Beleid voor AMP-bestand configureren en testen via FDM

Inhoud

Inleiding

Dit document beschrijft hoe u een Advanced Malware Protection (AMP)-bestandsbeleid kunt configureren en testen via Firepower Device Manager (FDM).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Device Manager (FDM)
- Firepower Threat Defense (FTD)

Gebruikte componenten

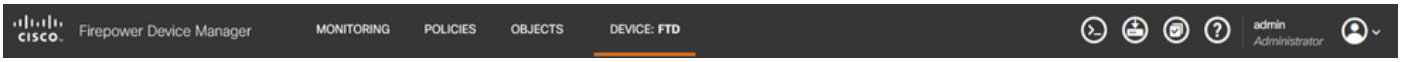
- Cisco virtuele FTD versie 7.0 beheerd via FDM
- Evaluatielicentie (evaluatielicentie) wordt gebruikt voor demonstratiedoeleinden. Cisco raadt aan een geldige licentie te verkrijgen en te gebruiken)

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Instructies

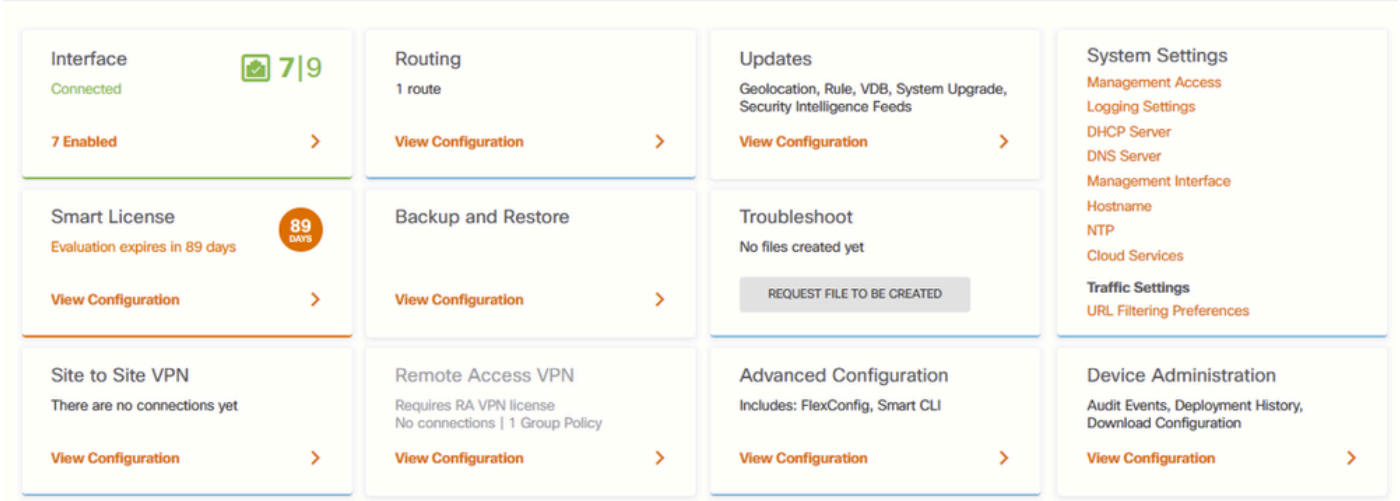
Licentie

1. Om de malware-licentie in te schakelen, navigeer naar de APPARAATpagina op de FDM GUI.



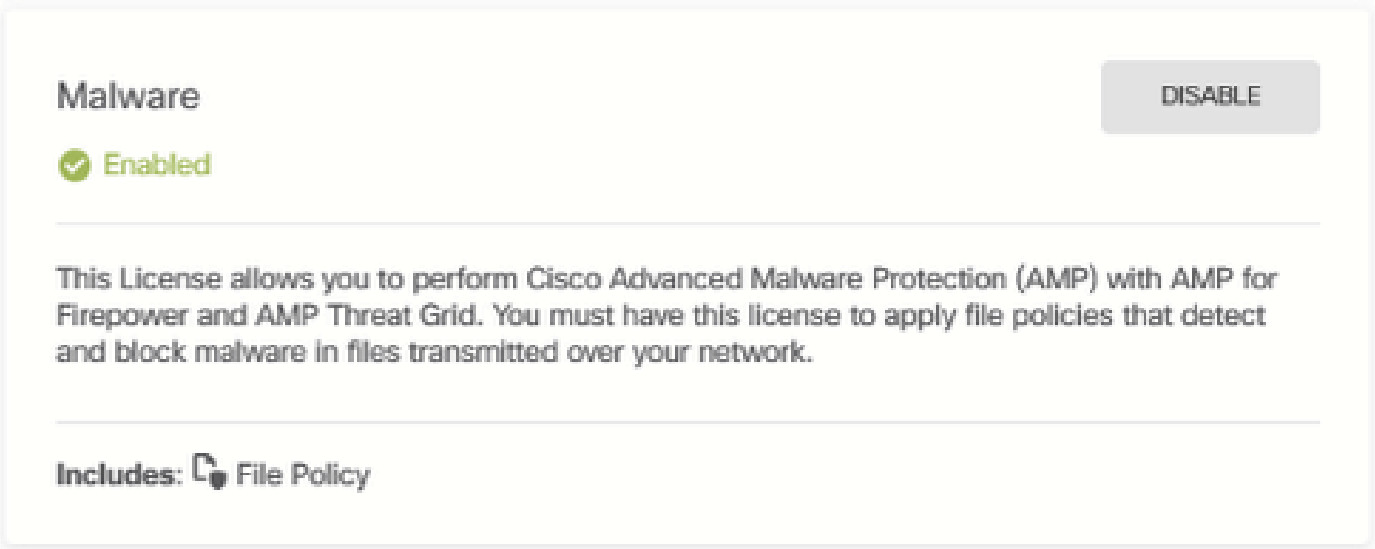
Tabblad FDM-apparaat

2. Zoek het vak met de naam Smart License (slimme licentie) en klik op View Configuration.



FDM-apparaatpagina

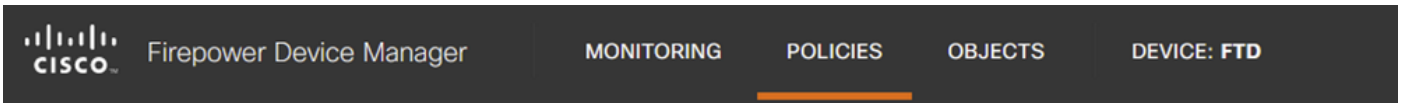
3. Schakel de licentie met het label Malware in.



Malware-licentie

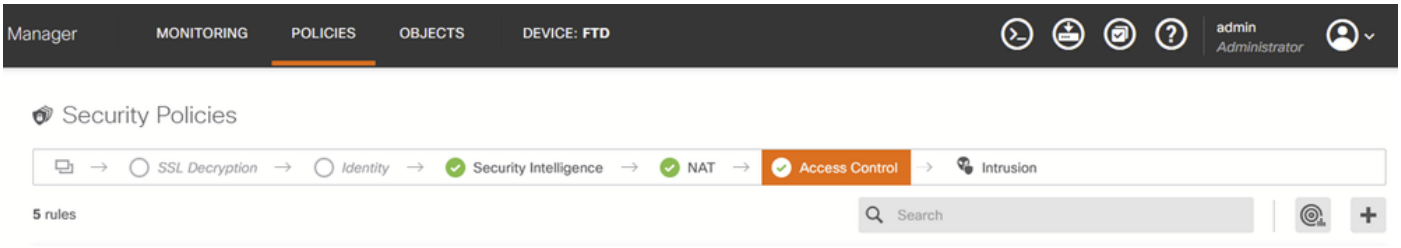
Configuratie

1. Navigeer naar de beleidspagina op de FDM.



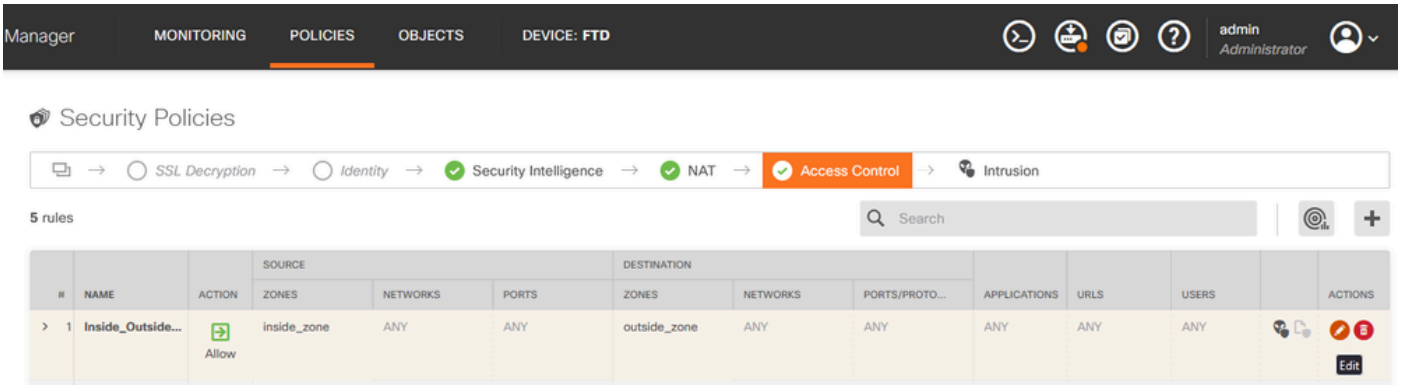
FDM-tabblad Beleid

2. Ga onder Beveiligingsbeleid naar het gedeelte Toegangsbeheer.



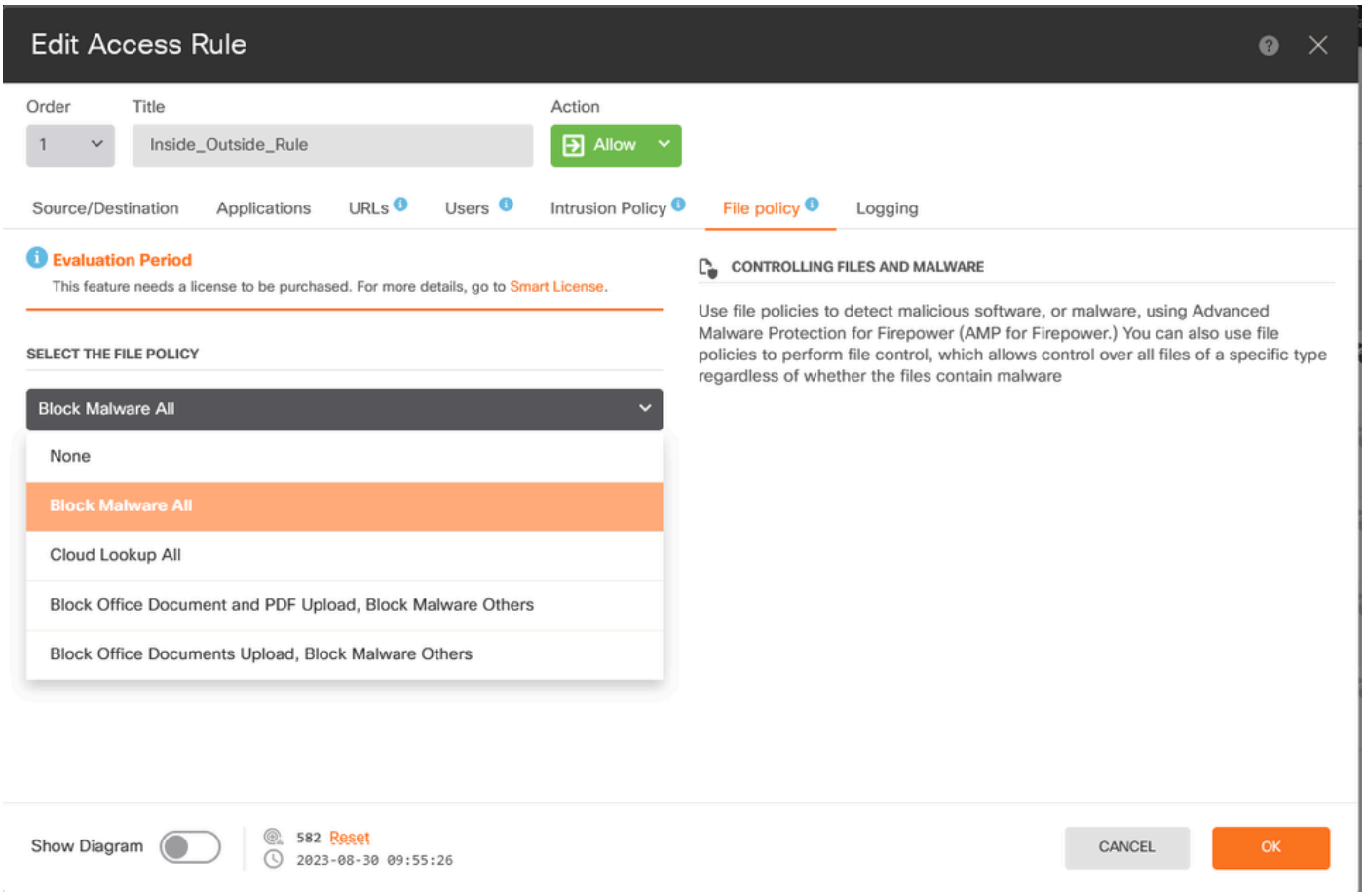
FDM-tabblad Toegangsbeheer

3. Zoek of creëer een toegangsregel om het bestandsbeleid te configureren. Klik op de editor Toegangsregels. Zie deze link voor instructies over het maken van een toegangsregel.



FDM-toegangscontroleregel

4. Klik op het gedeelte Bestandsbeleid in de toegangsregel en selecteer de gewenste optie Bestandsbeleid in de vervolgkeuzelijst. Klik op OK om de wijzigingen in de regel op te slaan.

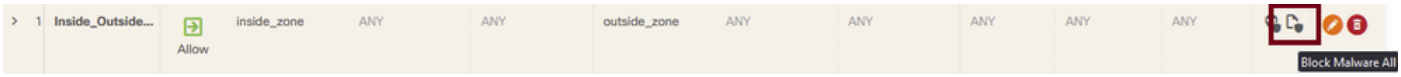


Tabblad FDM-toegangscontrolelijn voor bestandsbeleid

5. Controleer of het bestandsbeleid op de toegangsregel is toegepast door te controleren of het pictogram Bestandsbeleid is ingeschakeld.

Pictogram

voor



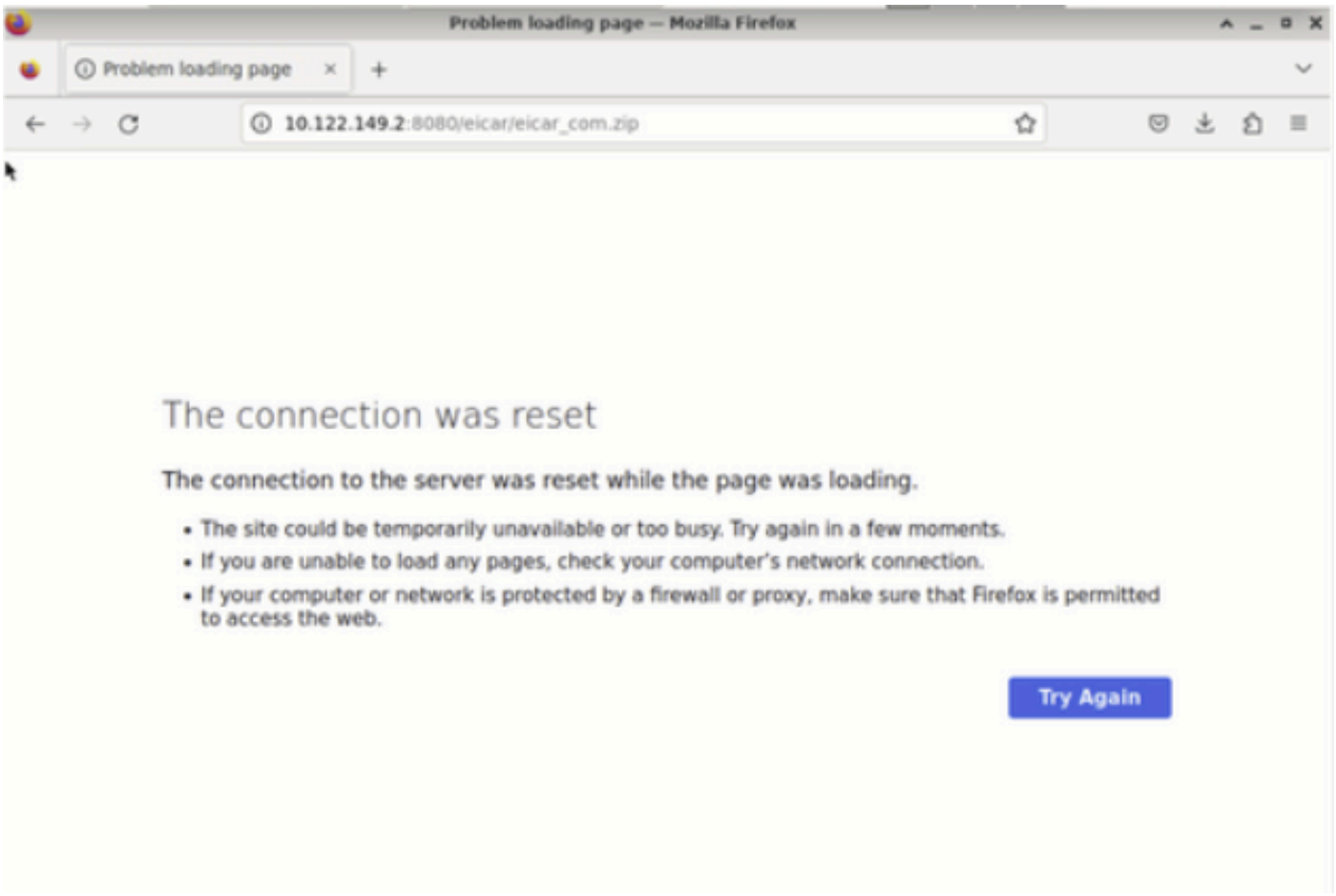
bestandsbeleid ingeschakeld

6. Opslaan en implementeren van de wijzigingen in het beheerde apparaat.

Testen

Om te controleren of het geconfigureerd beleid voor malware bescherming werkt, gebruik deze testscenario pogingen om een malware testbestand te downloaden van de webbrowser van een end-host.

Zoals weergegeven in deze screenshot, is het downloaden van een malware testbestand van de webbrowser niet geslaagd.



Browser Download test

Vanuit de FTD CLI laat het spoor voor systeemondersteuning zien dat het downloaden van bestanden is geblokkeerd door het bestandsproces. Zie deze link voor instructies hoe u een spoor voor systeemondersteuning kunt uitvoeren via de FTD CLI.

```
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 File signature verdict Reject and flags 0x00005A00 for 2546d
cffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad of instance 0
192.168.0.10-40016 > 10.122.149.2-8080 6 File Process: drop /eicar/eicar_com.zip
192.168.0.10-40016 > 10.122.149.2-8080 6 IPS Event: gid 147, sid 1, drop
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 File malware event for 2546dcffc5ad854d4ddc64fbf056871cd5a00
f2471cb7a5bfd4ac23b6e9eedad named eicar_com.zip with disposition Malware and action Block Malware
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 Archive childs been processed No
192.168.0.10-40016 > 10.122.149.2-8080 6 Snort detect_drop: gid 147, sid 1, drop
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 deleting firewall session
192.168.0.10-40016 > 10.122.149.2-8080 6 Snort id 0, NAP id 2, IPS id 0, Verdict BLACKLIST
192.168.0.10-40016 > 10.122.149.2-8080 6 ===> Blocked by File Process
Verdict reason is sent to DAQ
```

Tracetest voor systeemondersteuning

Dit bevestigt dat de bestandsbeleidsconfiguratie succesvol was in het blokkeren van malware.

Probleemoplossing

In het geval dat malware niet met succes wordt geblokkeerd bij het gebruik van de vorige configuraties, raadpleeg deze suggesties voor probleemoplossing:

1. Controleer of de malware-licentie niet is verlopen.

2. Bevestig dat de toegangscontroleregel op correct verkeer is gericht.

3. Bevestig dat de geselecteerde optie van het bestandsbeleid correct is voor gericht verkeer en gewild malware bescherming.

Als de kwestie nog steeds niet kan worden opgelost, neemt u contact op met Cisco TAC voor extra ondersteuning.

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.