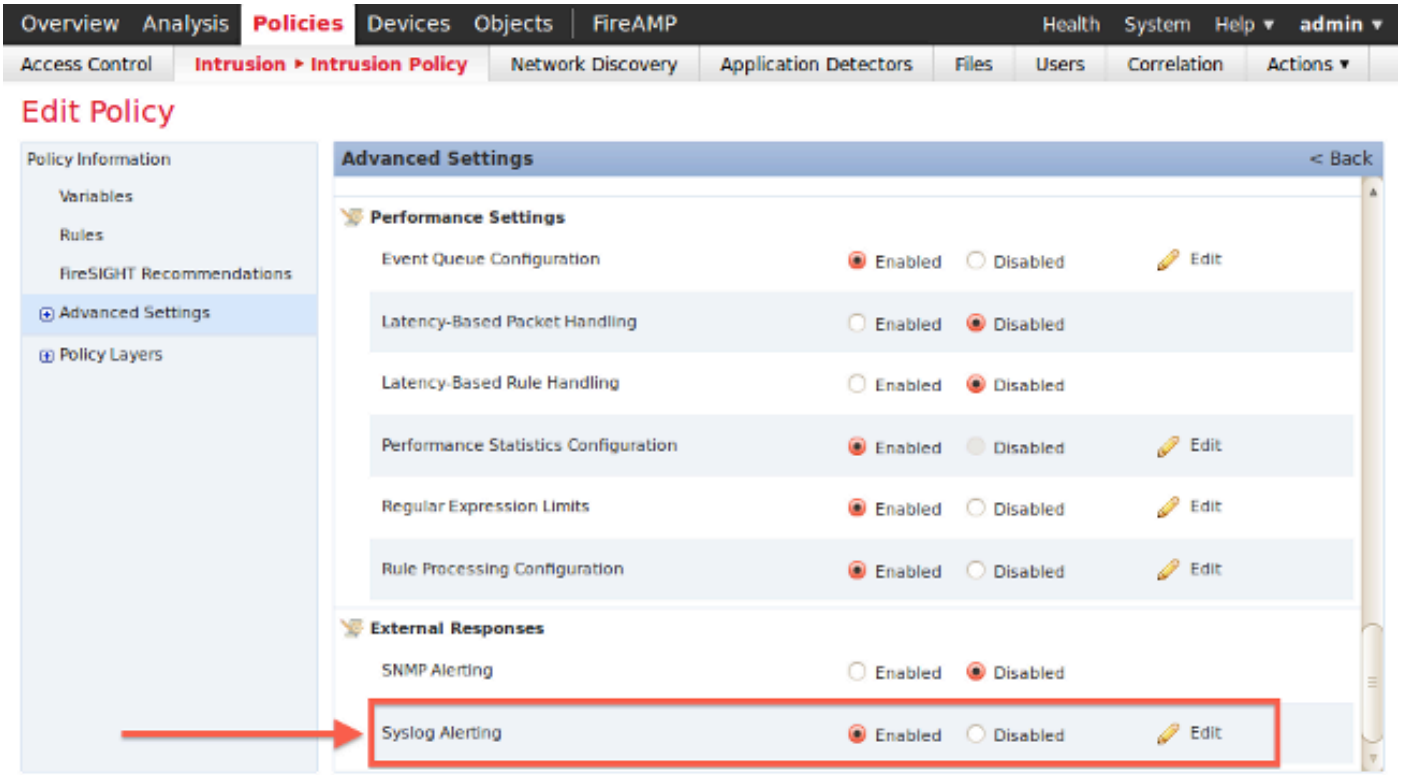
1. Log in op de webgebruikersinterface van uw FireSIGHT Management Center.

2. Ga naar **Beleid** > **Inbraakbeleid** > **Inbraakbeleid**.

3. Klik op **Bewerken** naast het beleid dat u wilt toepassen.

4. Klik op **Geavanceerde instellingen**.

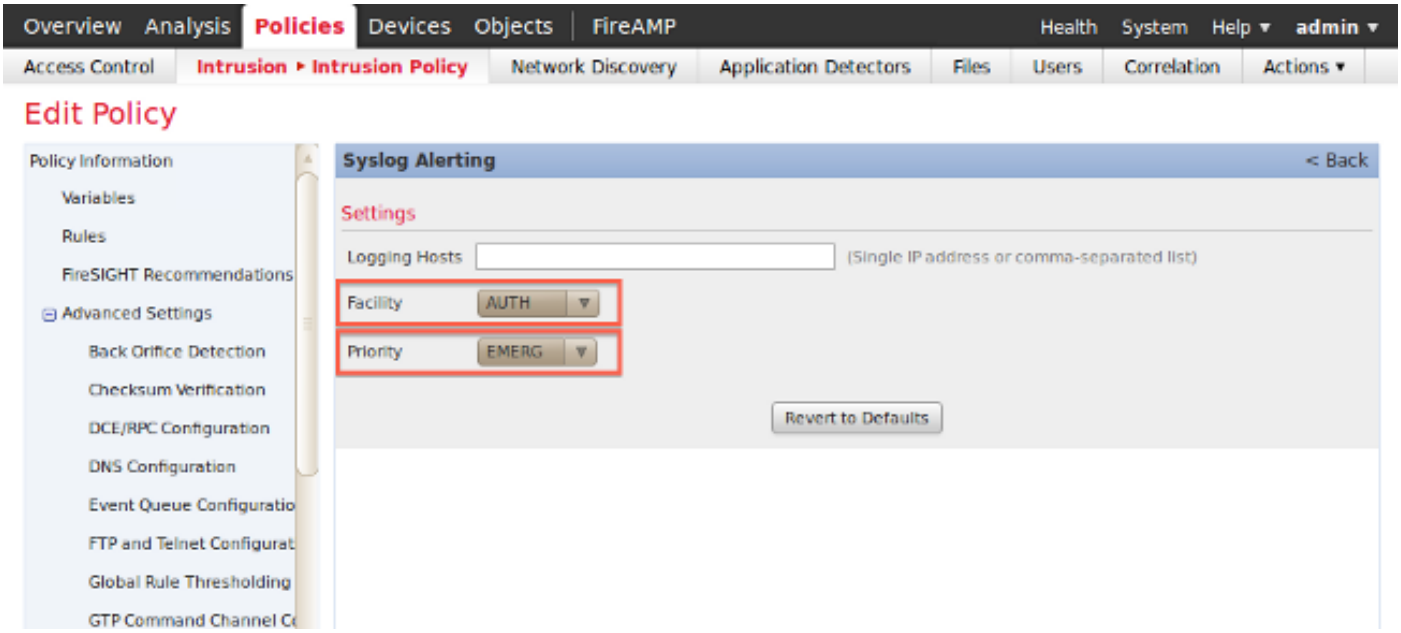
5. Zoek **Syslog Alerting** in de lijst en stel het in op **Ingeschakeld**.



6. Klik op **Bewerken** rechts van **Syslog Alerting**.

7. Typ het IP-adres van uw syslogserver in het veld **Logging Hosts**.

8. Kies een geschikte **voorziening** en **ernst** uit het vervolgkeuzemenu. Deze kunnen bij de standaardwaarden worden gelaten tenzij een syslogserver wordt geconfigureerd om waarschuwingen voor een bepaalde faciliteit of ernst te accepteren.



9. Klik op **Beleidsinformatie** linksboven op dit scherm.

10. Klik op de knop **Opdrachtwijzigingen**.

11. Pas uw inbraakbeleid opnieuw toe.

> **Opmerking:** Gebruik dit inbraakbeleid in de toegangscontroleregel om waarschuwingen te genereren. Als er geen toegangscontroleregel is geconfigureerd, stel dit inbraakbeleid dan in om te worden gebruikt als de standaardactie van het toegangscontrolebeleid en pas het toegangscontrolebeleid opnieuw toe.

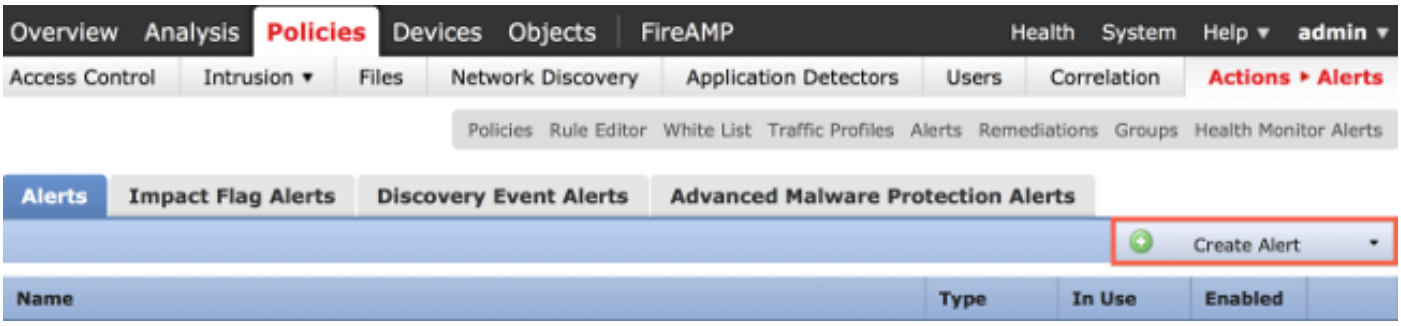
Nu als een inbraakgebeurtenis op dat beleid wordt teweeggebracht, zal een alarm ook naar de syslog server worden verzonden die op het inbraakbeleid wordt gevormd.

Gezondheidswaarschuwingen verzenden

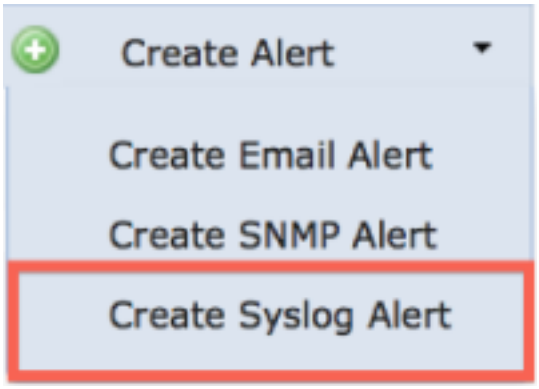
Deel 1: Een systeemwaarschuwing maken

1. Log in op de webgebruikersinterface van uw FireSIGHT Management Center.

2. Ga naar **Beleid > Acties > Waarschuwingen**.



3. Selecteer **Waarschuwing maken** aan de rechterkant van de webinterface.



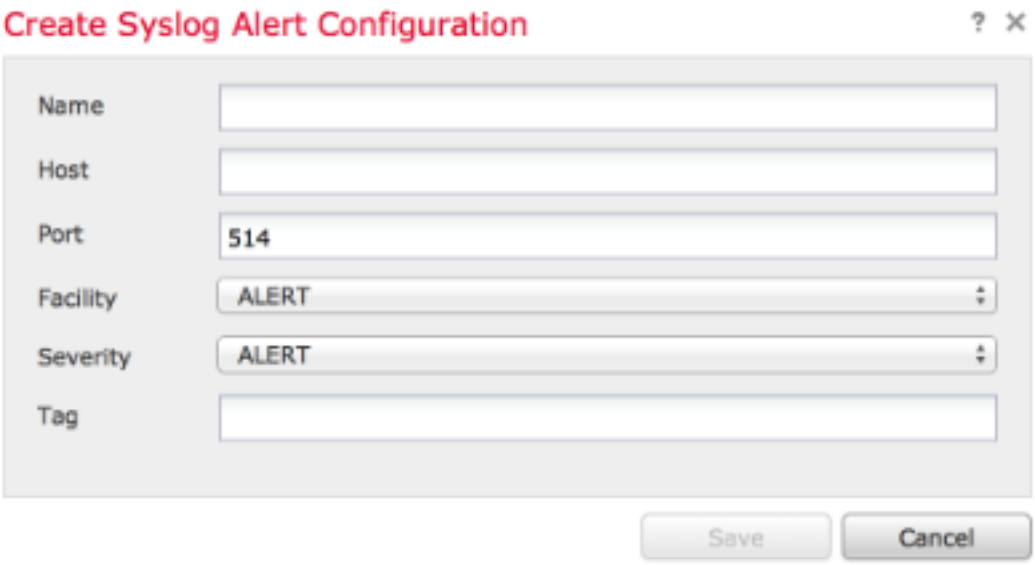
4. Klik op **Syslog-waarschuwing maken**. Er verschijnt een pop-upvenster voor configuratie.

5. Geef een naam voor de signalering.

6. Vul het IP-adres van uw syslogserver in in het veld **Host**.

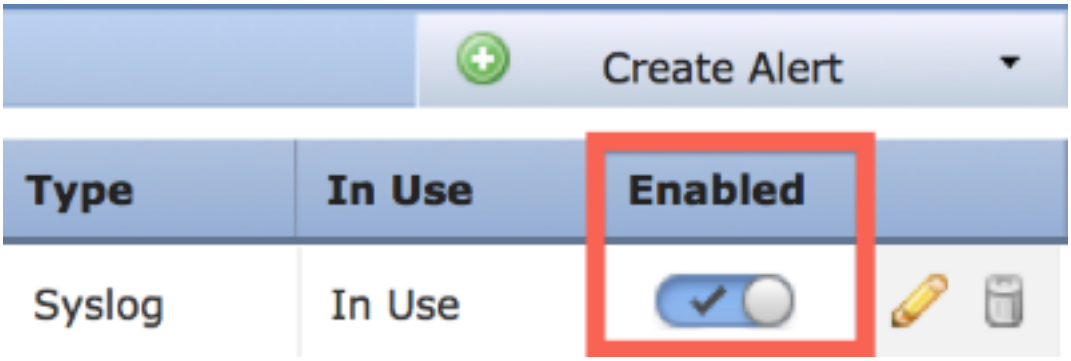
7. Verander de poort indien nodig door uw syslogserver (de standaardpoort is 514).

8. Selecteer een geschikte **voorziening** en **ernst**.



9. Klik op de knop **Opslaan**. U keert terug naar de pagina **Beleid > Acties > Waarschuwingen**.

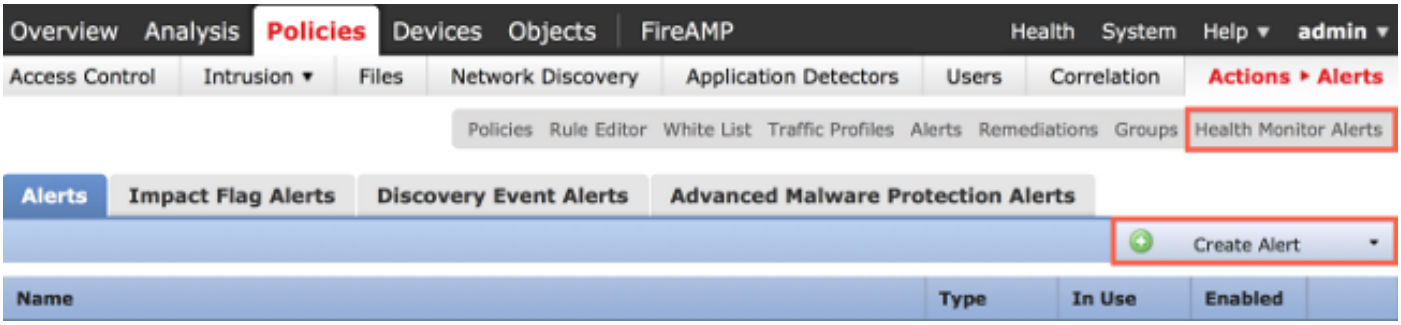
10. Schakel de Syslog-configuratie in.



Deel 2: Waarschuwingen voor Health Monitor aanmaken

De volgende instructie beschrijft de stappen om **Waarschuwingen voor** gezondheidsmonitor te configureren die gebruik maken van de syslogwaarschuwing die u zojuist hebt aangemaakt (in de vorige sectie):

1. Ga naar **Beleid > Acties > Waarschuwingen** pagina en kies **Waarschuwingen voor gezondheidsmonitor**, die zich boven aan de pagina bevindt.



2. Geef de gezondheidswaarschuwing een naam.

3. Kies een **Ernst** (door de CTRL-toets ingedrukt te houden terwijl u op de knop klikt, kan meer dan één ernsttype worden geselecteerd).

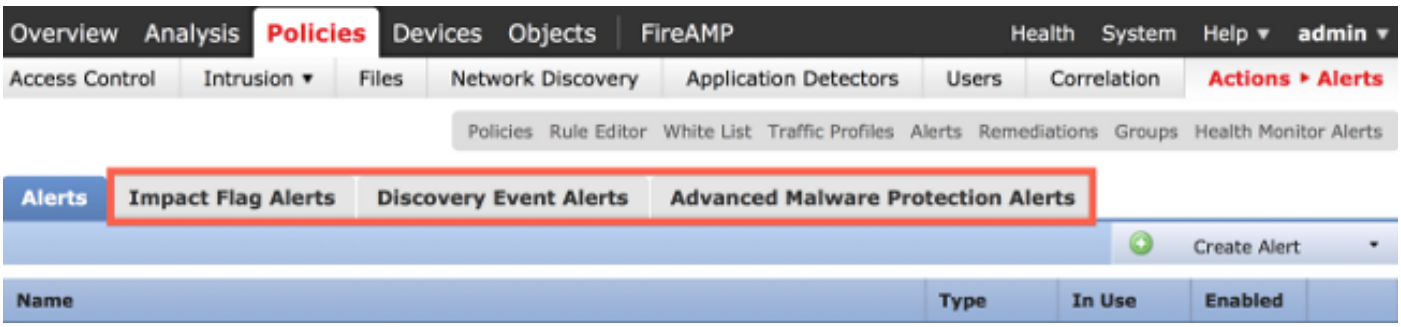
4. Kies in de **Module-kolom** de gezondheidsmodules waarvoor u meldingen naar de syslogserver wilt verzenden (bijvoorbeeld Disk Usage).

5. Selecteer een eerder gemaakt syslog-waarschuwing in de kolom **Waarschuwingen**.

6. Klik op de knop **Opslaan**.

Impact Flag verzenden, gebeurtenissen ontdekken en meldingen van malware opsporen

U kunt ook een FireSIGHT Management Center configureren om syslog-waarschuwingen te verzenden voor gebeurtenissen met een specifieke impactvlag, een specifiek type ontdekkingsgebeurtenissen en malware-gebeurtenissen. Om dat te doen, moet u Deel 1: Maak een Syslog Alert en stel vervolgens het type gebeurtenissen in dat u naar uw syslog server wilt verzenden. U kunt dat doen door te navigeren naar de pagina **Beleid > Acties > Waarschuwingen** en vervolgens een tabblad te selecteren voor het gewenste type waarschuwing.



Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.