URL-filtering op een FireSIGHT-systeemconfiguratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft de stappen om URL-filtering op FireSIGHT System te configureren. Met de functie URL-filtering op FireSIGHT Management Center kunt u een voorwaarde in een toegangscontroleregel schrijven om te bepalen welk verkeer via een netwerk verloopt op basis van niet-versleutelde URL-verzoeken van de gecontroleerde hosts.

Voorwaarden

Vereisten

Dit document bevat een aantal specifieke vereisten voor de URL-filteringslicentie en de poort.

Vereiste URL-filteringslicentie

Een FireSIGHT Management Center vereist een URL-filtering licentie om regelmatig contact op te nemen met de cloud voor een update van URL-informatie. U kunt op categorie en reputatie gebaseerde URL-voorwaarden toevoegen aan toegangscontroleregels zonder URL-filtering licentie; u kunt het toegangscontrolebeleid echter pas toepassen als u eerst een URL-filtering-licentie aan het FireSIGHT Management Center toevoegt en deze vervolgens inschakelt op de apparaten waarop het beleid is gericht.

Als een URL-filtering-licentie verloopt, stoppen de toegangscontroleregels met op categorie en reputatie gebaseerde URL-voorwaarden met het filteren van URL's en neemt het FireSIGHT Management Center niet langer contact op met de cloudservice. Zonder een URL-filtering-licentie kunnen afzonderlijke URL's of groepen URL's worden ingesteld om toe te staan of te blokkeren,

maar de URL-categorie of reputatiegegevens kunnen niet worden gebruikt om het netwerkverkeer te filteren.

Poortvereiste

Een FireSIGHT-systeem maakt gebruik van poorten 443/HTTPS en 80/HTTP om te communiceren met de cloudservice. Port 443/HTTPS moet bidirectioneel worden geopend en inkomende toegang tot poort 80/HTTP moet worden toegestaan op het FireSIGHT Management Center.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies:

- FirePOWER-applicaties: 7000 Series, 8000 Series
- Virtuele applicatie voor Next Generation Inbraakpreventiesysteem (NGIPS)
- Adaptieve security applicatie (ASA) FirePOWER
- Sourcefire-softwareversie 5.2 of hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

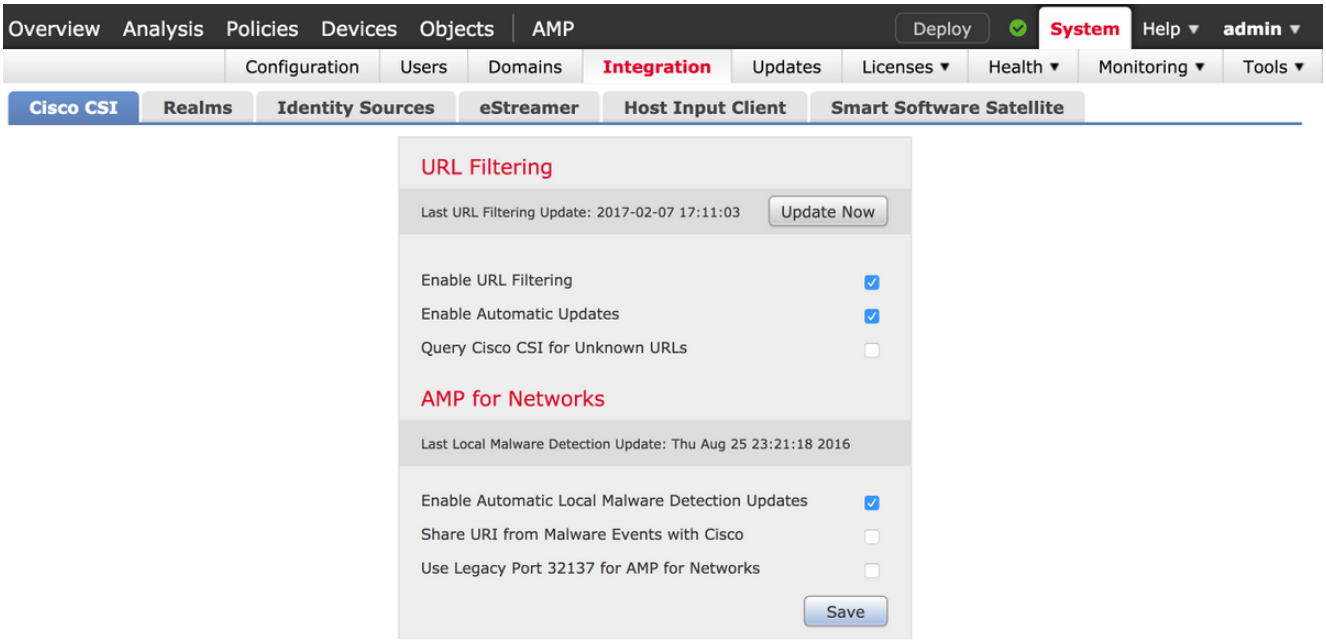
URL-filtering voor FireSIGHT Management Center inschakelen

Voltooi de volgende stappen om URL-filtering in te schakelen:

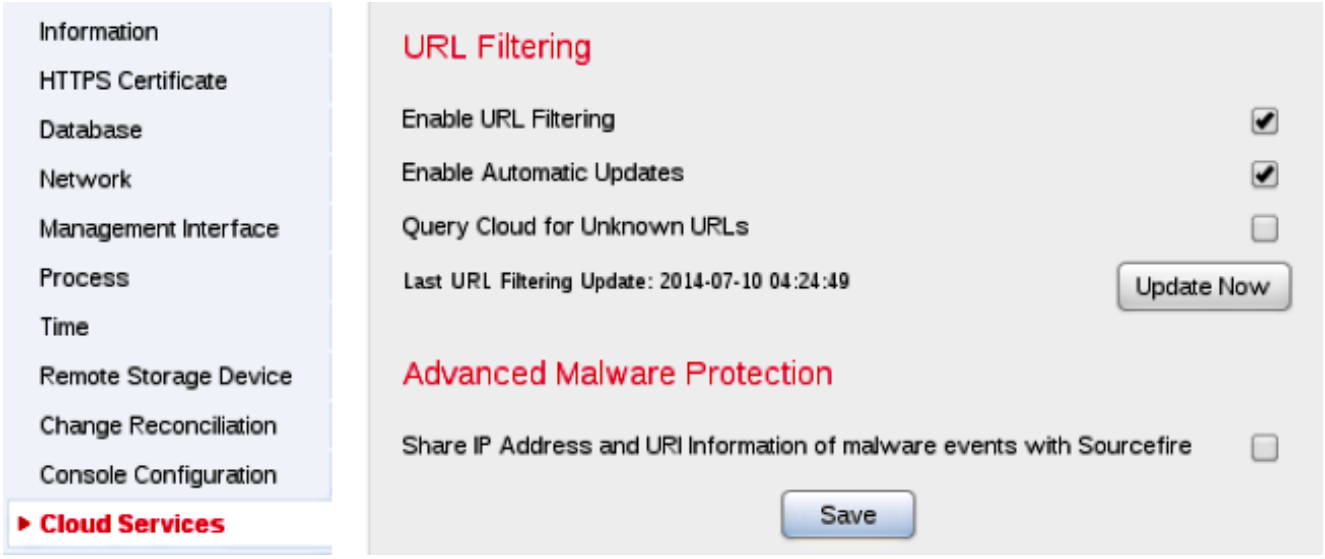
1. Log in op de webgebruikersinterface van het FireSIGHT Management Center.

2. De navigatie is anders op basis van de softwareversie die u uitvoert:

   Kies in versie 6.1.x **Systeem > Integratie > Cisco CSI**.



Kies in Versie 5.x **Systeem > Lokaal > Configuratie**. Kies **voor cloudservices**.



3. Controleer het aanvinkvakje **URL-filtering inschakelen** om URL-filtering in te schakelen.
4. Desgewenst schakelt u het aanvinkvakje **Automatische updates inschakelen** in om automatische updates in te schakelen. Met deze optie kan het systeem regelmatig contact opnemen met de cloudservice om updates voor de URL-gegevens in de lokale gegevenssets van het apparaat te verkrijgen.

   Opmerking: Hoewel de cloudservice zijn gegevens doorgaans één keer per dag bijwerkt, dwingt deze, als u automatische updates inschakelt, het FireSIGHT Management Center om elke 30 minuten te controleren om ervoor te zorgen dat de informatie altijd actueel is. Hoewel de dagelijkse updates vaak klein zijn, als het meer dan vijf dagen sinds de laatste update is geweest, zouden de nieuwe URL filtering gegevens tot 20 minuten kunnen duren om te downloaden. Nadat de updates zijn gedownload, kan het tot 30 minuten duren om de update zelf uit te voeren.

5. Desgewenst schakelt u het selectievakje **Query Cloud for Unknown URL** for Unknown URLs in om de cloudservice voor onbekende URL's te doorzoeken. Met deze optie kan het systeem de Sourcefire-cloud opvragen wanneer iemand op uw bewaakte netwerk probeert te

bladeren naar een URL die niet in de lokale gegevensset staat. Als de cloud de categorie of reputatie van een URL niet kent, of als het FireSIGHT Management Center geen contact kan opnemen met de cloud, komt de URL niet overeen met toegangscontroleregels met op categorie of reputatie gebaseerde URL-voorwaarden.

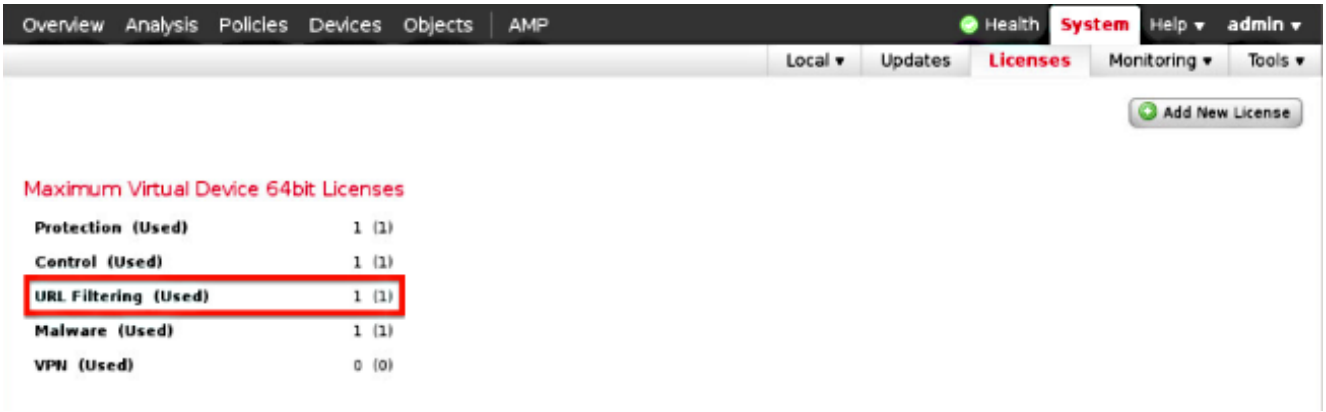
Opmerking: U kunt geen categorieën of reputaties handmatig aan URL's toewijzen. Schakel deze optie uit als u niet wilt dat uw niet-gecategoriseerde URL's worden gecatalogiseerd door de Sourcefire-cloud, bijvoorbeeld om privacyredenen.

6. Klik op **Save** (Opslaan). URL-filtering-instellingen worden opgeslagen.

   Opmerking: Gebaseerd op de tijdsduur sinds URL-filtering voor het laatst is ingeschakeld of als dit de eerste keer is dat u URL-filtering hebt ingeschakeld, haalt een FireSIGHT Management Center de URL-filtering gegevens van de cloudservice op.

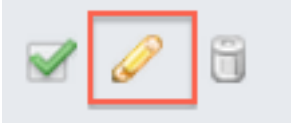
Licentie voor URL-filtering toepassen op een beheerd apparaat

1. Controleer of de URL-filtering op het FireSIGHT Management Center is geïnstalleerd. Ga naar de pagina **Systeem > Licenties** om een lijst met licenties te vinden.

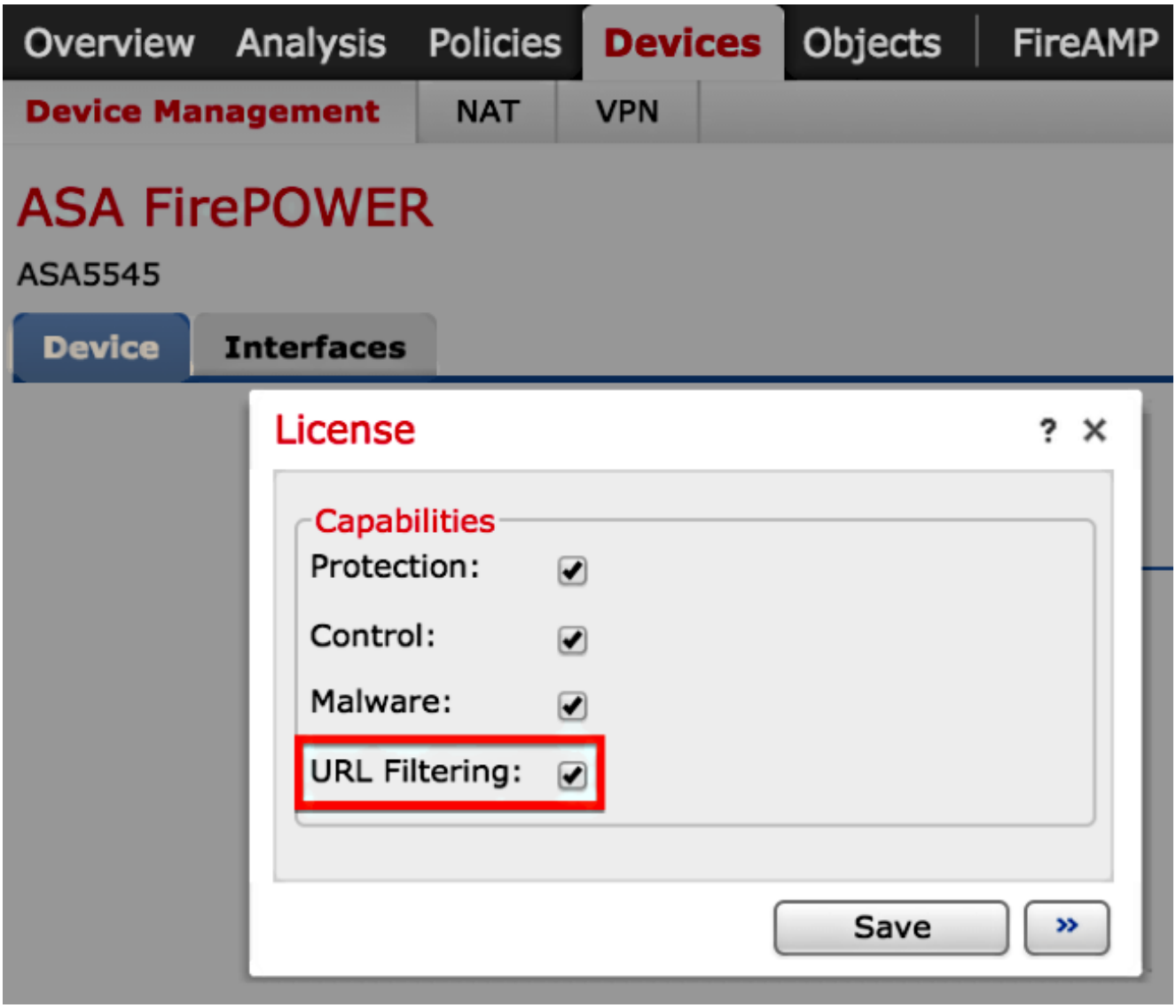


2. Ga naar de pagina **Apparaten > Apparaatbeheer** en controleer of de URL-filterlicentie is toegepast op het apparaat dat het verkeer controleert.

3. Als de URL-filtering licentie niet op een apparaat wordt toegepast, klikt u op het **potlood-**pictogram om de instellingen te bewerken. Het pictogram bevindt zich naast de apparaatnaam.



4. U kunt de URL-filtering licentie op een apparaat inschakelen via het tabblad **Apparaten**.



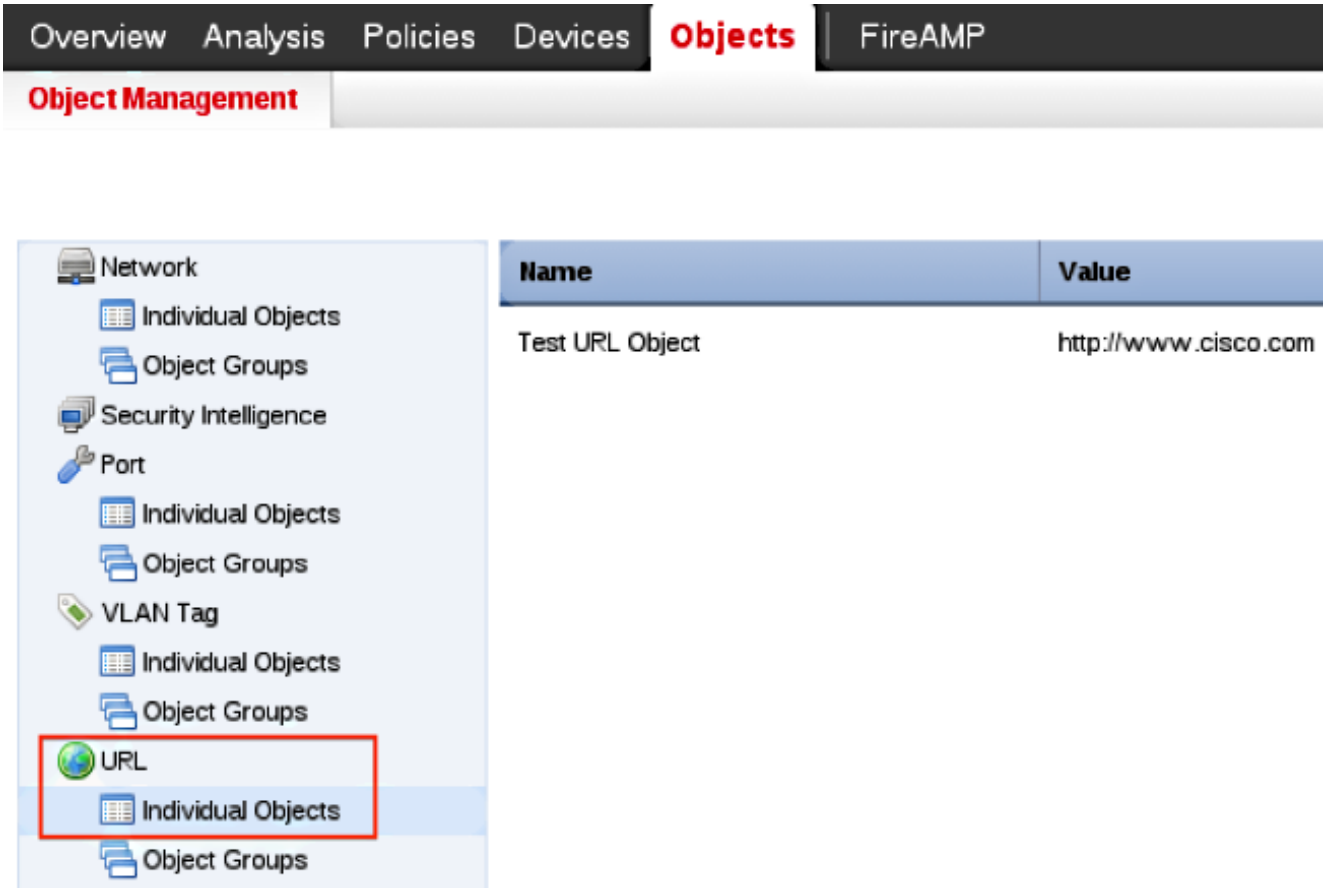
5. Nadat u een licentie hebt ingeschakeld en uw wijzigingen hebt opgeslagen, moet u ook op **Wijzigingen toepassen** klikken om de licentie op uw beheerde apparaat toe te passen.

Uitsluiting van een specifieke site van geblokkeerde URL-categorie

FireSIGHT Management Center staat u niet toe om een lokale classificatie van URL's te hebben die de standaard opgegeven categorieën van Sourcefire overschreven. Om deze taak te kunnen uitvoeren, moet u een toegangscontrolebeleid gebruiken. Deze instructies beschrijven hoe u een URL-object in een toegangscontroleregel kunt gebruiken om een specifieke site uit te sluiten van een blokcategorie.

1. Ga naar de pagina **Objecten > Objectbeheer**.

2. **Kies Individuele objecten** voor URL en klik op de knop **URL toevoegen**. Het venster **URL-objecten** wordt weergegeven.

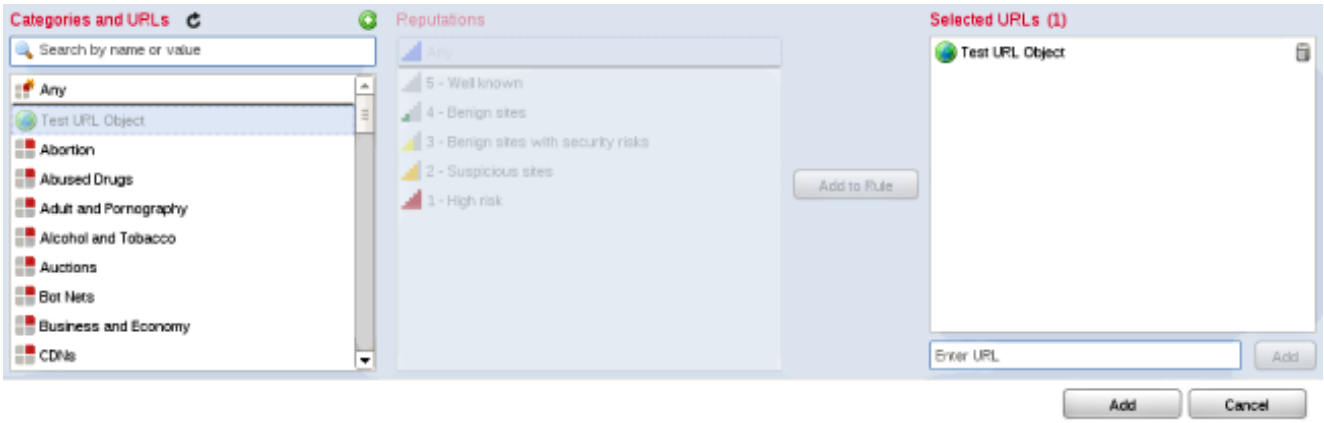


3. Nadat u de wijzigingen hebt opgeslagen, kiest u **Beleid > Toegangsbeheer** en klikt u op het **potlood-**pictogram om het Toegangsbeheer te bewerken.

4. Klik op **Regel toevoegen**.

5. Voeg uw URL-object toe aan de regel met de actie **Toestaan** en plaats het boven de URL-

categorieregel, zodat de regelactie eerst wordt geëvalueerd.



6. Nadat u de regel hebt toegevoegd, klikt u op **Opslaan en Toepassen**. Het slaat de nieuwe wijzigingen op en past het beleid voor toegangscontrole toe op beheerde apparaten.

Verifiëren

Raadpleeg voor informatie over verificatie of probleemoplossing het artikel **Problemen oplossen met URL-filtering op FireSIGHT System** dat is gekoppeld in het gedeelte Verwante informatie.

Problemen oplossen

Raadpleeg voor Controleer of problemen oplossen de volgende informatie: **Problemen oplossen met URL-filtering op FireSIGHT-systeem** artikel in het gedeelte Verwante informatie.

Gerelateerde informatie

- Problemen oplossen met URL-filtering op FireSIGHT-systeem
- Technische ondersteuning en documentatie – Cisco Systems

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.