Konfigurieren und Testen der AMP-Dateirichtlinie über FDM

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie eine AMP-Dateirichtlinie (Advanced Malware Protection) über den FirePOWER Device Manager (FDM) konfigurieren und testen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- FirePOWER-Gerätemanager (FDM)
- Firepower Threat Defense (FTD)

Verwendete Komponenten

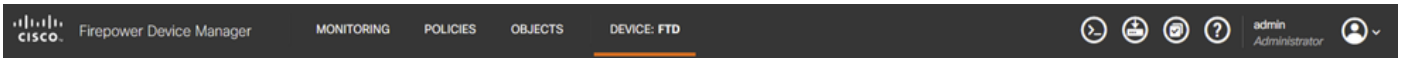
- Virtuelle Cisco FTD Version 7.0, verwaltet über FDM
- Evaluation-Lizenz (Evaluation-Lizenz wird zu Demonstrationszwecken verwendet. Cisco empfiehlt den Erwerb und die Nutzung einer gültigen Lizenz.)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Anweisungen

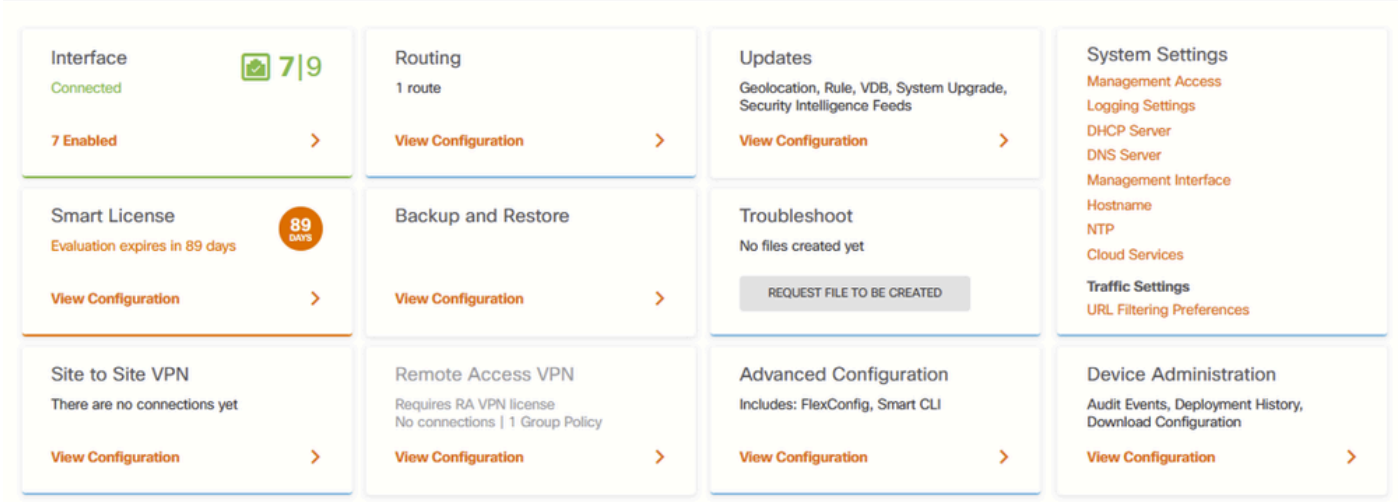
Lizenzierung

1. Um die Malware-Lizenz zu aktivieren, navigieren Sie auf der GERÄTE-Seite der FDM-GUI zur entsprechenden Seite.



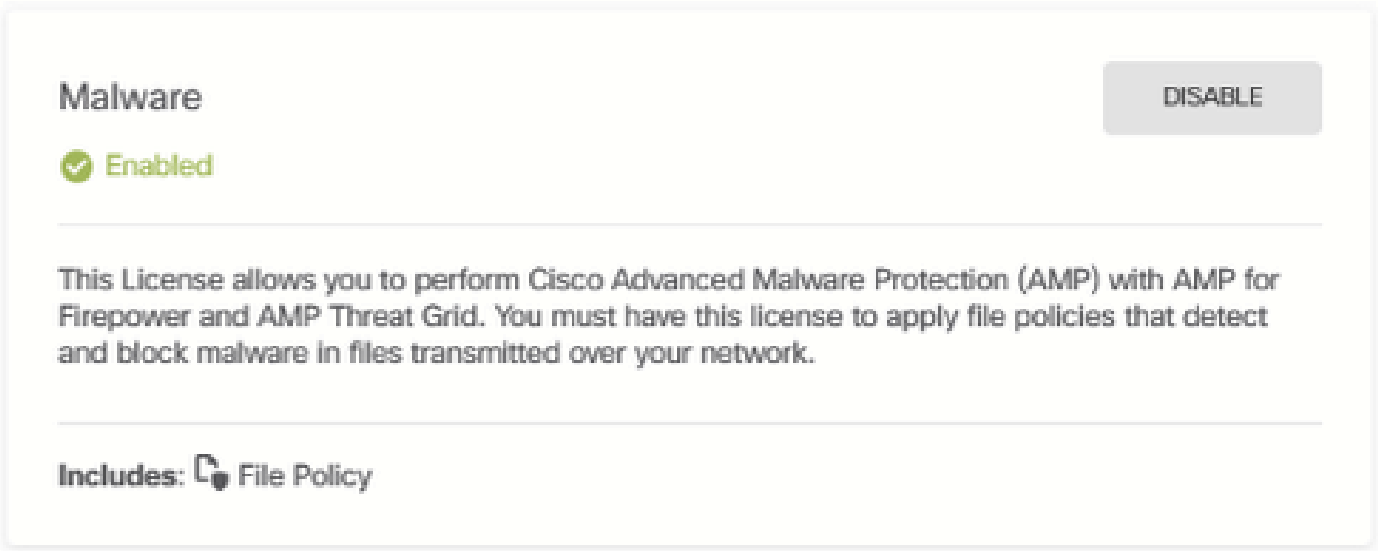
Registerkarte "FDM Device"

2. Suchen Sie das Feld mit der Bezeichnung Smart License, und klicken Sie auf Konfiguration anzeigen.



Seite für FDM-Geräte

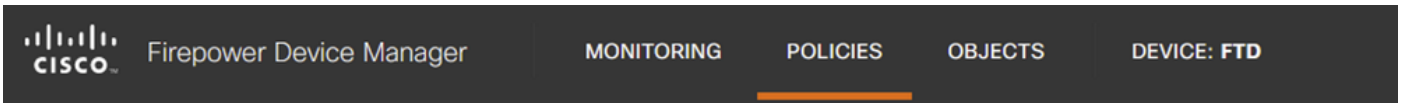
3. Aktivieren Sie die Lizenz mit der Bezeichnung Malware.



Malware-Lizenz

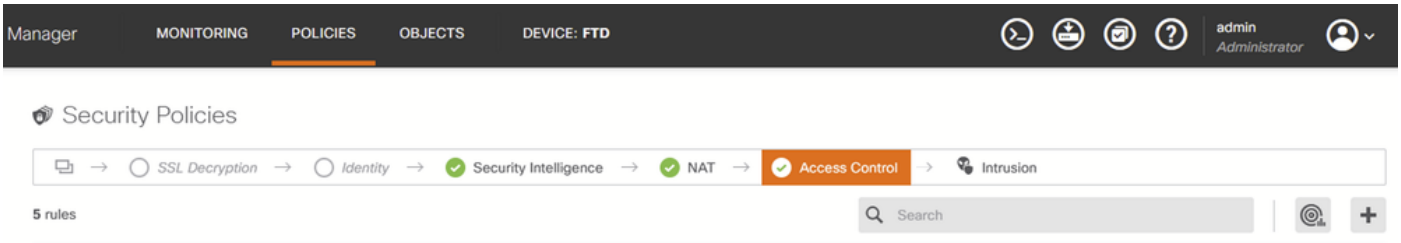
Konfiguration

1. Navigieren Sie zur Seite POLICIES im FDM.



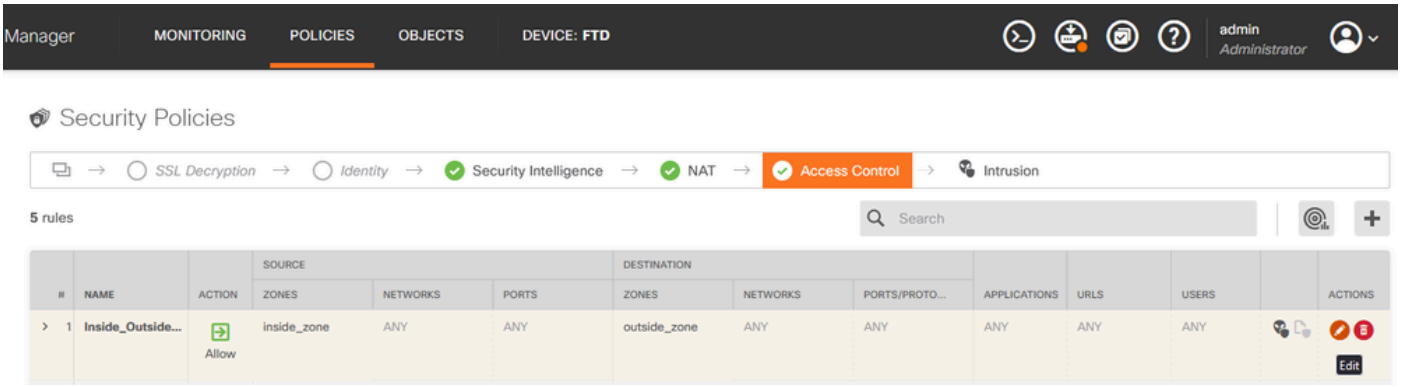
Registerkarte "FDM-Richtlinien"

2. Navigieren Sie unter Sicherheitsrichtlinien zum Abschnitt Zugriffskontrolle.



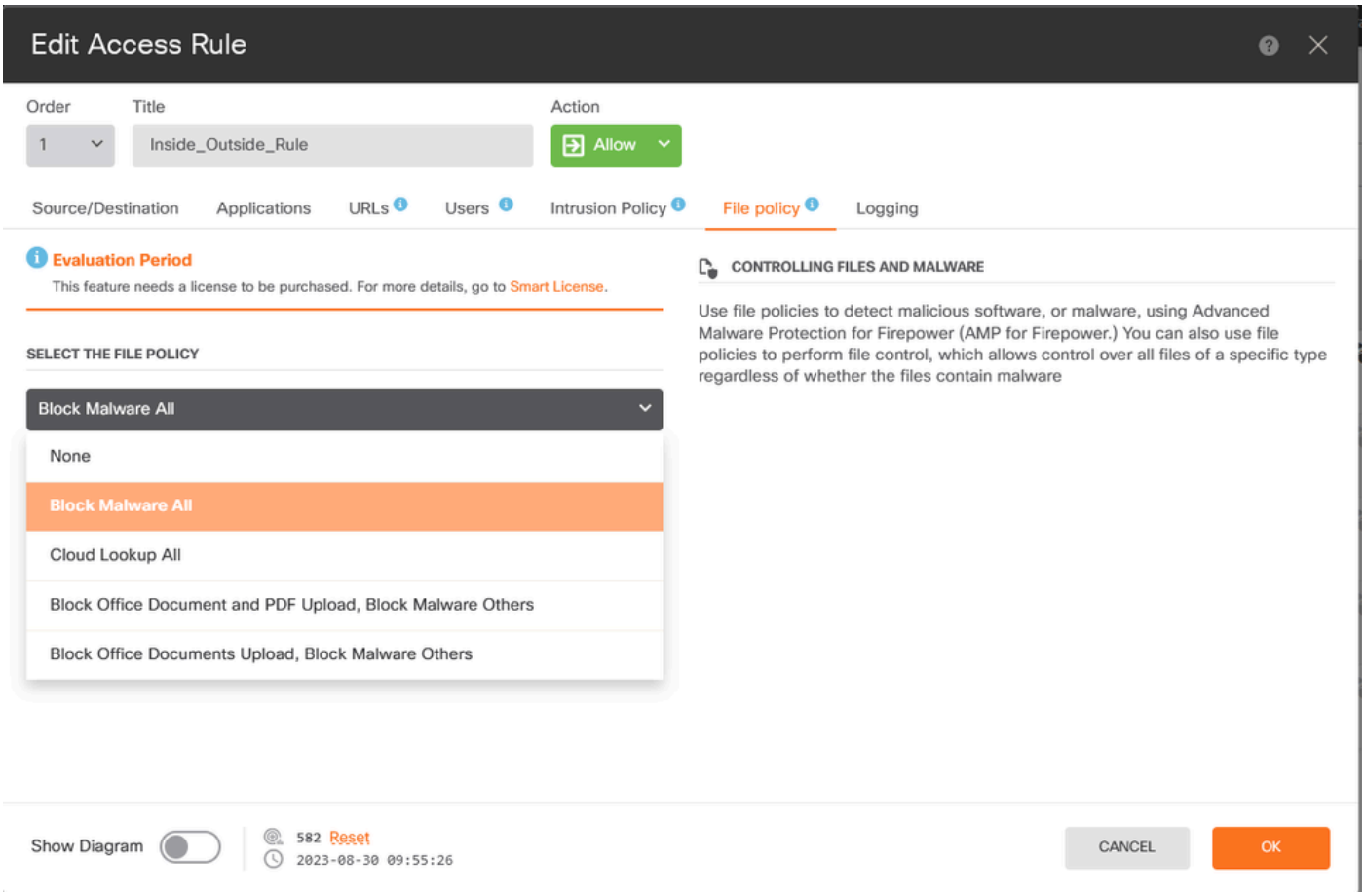
Registerkarte "FDM Access Control"

3. Suchen oder erstellen Sie eine Zugriffsregel, um die Dateirichtlinie zu konfigurieren. Klicken Sie auf den Editor für Zugriffsregeln. Anweisungen zum Erstellen einer Zugriffsregel finden Sie unter diesem Link.



FDM-Zugriffskontrollregel

4. Klicken Sie auf den Abschnitt Dateirichtlinie der Zugriffsregel und wählen Sie die bevorzugte Dateirichtlinie aus dem Dropdown-Menü aus. Klicken Sie auf OK, um die Änderungen an der Regel zu speichern.



FDM-Zugriffskontrollregel Registerkarte Dateirichtlinie

5. Vergewissern Sie sich, dass die Dateirichtlinie auf die Zugriffsregel angewendet wurde, indem Sie überprüfen, ob das Symbol Dateirichtlinie aktiviert ist.

Dateirichtlinien

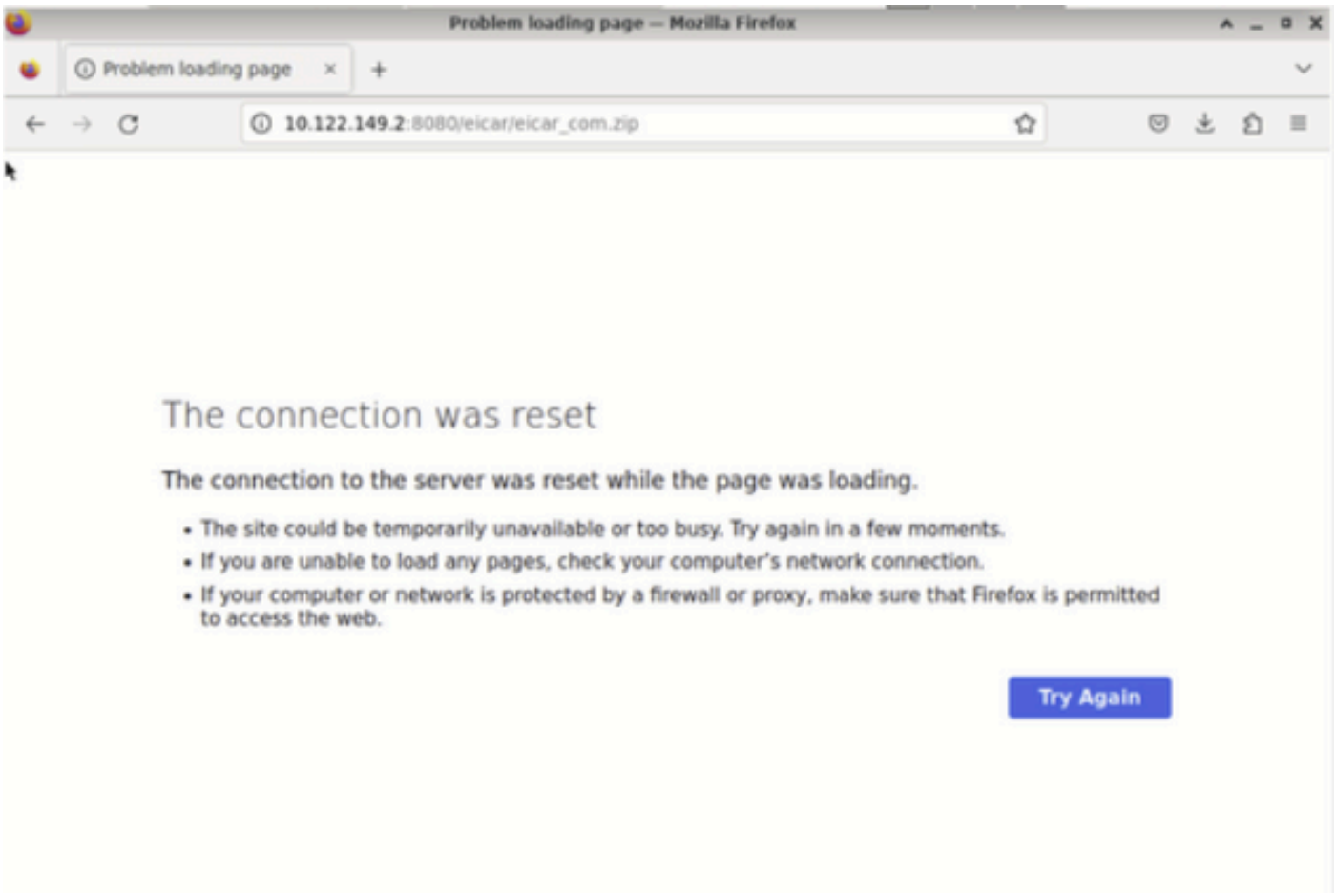
Symbol aktiviert

6. Speichern und Bereitstellen der Änderungen auf dem verwalteten Gerät

Test

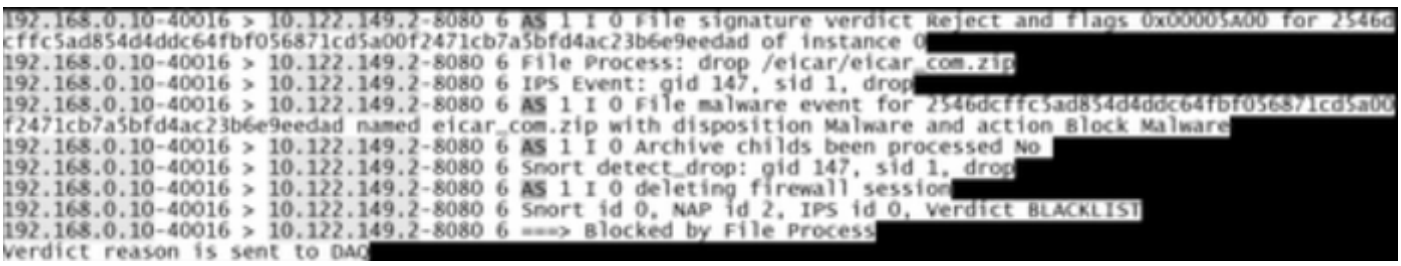
Um zu überprüfen, ob die konfigurierte Dateirichtlinie für den Malware-Schutz funktioniert, verwenden Sie diese Testszenarien, um eine Malware-Testdatei vom Webbrowser eines Endhosts herunterzuladen.

Wie in diesem Screenshot gezeigt, ist der Versuch, eine Malware-Testdatei vom Webbrowser herunterzuladen, fehlgeschlagen.



Browser-Download-Test

In der FTD-CLI zeigt die Systemsupportüberwachung an, dass der Dateidownload durch den Dateiprozess blockiert wurde. Anweisungen zum Ausführen einer Systemsupport-Ablaufverfolgung über die FTD-CLI finden Sie unter diesem Link.



Trace-Test zur Systemunterstützung

Dies bestätigt, dass die Dateirichtlinienkonfiguration Malware erfolgreich blockiert hat.

Fehlerbehebung

Falls Malware bei Verwendung der vorherigen Konfigurationen nicht erfolgreich blockiert wird, schlagen Sie folgende Fehlerbehebungsvorschläge vor:

1. Überprüfen Sie, ob die Malware-Lizenz abgelaufen ist.

2. Die Zugriffskontrollregel bestätigen betrifft den richtigen Datenverkehr.

3. Bestätigen Sie, dass die ausgewählte Dateirichtlinienoption für den Zieldatenverkehr und den Schutz vor erwünschter Malware richtig ist.

Wenn das Problem weiterhin nicht behoben werden kann, wenden Sie sich an das Cisco TAC, um zusätzlichen Support zu erhalten.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.