

Configurar e testar a política de arquivos do AMP via FDM

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Instruções](#)

[Licenciamento](#)

[Configuração](#)

[Teste](#)

[Troubleshooting](#)

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

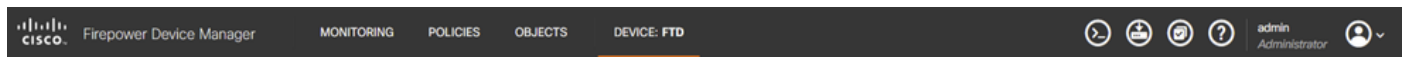
- FTD virtual Cisco versão 7.0 gerenciado via FDM
- Licença de avaliação (A licença de avaliação é usada para fins de demonstração. A recomendação da Cisco é adquirir e utilizar uma licença válida)

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

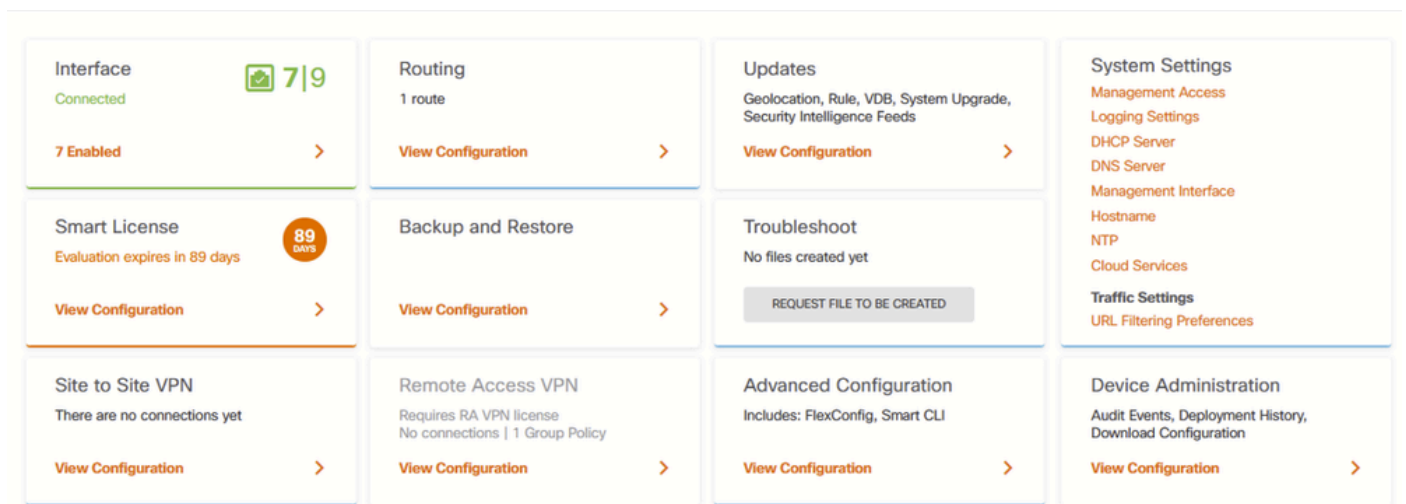
Licenciamento

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



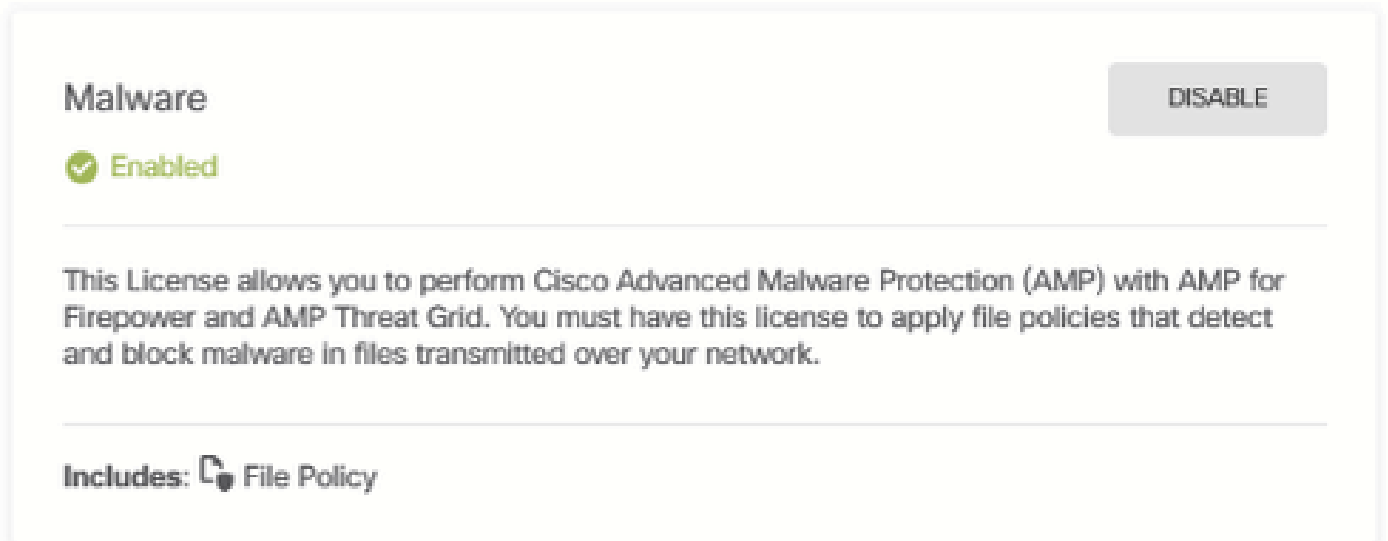
Guia Dispositivo do FDM

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



Página Dispositivo FDM

3. Ative a licença rotulada Malware.



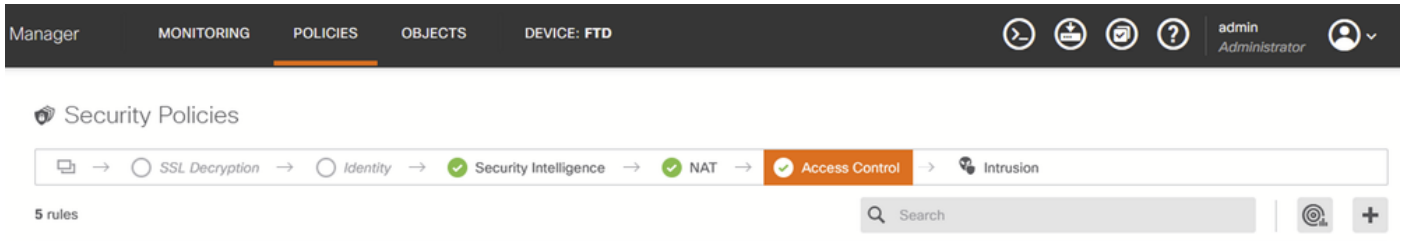
Licença de malware

Configuração

1. Navegue até a página POLÍTICAS no FDM.

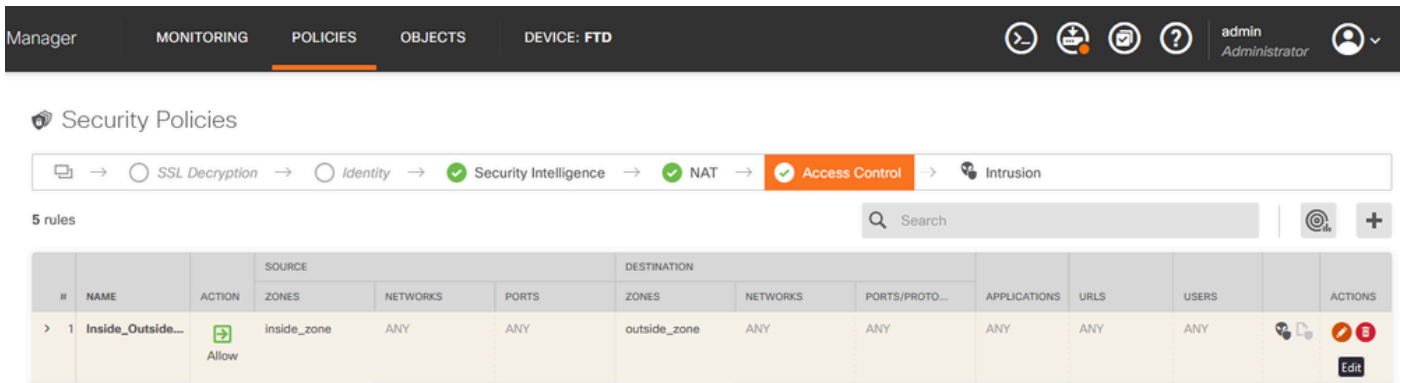
Guia Políticas do FDM

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.

Edit Access Rule

Order: 1 | Title: Inside_Outside_Rule | Action: Allow

Source/Destination | Applications | URLs | Users | Intrusion Policy | **File policy** | Logging

Evaluation Period
This feature needs a license to be purchased. For more details, go to [Smart License](#).

CONTROLLING FILES AND MALWARE
Use file policies to detect malicious software, or malware, using Advanced Malware Protection for Firepower (AMP for Firepower.) You can also use file policies to perform file control, which allows control over all files of a specific type regardless of whether the files contain malware

SELECT THE FILE POLICY

- Block Malware All (Selected)
- None
- Block Malware All
- Cloud Lookup All
- Block Office Document and PDF Upload, Block Malware Others
- Block Office Documents Upload, Block Malware Others

Show Diagram | 582 Reset | 2023-08-30 09:55:26

CANCEL OK

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

>	1	Inside_Outside...	Allow	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Block Malware All
---	---	-------------------	-------	-------------	-----	-----	--------------	-----	-----	-----	-----	-----	-----	-----	-----	-------------------

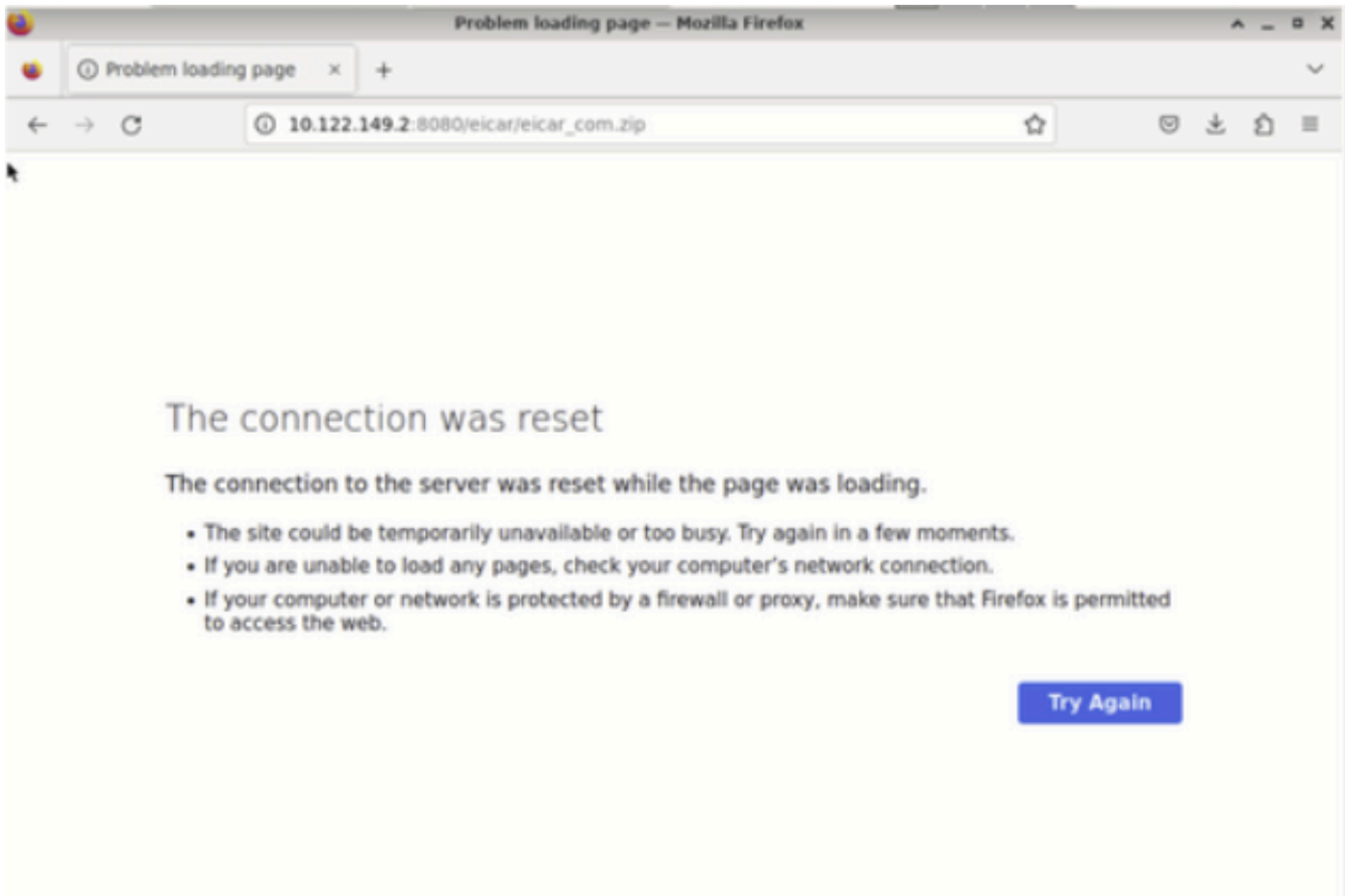
Arquivo Habilitado

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](#).

```
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 File signature verdict reject and flags 0x00005A00 for 2546dcffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad 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 2546dcffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad 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 child's 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
```

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.