Configurar e testar a política de arquivos do AMP via FDM

Contents

Introdução

Este documento descreve como configurar e testar uma política de arquivo de proteção avançada contra malware (AMP) através do Firepower Device Manager (FDM).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

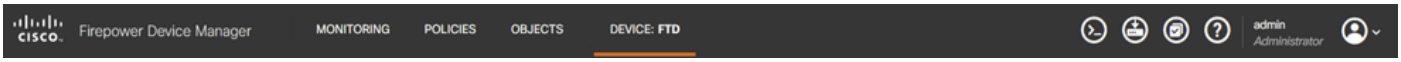
- FTD virtual Cisco versão 7.0 gerenciado via FDM
- Licença de avaliação (A licença de avaliação é usada para fins de demonstração. A recomendação da Cisco é adquirir e utilizar uma licença válida)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Instruções

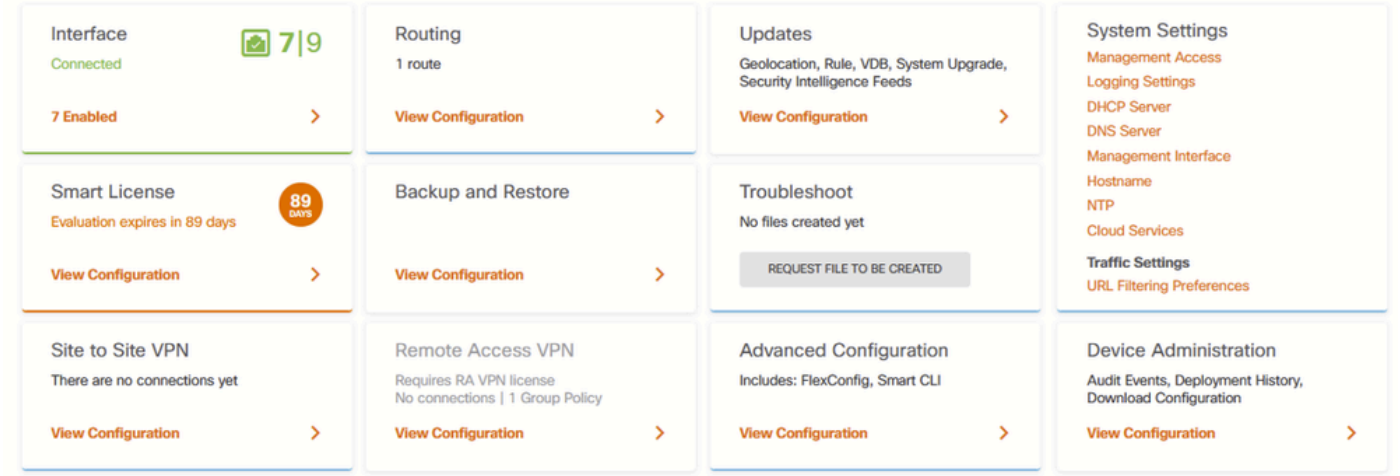
Licenciamento

1. Para habilitar a licença de malware, navegue até a página DEVICE na GUI do FDM.



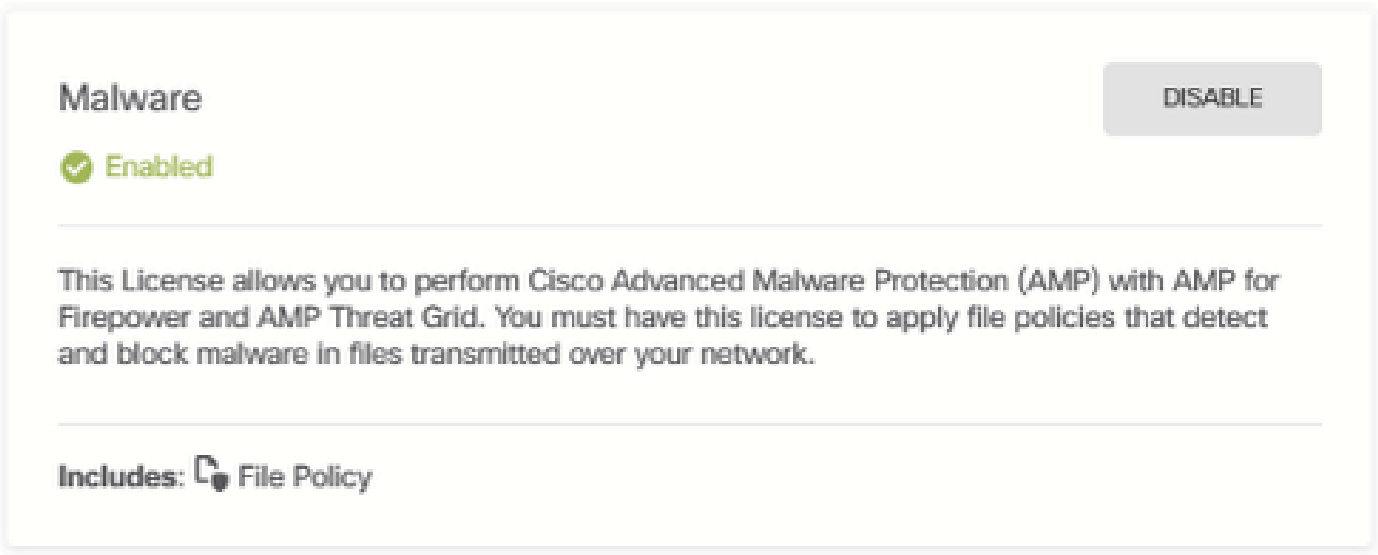
Guia Dispositivo do FDM

2. Localize a caixa denominada Smart License e clique em View Configuration.



Página Dispositivo FDM

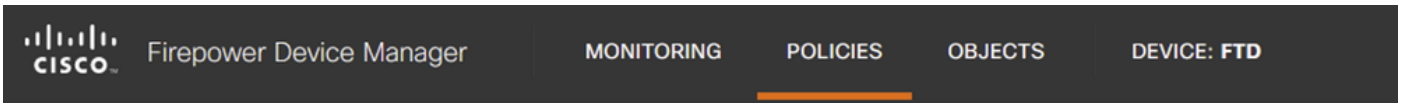
3. Ative a licença rotulada Malware.



Licença de malware

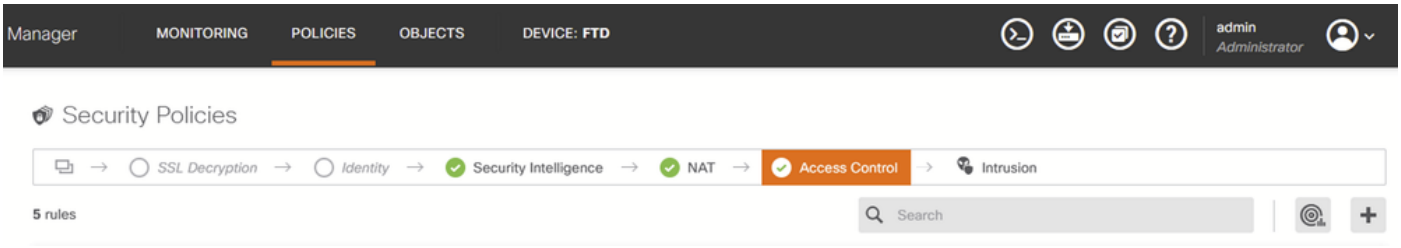
Configuração

1. Navegue até a página POLÍTICAS no FDM.



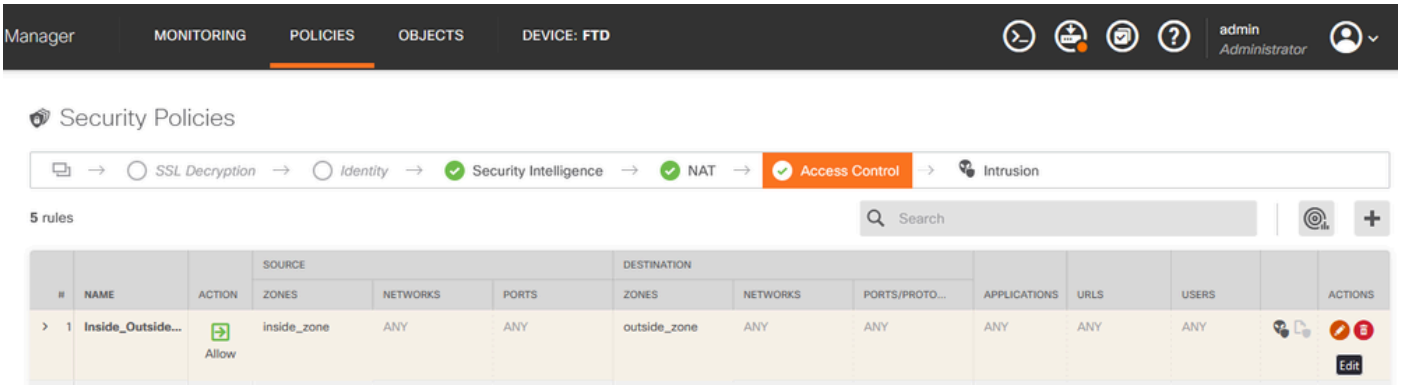
Guia Políticas do FDM

2. Em Security Policies, navegue até a seção Access Control.



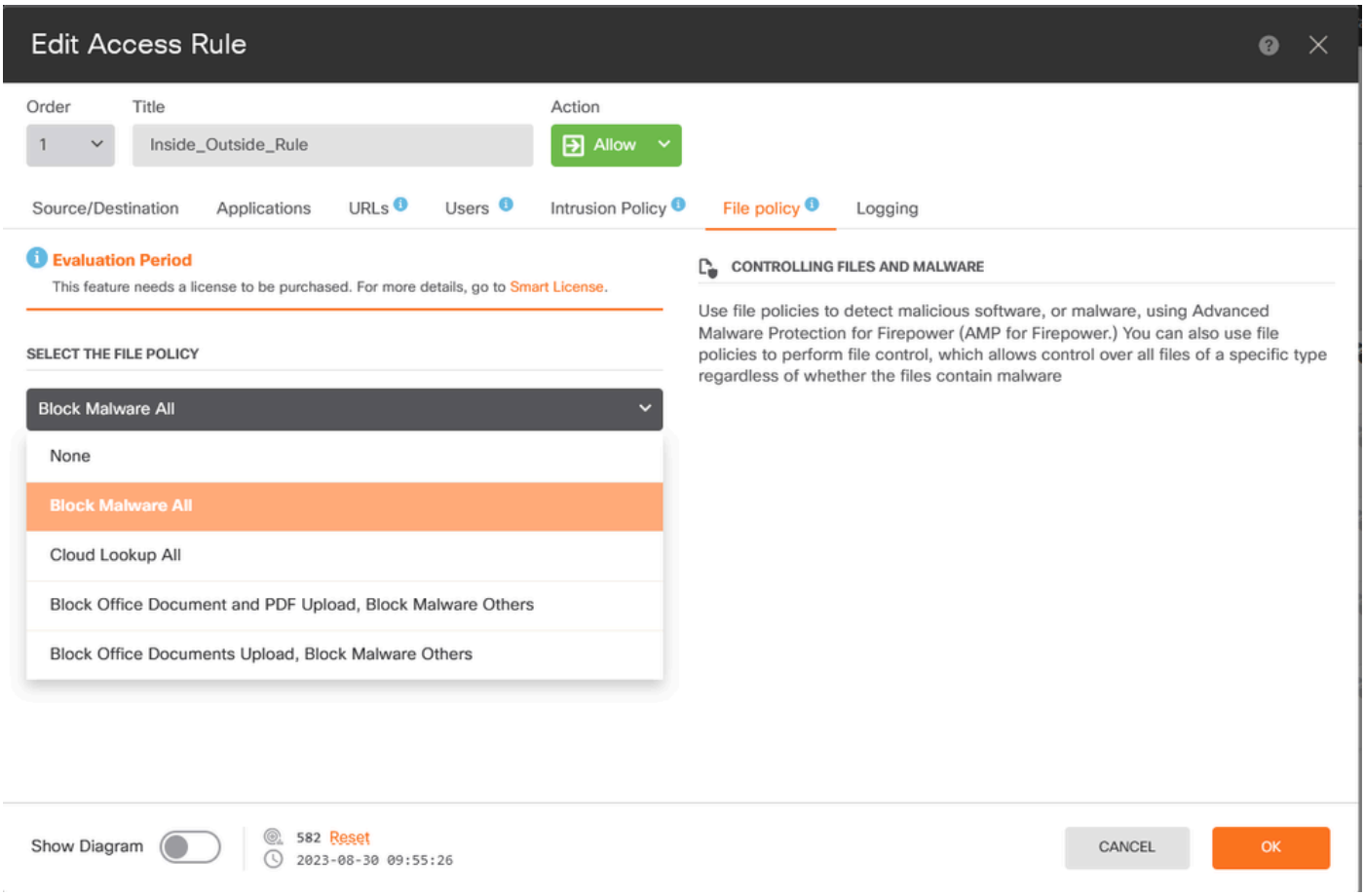
Guia Controle de Acesso do FDM

3. Localize ou crie uma Regra de Acesso para configurar a Política de Arquivo. Clique no editor Access Rule. Para obter instruções sobre como criar uma Regra de Acesso, consulte este link.



Regra de Controle de Acesso do FDM

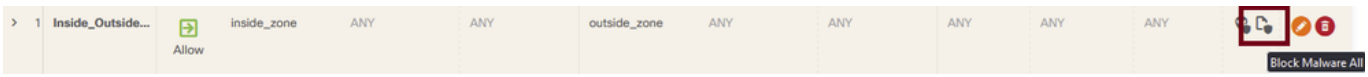
4. Clique na seção File Policy na Access Rule e selecione a opção File Policy preferida no menu suspenso. Clique em OK para salvar as alterações feitas na regra.



Guia Política de Arquivo de Regra de Controle de Acesso do FDM

5. Confirme se a Diretiva de Arquivo foi aplicada à Regra de Acesso verificando se o ícone Diretiva de Arquivo está ativado.

Ícone de Diretiva



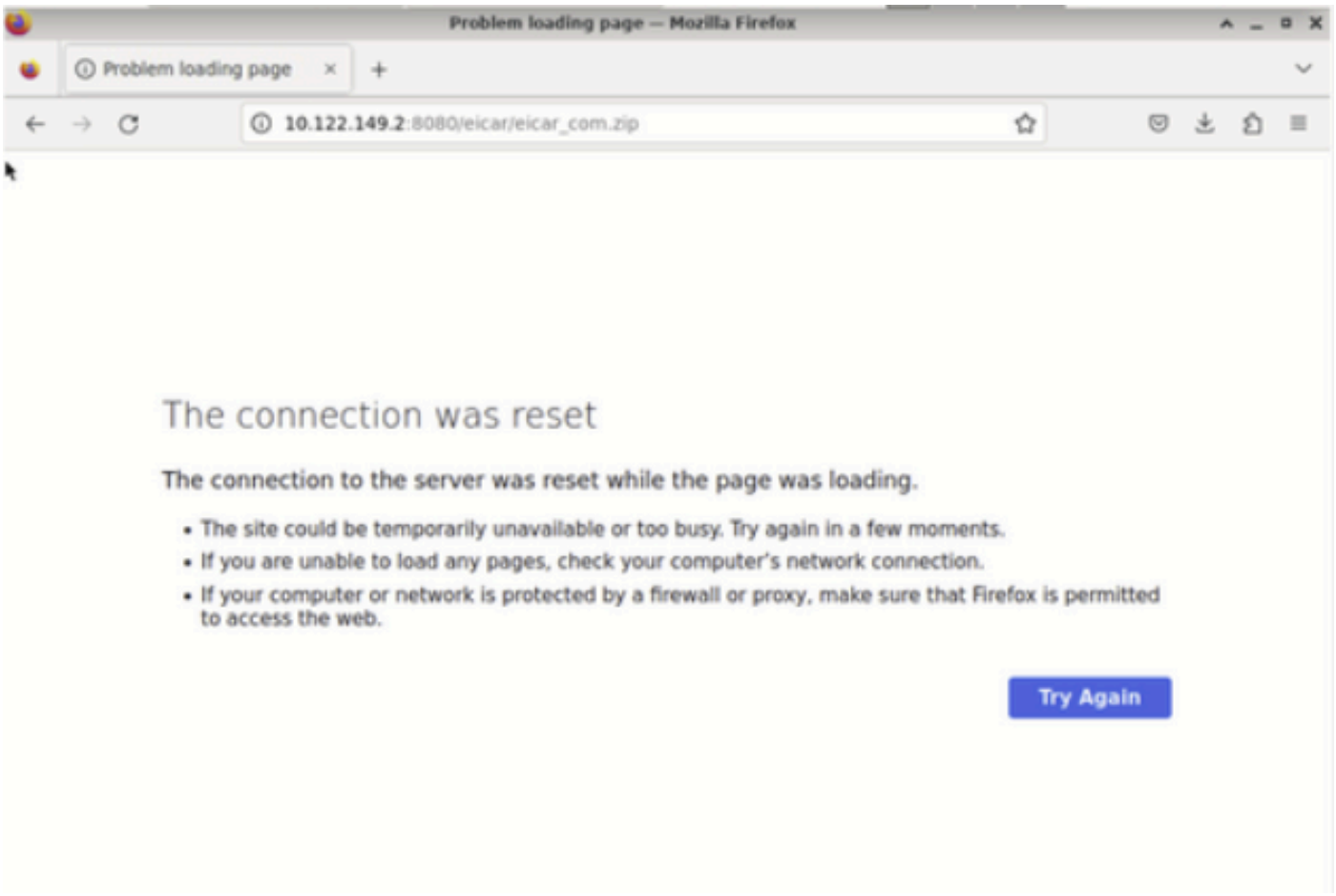
de Arquivo Habilitado

6. Salve e implante as alterações no dispositivo gerenciado.

Teste

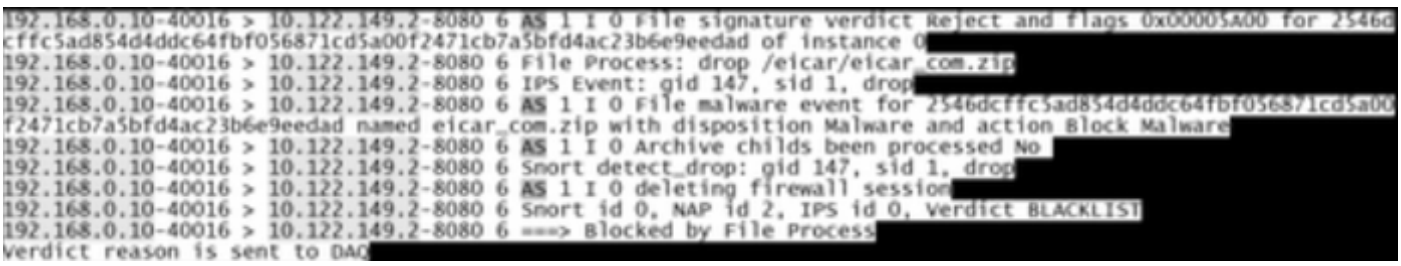
Para verificar se a política de arquivo configurada para proteção contra malware está funcionando, use este cenário de teste para fazer download de um arquivo de teste de malware do navegador da Web de um host final.

Como mostrado nesta captura de tela, a tentativa de baixar um arquivo de teste de malware do navegador da Web não foi bem-sucedida.



Teste de Download do Navegador

Na CLI do FTD, o rastreamento de suporte do sistema mostra que o download do arquivo foi bloqueado pelo processo de arquivo. Para obter instruções sobre como executar um rastreamento de suporte do sistema por meio da CLI do FTD, consulte este link.



Teste de Rastreamento de Suporte do Sistema

Isso confirma que a configuração da política de arquivo teve êxito no bloqueio de malware.

Troubleshooting

Caso o malware não seja bloqueado com êxito ao usar as configurações anteriores, consulte estas sugestões de solução de problemas:

1. Verifique se a licença do malware não expirou.

2. Confirme se a regra de controle de acesso está visando o tráfego correto.

3. Confirme se a opção de política de arquivo selecionada está correta para o tráfego direcionado e a proteção contra malware desejada.

Se o problema ainda não puder ser resolvido, entre em contato com o TAC da Cisco para obter suporte adicional.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.