Adicionar Acesso do FDM por Meio da Interface de Dados Quando a Interface de Gerenciamento Falhar

Contents

Introdução

Pré-requisitos

- Requisitos
- Componentes Utilizados

Configurar

- Configurações

Verificar

Troubleshooting

Introdução

Este documento descreve como adicionar o acesso ao HyperText Transfer Protocol (HTTP) a um Firepower Thread Defense (FTD) quando a porta de gerenciamento falhar.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso do console ao dispositivo

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Firepower 1120 Thread Defense versão 7.4.2

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.

Configurar

Configurações

Etapa 1. Na sessão de console do dispositivo, conecte-se ao FTD Command Line Interface Shell (CLISH):

```
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license.

Certain components of this software are licensed under the "GNU General Public
License, version 3" provided with ABSOLUTELY NO WARRANTY under the terms of
"GNU General Public License, Version 3", available here:
http://www.gnu.org/licenses/gpl.html. See User Manual (''Licensing'') for
details.

Certain components of this software are licensed under the "GNU General Public
License, version 2" provided with ABSOLUTELY NO WARRANTY under the terms of
"GNU General Public License, version 2", available here:
http://www.gnu.org/licenses/old-licenses/gpl-2.0.html. See User Manual
(''Licensing'') for details.

Certain components of this software are licensed under the "GNU LESSER GENERAL
PUBLIC LICENSE, version 3" provided with ABSOLUTELY NO WARRANTY under the terms
of "GNU LESSER GENERAL PUBLIC LICENSE" Version 3", available here:
http://www.gnu.org/licenses/lgpl.html. See User Manual (''Licensing'') for
details.

Certain components of this software are licensed under the "GNU Lesser General
Public License, version 2.1" provided with ABSOLUTELY NO WARRANTY under the
terms of "GNU Lesser General Public License, version 2", available here:
http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html. See User Manual
(''Licensing'') for details.

Certain components of this software are licensed under the "GNU Library General
Public License, version 2" provided with ABSOLUTELY NO WARRANTY under the terms
of "GNU Library General Public License, version 2", available here:
http://www.gnu.org/licenses/old-licenses/lgpl-2.0.html. See User Manual
(''Licensing'') for details.

KSEC-FPR1140-1# connect ftd
```

Etapa 2. A partir da CLISH do FTD, acesse o shell do Linux por meio do comando expert e obtenha privilégios de administrador:

```
>
> expert
admin@KSEC-FPR1140-1:/$ sudo su
Password:
root@KSEC-FPR1140-1:/#
```

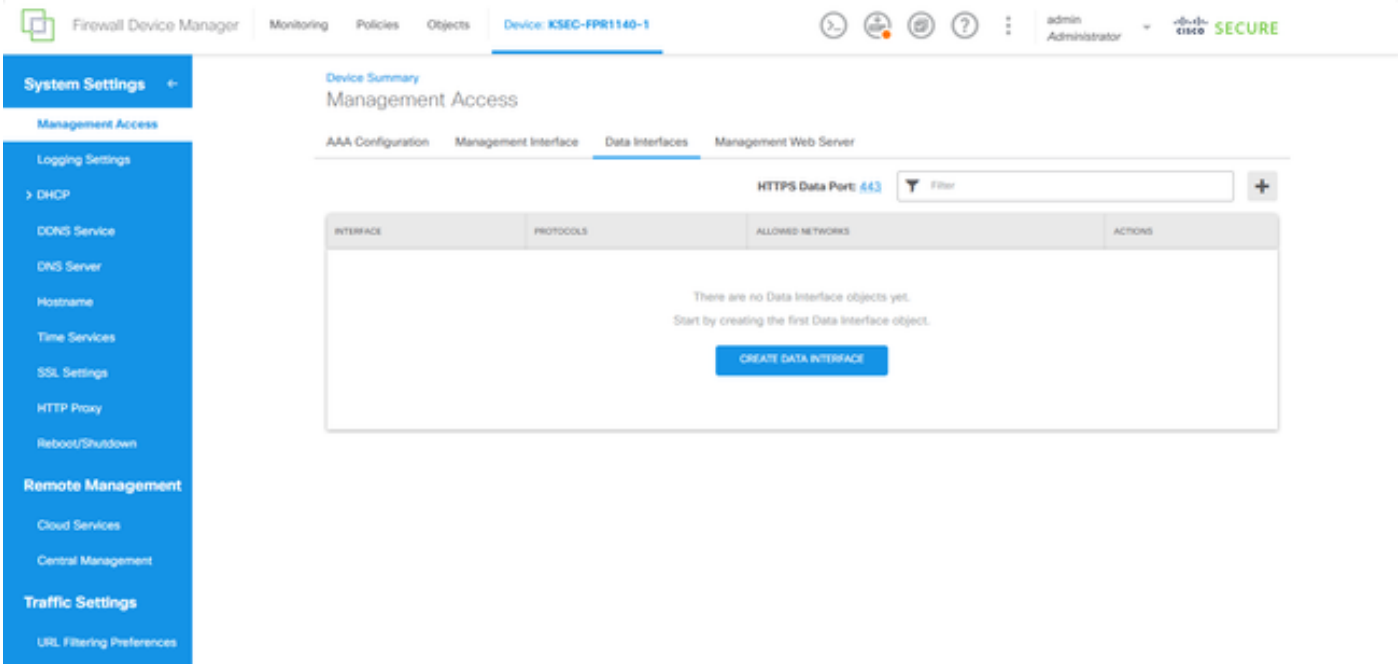
Etapa 3. Empurre as entradas do comando HTTP para a configuração Lina usando a LinaConfigTool e crie uma rota estática para enviar o tráfego do servidor Web em execução no lado do Linux para a interface nlp_int_tap no lado da Lina:

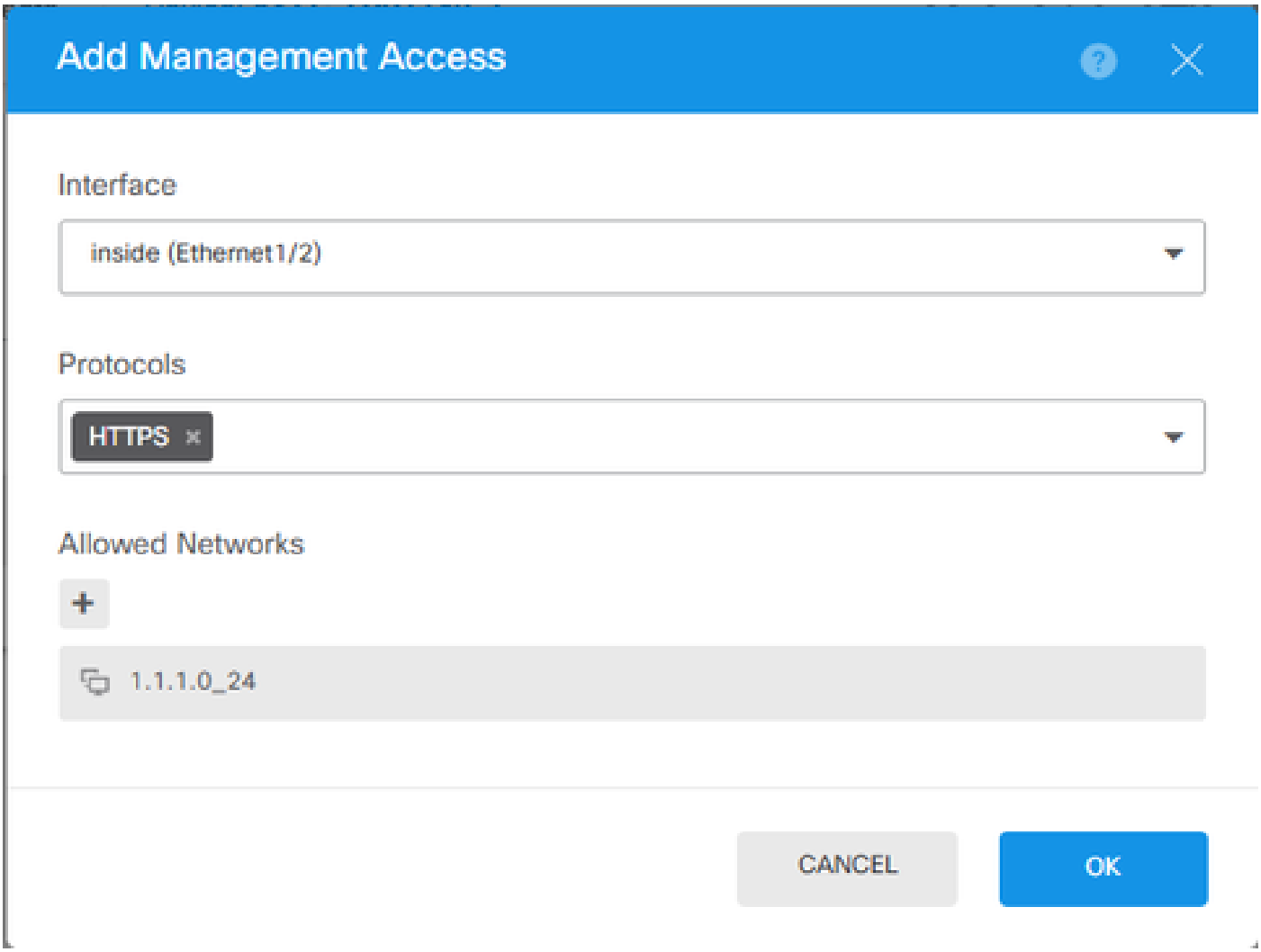
```
root@KSEC-FPR1140-1:/# LinaConfigTool "http 192.168.1.0 255.255.255.0 inside"
root@KSEC-FPR1140-1:/#
root@KSEC-FPR1140-1:/# ip route add 192.168.1.0/24 via 169.254.1.1
root@KSEC-FPR1140-1:/#
root@KSEC-FPR1140-1:/#
```

Etapa 4. Volte para a CLISH de FTD e confirme se a regra NAT (Network Address Translation, Conversão de endereço de rede) foi criada automaticamente:

```
root@KSEC-FPR1140-1:/#
root@KSEC-FPR1140-1:/#
root@KSEC-FPR1140-1:/# exit
exit
admin@KSEC-FPR1140-1:/$ exit
logout
> show nat detail
Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (inside) source static nlp_server__http_192.168.1.0_intf4 interface  destination sta
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 169.254.1.3/32, Translated: 10.10.105.87/24
    Destination - Origin: 192.168.1.0/24, Translated: 192.168.1.0/24
    Service - Protocol: tcp Real: https Mapped: https
```

Etapa 5. Acesse a interface do usuário do FDM na interface de dados e crie o acesso de gerenciamento na interface de dados a partir da interface do usuário para manter as alterações permanentes:





Verificar

Abra um navegador e tente acessar o FDM usando o endereço IP da interface de dados.

Troubleshooting

Execute uma captura de pacotes e confirme se:

- O tráfego está chegando à interface de dados.
- O tráfego está sendo encaminhado para a interface nlp_int_tap.

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.