Configurazione e test dei criteri dei file AMP tramite FDM

Sommario

[Introduzione](#)

[Prerequisiti](#)

- [Requisiti](#)
- [Componenti usati](#)

[Istruzione](#)

- [Licenze](#)
- [Configurazione](#)
- [Test](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare e provare una policy sui file di Advanced Malware Protection (AMP) tramite Firepower Device Manager (FDM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

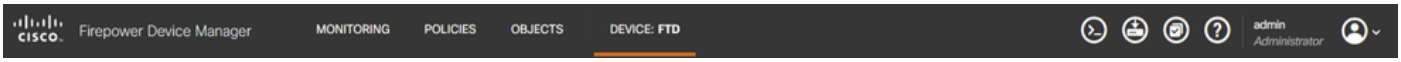
- Cisco virtual FTD versione 7.0 gestito tramite FDM
- Licenza di valutazione (la licenza di valutazione viene utilizzata a scopo dimostrativo. Si consiglia a Cisco di acquistare e utilizzare una licenza valida)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Istruzione

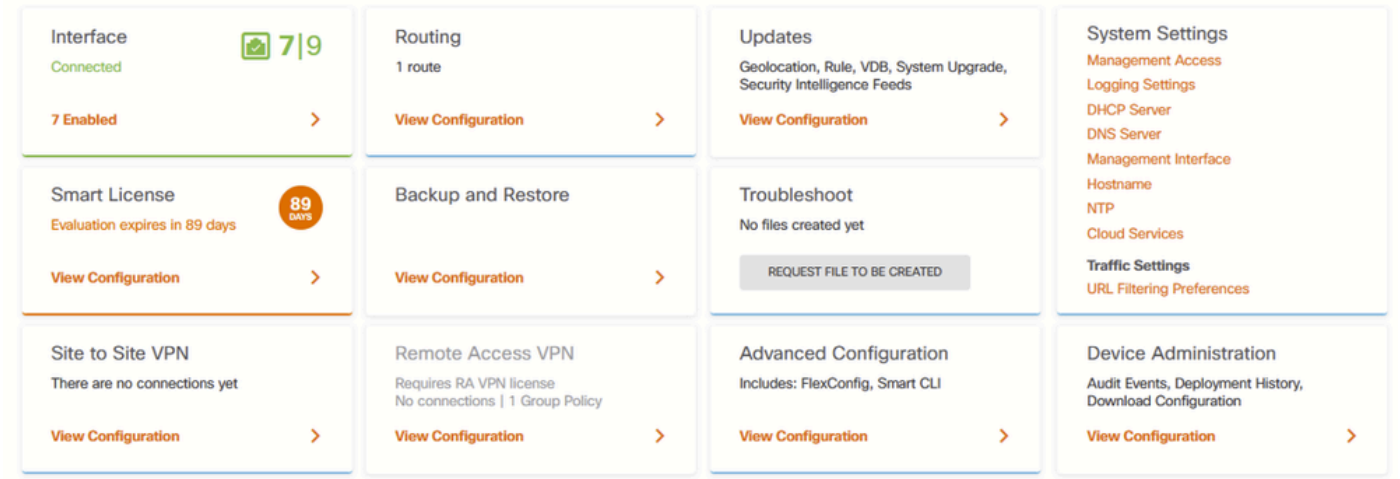
Licenze

1. Per abilitare la licenza malware, passare alla pagina DEVICE nell'interfaccia utente di FDM.



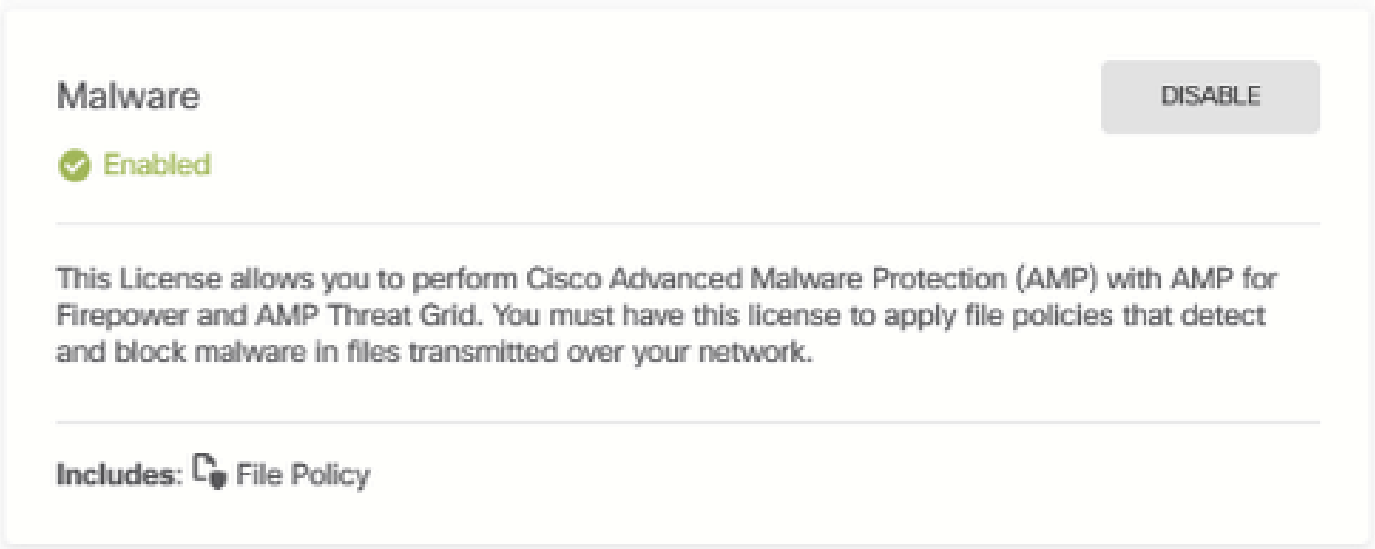
Scheda Periferica di FDM

2. Individuare la casella Smart License e fare clic su View Configuration.



Pagina Dispositivo FDM

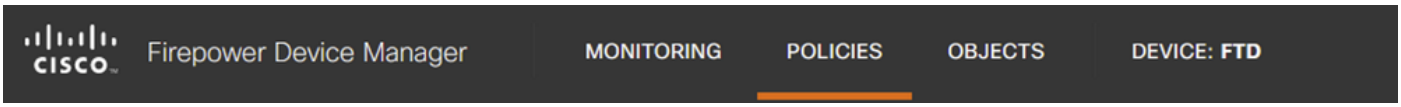
3. Abilitare la licenza Malware.



Licenza per malware

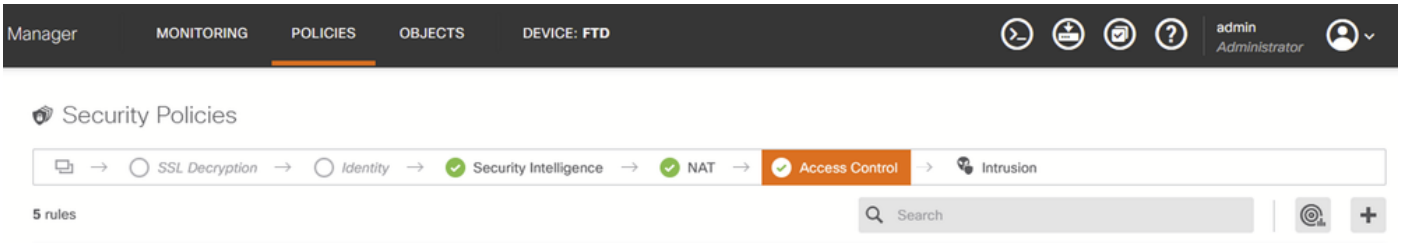
Configurazione

1. Passare alla pagina CRITERI in FDM.



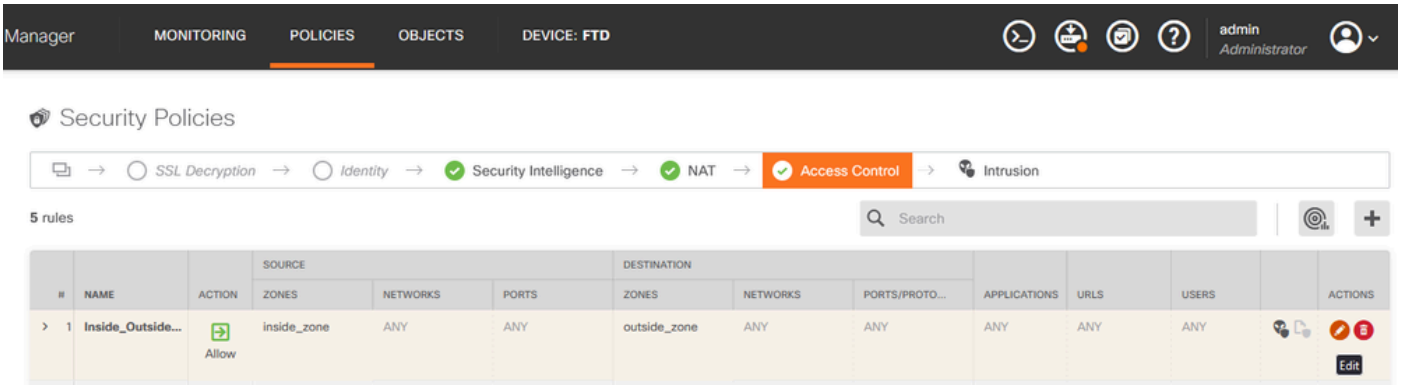
Scheda Criteri FDM

2. In Criteri di sicurezza, passare alla sezione Controllo di accesso.



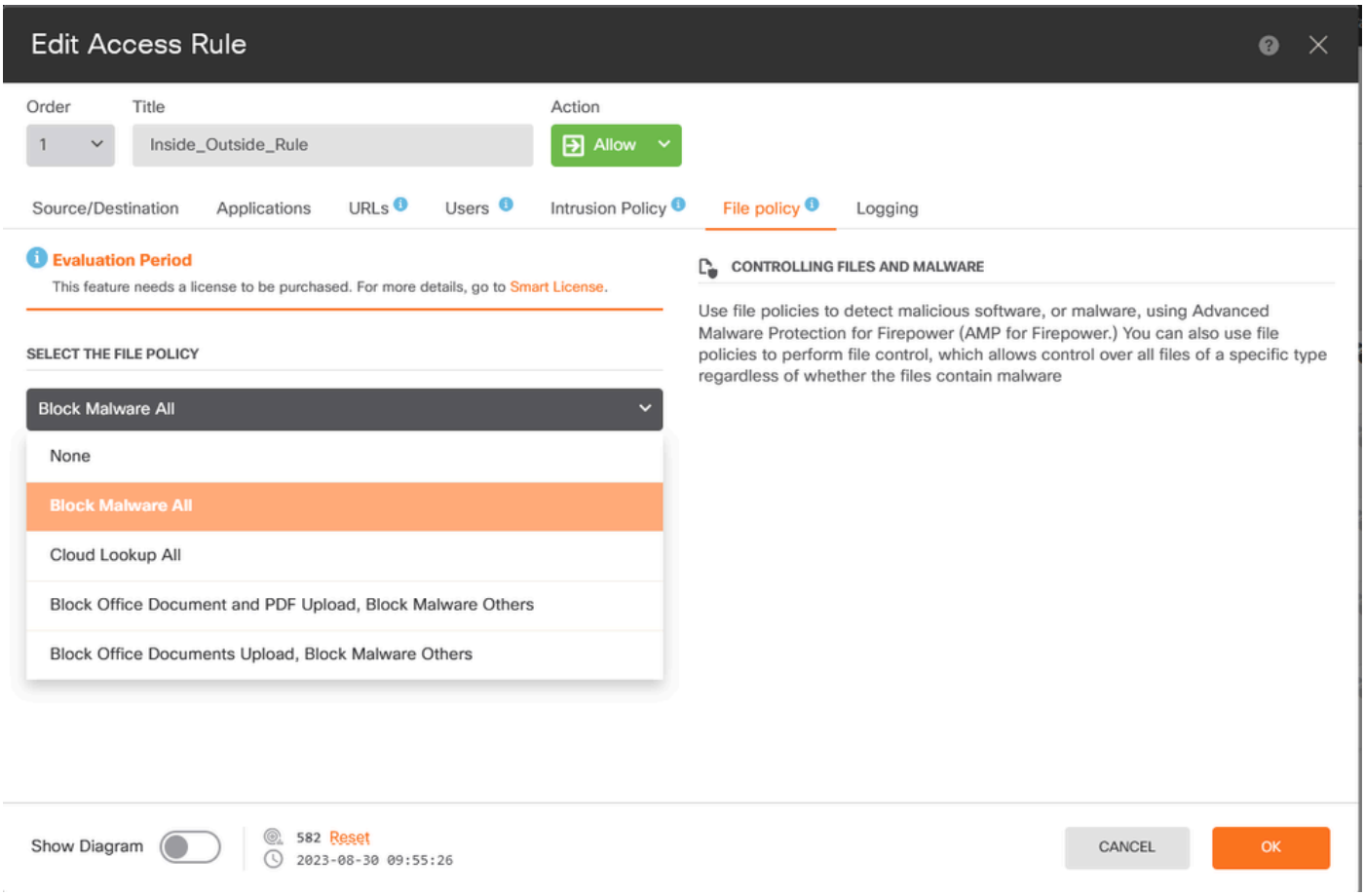
Scheda Controllo accesso di FDM

3. Individuare o creare una regola di accesso per configurare il criterio file. Fare clic sull'editor Regole di accesso. Per istruzioni su come creare una regola di accesso, fare riferimento a questo collegamento.



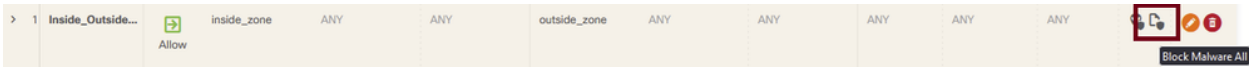
Regola di controllo di accesso FDM

4. Fare clic sulla sezione Criterio file nella regola di accesso e selezionare l'opzione Criterio file preferito dall'elenco a discesa. Fare clic su OK per salvare le modifiche apportate alla regola.



Scheda Criterio file delle regole di controllo d'accesso FDM

5. Verificare che il criterio file sia stato applicato alla regola di accesso verificando se l'icona Criterio file è attivata.



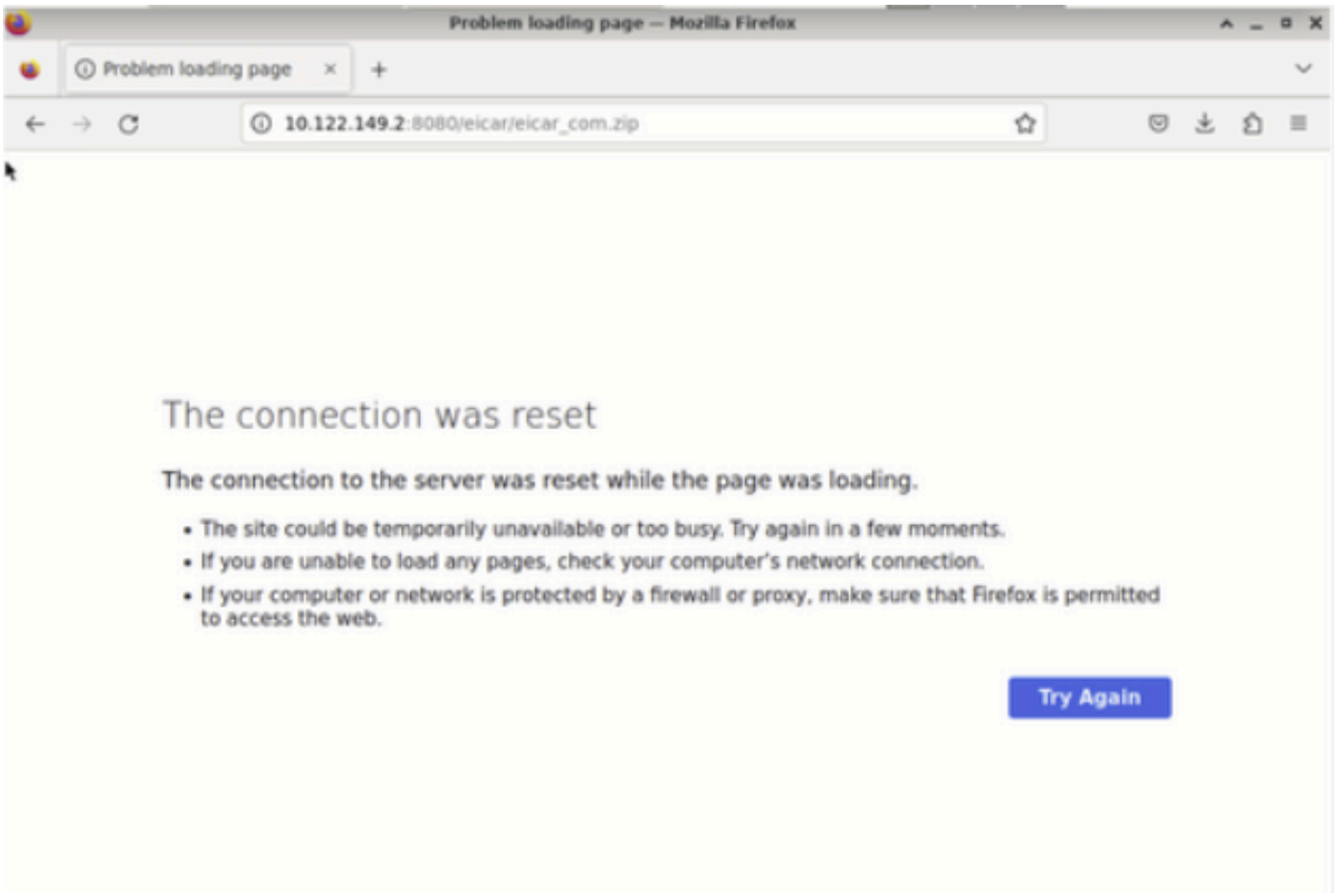
Icona Criterio file abilitata

6. Salvare e distribuire le modifiche al dispositivo gestito.

Test

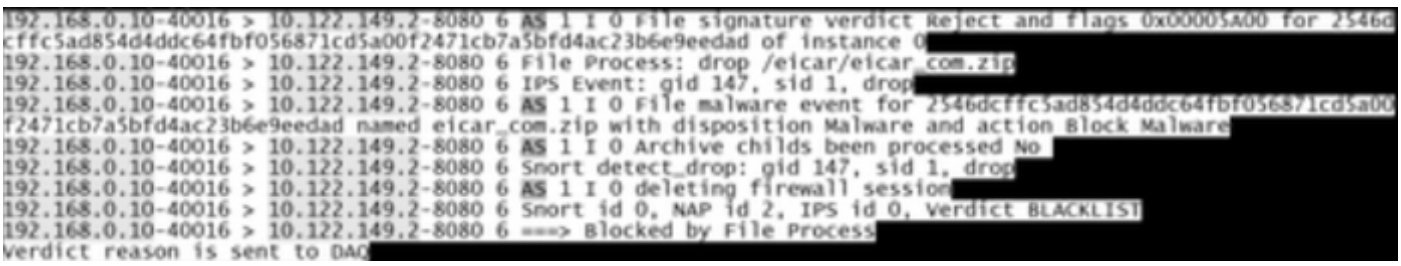
Per verificare il corretto funzionamento dei criteri file configurati per la protezione da malware, utilizzare questo scenario di test per tentare di scaricare un file di test malware dal browser Web di un host finale.

Come mostrato in questa schermata, il tentativo di scaricare un file di test malware dal Web browser non è riuscito.



Test di download browser

Dalla CLI di FTD, la traccia di supporto del sistema indica che il download del file è stato bloccato dall'elaborazione del file. Per istruzioni su come eseguire una traccia di supporto del sistema tramite la CLI FTD, fare riferimento a questo collegamento.



Test di traccia supporto di sistema

Ciò conferma che la configurazione dei criteri file è riuscita a bloccare il malware.

Risoluzione dei problemi

Se il malware non viene bloccato correttamente durante l'utilizzo delle configurazioni precedenti, fare riferimento ai seguenti suggerimenti per la risoluzione dei problemi:

1. Verificare che la licenza malware non sia scaduta.

2. Verificare che la regola di controllo di accesso sia destinata al traffico corretto.

3. Conferma che l'opzione criterio file selezionata è corretta per il traffico di destinazione e la protezione da malware desiderata.

Se il problema persiste, contattare Cisco TAC per ulteriore supporto.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).