Configuration et test de la politique de fichiers AMP via FDM

Table des matières

Introduction

Ce document décrit comment configurer et tester une politique de fichiers AMP (Advanced Malware Protection) via Firepower Device Manager (FDM).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestionnaire de périphériques Firepower (FDM)
- Firepower Threat Defense (FTD)

Composants utilisés

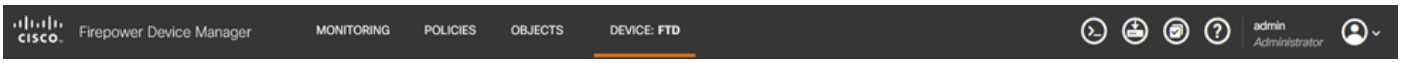
- Cisco Virtual FTD version 7.0 géré via FDM
- Licence d'évaluation (la licence d'évaluation est utilisée à des fins de démonstration. Cisco recommande d'acquérir et d'utiliser une licence valide)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Instructions

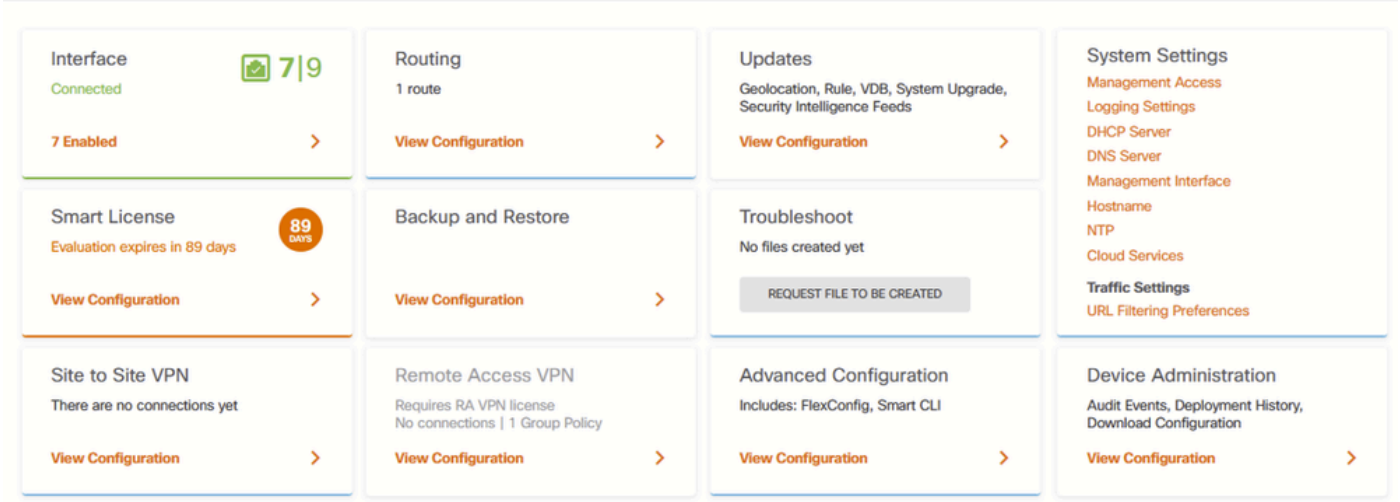
Licences

1. Afin d'activer la licence de programme malveillant, naviguez vers la page DEVICE sur l'interface utilisateur graphique de FDM.



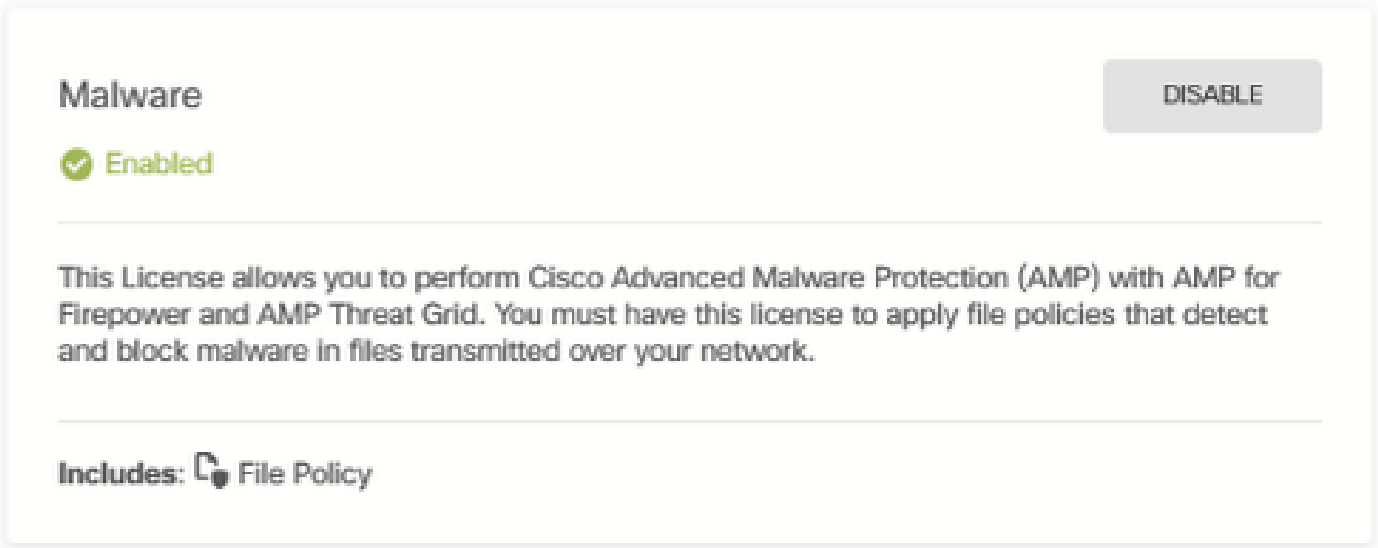
Onglet Périphérique FDM

2. Localisez la zone intitulée Smart License et cliquez sur View Configuration.



Page Périphérique FDM

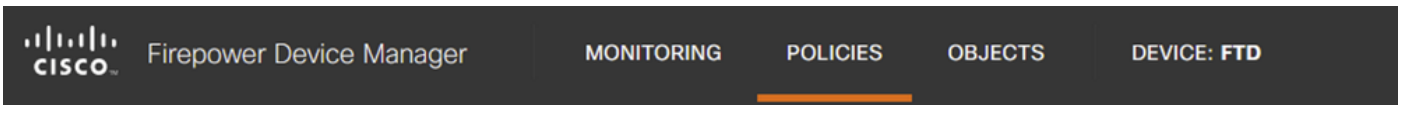
3. Activez la licence étiquetée Malware.



Licence de programme malveillant

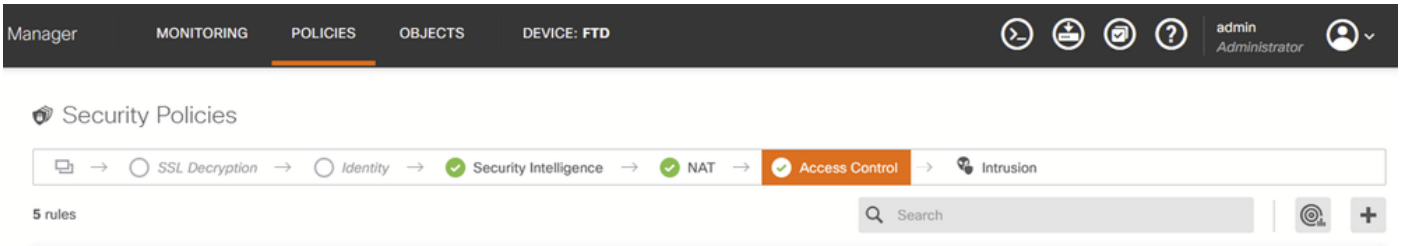
Configuration

1. Accédez à la page POLICIES sur FDM.



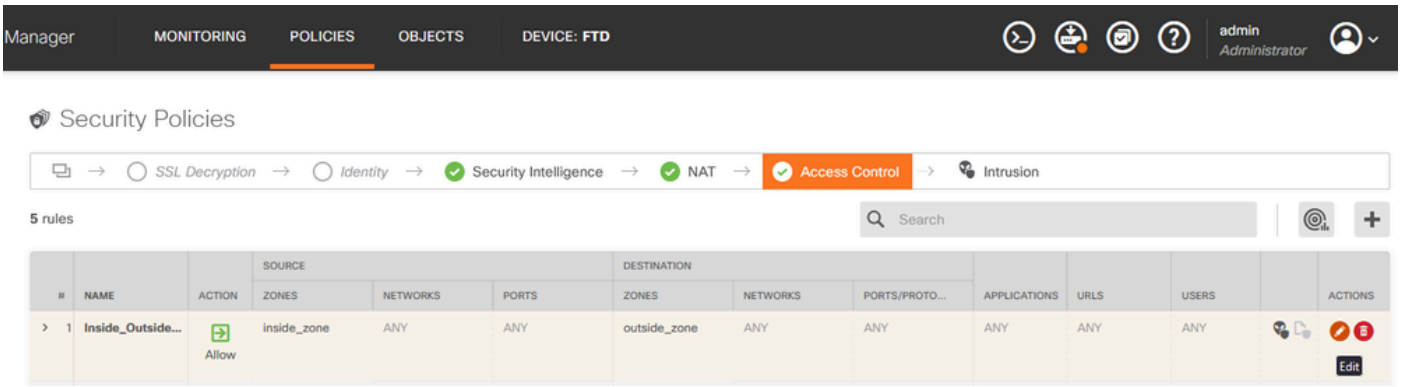
Onglet Politiques FDM

2. Sous Security Policies, accédez à la section Access Control.



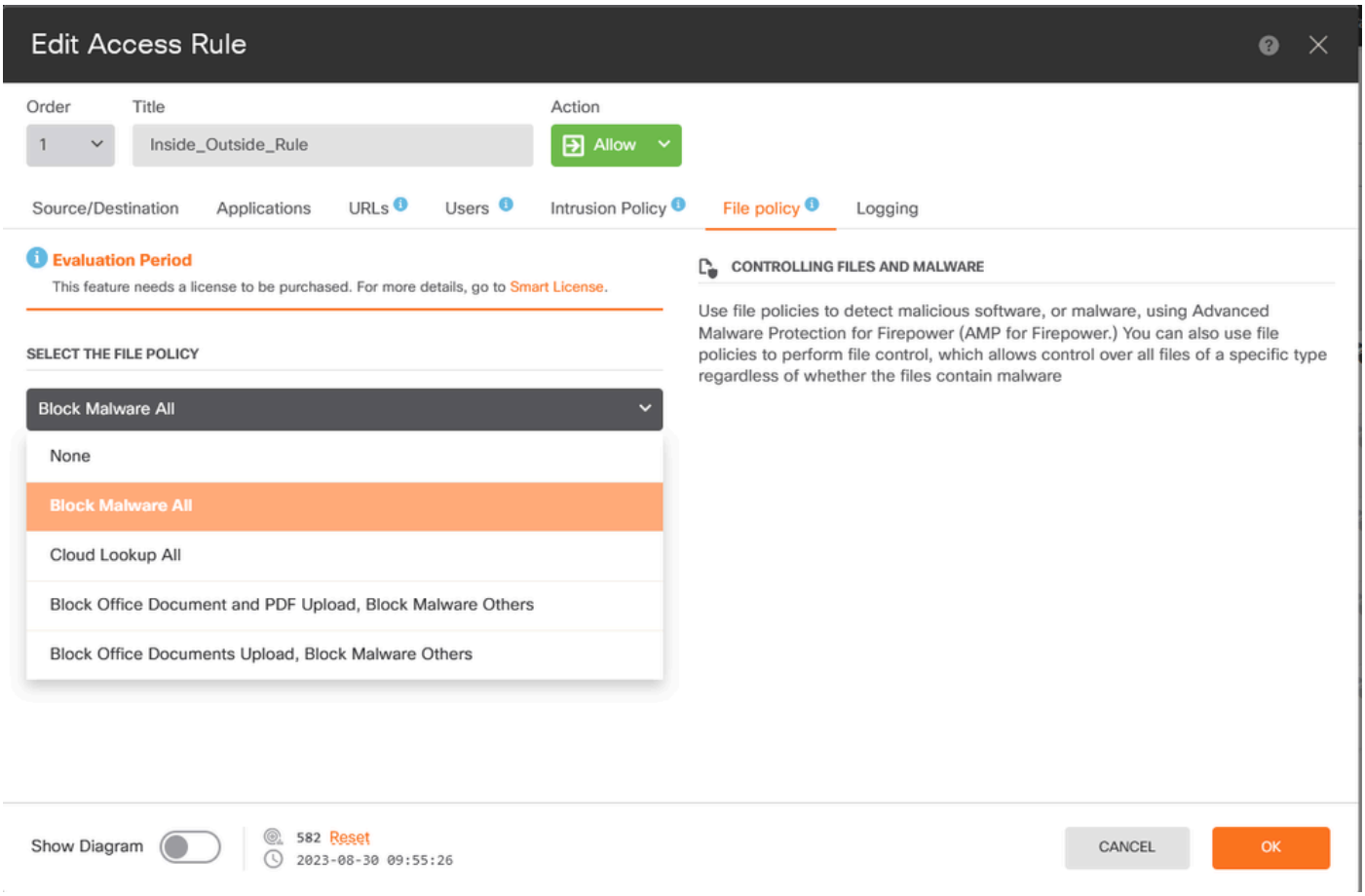
Onglet Contrôle d'accès FDM

3. Recherchez ou créez une règle d'accès pour configurer la stratégie de fichier. Cliquez sur l'éditeur Access Rule. Pour obtenir des instructions sur la création d'une règle d'accès, reportez-vous au lien this.



Règle de contrôle d'accès FDM

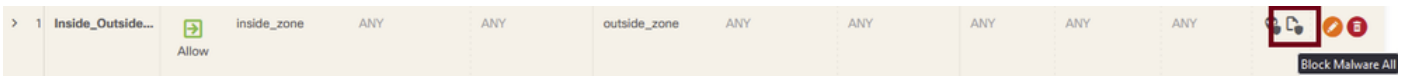
4. Cliquez sur la section File Policy sur la règle d'accès et sélectionnez l'option préférée de File Policy dans la liste déroulante. Cliquez sur OK pour enregistrer les modifications apportées à la règle.



Onglet Politique de fichier de règle de contrôle d'accès FDM

5. Vérifiez que la stratégie de fichiers a été appliquée à la règle d'accès en vérifiant si l'icône Stratégie de fichiers est activée.

Icône de



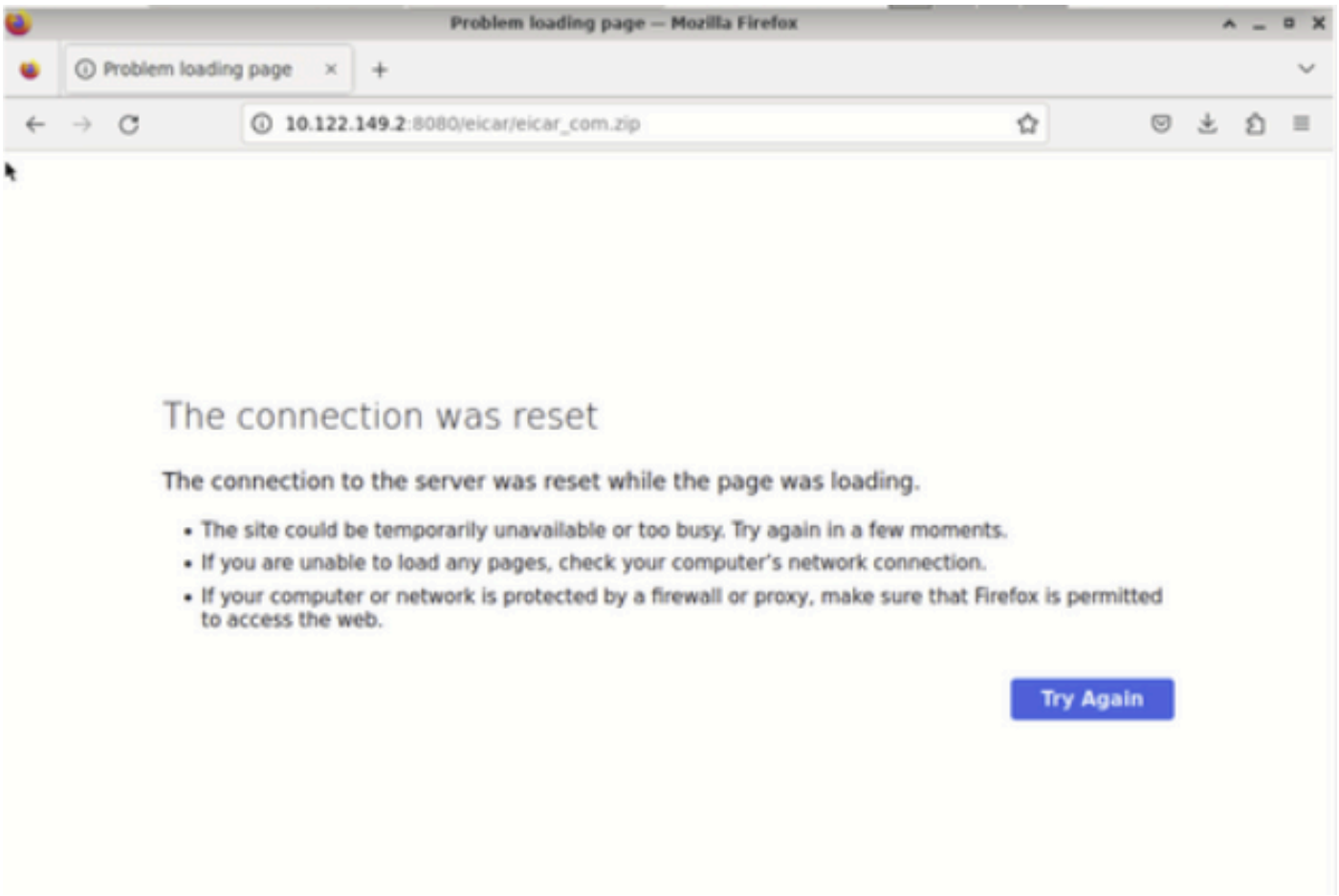
stratégie de fichiers activée

6. Enregistrez et déployez les modifications sur le périphérique géré.

Essai

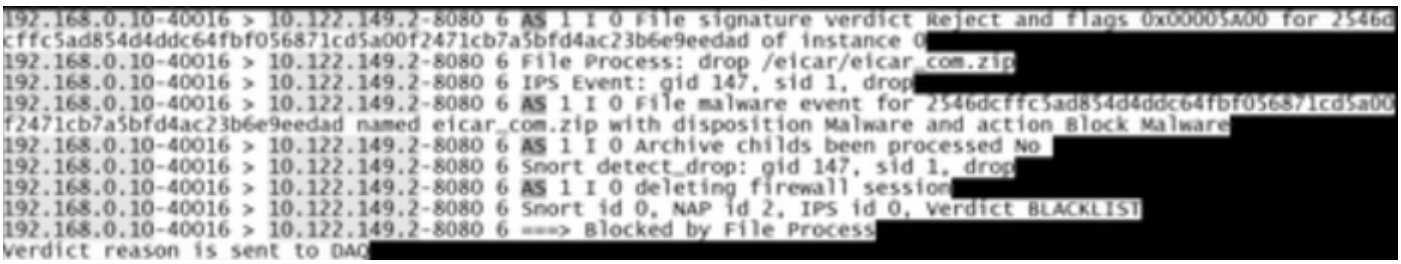
Pour vérifier que la stratégie de fichier configurée pour la protection contre les programmes malveillants fonctionne, utilisez ces scénarios de test pour tenter de télécharger un fichier de test de programme malveillant à partir du navigateur Web d'un hôte final.

Comme indiqué dans cette capture d'écran, la tentative de téléchargement d'un fichier de test de programme malveillant à partir du navigateur Web a échoué.



Test de téléchargement du navigateur

À partir de l'interface de ligne de commande FTD, le suivi du support système indique que le téléchargement du fichier a été bloqué par le processus de fichier. Pour obtenir des instructions sur l'exécution d'un suivi de support système via l'interface de ligne de commande FTD, reportez-vous à ce lien.



Test de suivi de support système

Cela confirme que la configuration de la stratégie de fichier a réussi à bloquer les programmes malveillants.

Dépannage

Si les programmes malveillants ne sont pas correctement bloqués lors de l'utilisation des configurations précédentes, reportez-vous aux suggestions de dépannage suivantes :

1. Vérifiez que la licence du programme malveillant n'a pas expiré.

2. Vérifiez que la règle de contrôle d'accès cible le trafic correct.

3. Vérifiez que l'option de stratégie de fichier sélectionnée est correcte pour le trafic ciblé et la protection contre les programmes malveillants.

Si le problème n'est toujours pas résolu, contactez le TAC Cisco pour obtenir une assistance supplémentaire.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.