Alterar Interface de Dados de Acesso do Gerenciador de FTD

Contents

Introdução

Este documento descreve as etapas para alterar a interface de dados de acesso do gerenciador do Secure Firewall Threat Defense (FTD).

Pré-requisitos

Requisitos

- Conhecimento básico do produto.
- Familiaridade com gerenciamento e gerenciamento de FTD em interfaces de dados.

Componentes Utilizados

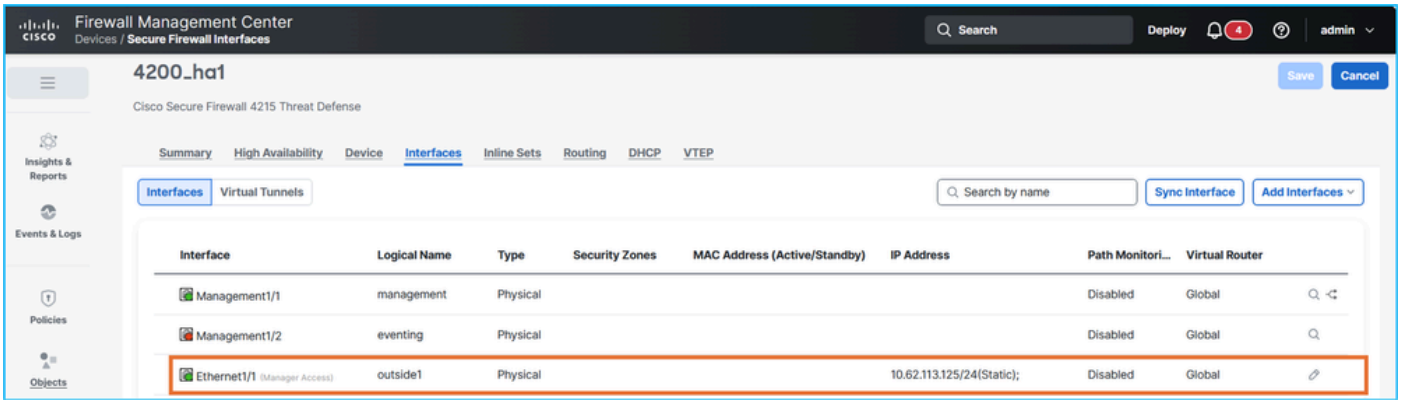
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

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

- Firewall seguro 4200
- Secure Firewall Threat Defense (FTD) 10.0.x, 7.6.4
- Centro de gerenciamento de firewall seguro (FMC) 10.0.x

Configuração inicial

1. O FMC gere o FTD em alta disponibilidade (HA) através da interface de dados Ethernet1/1 com o nome se outside1, utilizando os endereços IP ativo e em espera 10.62.113.125 e 10.62.113.126, respectivamente:



Verificação no FTD CLISH:

<#root>

>

show network management-data-interface

Physical Interface Name of the Interface

Ethernet1/1 outside1

>

show network

```
===============[ System Information ]===============
Hostname                  : CSF4215-3
..
DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
…
======[ System Information - Data Interfaces ]======
DNS Servers               : 192.0.2.100

Interfaces                : Ethernet1/1



==================[

Ethernet1/1

 ]===================

State                     : Enabled
Link                      : Up

Name                      : outside1


MTU                       : 1500
MAC Address               : 40:F4:9F:3D:5A:0E

----------------------[ IPv4 ]----------------------



Configuration             : Manual



Address                   : 10.62.113.125



Netmask                   : 255.255.255.0



Gateway                   : 10.62.113.1


…
```

2. São estabelecidas ligações sftunnel entre a unidade HA do FTD e o FMC:

<#root>

>

sftunnel-status-brief

PEER:fmc.example.org

SFTunnel Status:-

Channel A: Connected

Channel B: Connected

```
Peer channel Channel-A is valid  type (CONTROL), using 'tap_nlp', connected to '198.51.100.23' v
Peer channel Channel-B is valid  type (EVENT), using 'tap_nlp', connected to '198.51.100.23' vi
Registration: Completed.
IPv4 Connection to peer 'fmc.example.org' Start Time: Fri Jul 17 08:22:31 2026 UTC
Heartbeat Send Time:     Fri Jul 17 08:52:42 2026 UTC
Heartbeat Received Time: Fri Jul 17 08:53:03 2026 UTC
Last disconnect time   : Fri Jul 17 08:22:16 2026 UTC
Last disconnect reason : Process shutdown due to stop request from PM
```

3. O FTD depende da resolução DNS para se conectar ao FMC. O gerenciador é uma configuração baseada no FQDN (nome de domínio totalmente qualificado):

<#root>

>

show managers

```
Type                      : Manager
Host                      : fmc.example.org
```

```
Display name              : fmc.example.org


Version                   : 10.0.1 (Build 1)
Identifier                : 6d86efc4-c095-11f0-9244-48f1a7894b18
Registration              : Completed
Management type           : Configuration and analytics

>

show network


===============[ System Information ]===============
Hostname                  : KSEC-FPR-4215-3

Domains                   : example.org



DNS Servers               : 192.0.2.100


DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
…
```

Os servidores DNS podem ser acessados através da interface outside1.

4. As conexões sftunnel são estabelecidas através do mecanismo Lina:

<#root>

```
>

show conn all port 8305


26 in use, 32 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect


TCP nlp_int_tap  10.62.113.125(169.254.1.3):8305 outside1  198.51.100.23:45647, idle 0:00:03, bytes 2129
```

```
TCP nlp_int_tap  10.62.113.125(169.254.1.3):37141 outside1  198.51.100.23:8305, idle 0:00:04, bytes 1485
```

Configuration Steps

O objetivo é mover o acesso do gerenciador da interface outside1 atual para a interface outside2 de destino. Os endereços IP externo2 ativo e standby são 10.62.114.51/24 e 10.62.114.52/24, respectivamente.

Observe que as versões 7.7.0 ou posterior do FTD oferecem suporte a interfaces redundantes de dados de acesso do gerenciador, que permitem a configuração e a implantação de mais de uma interface de acesso do gerenciador. Este recurso não é suportado em versões anteriores à 7.7.0.

Devido a esse fato, as etapas específicas são ignoradas ou contêm ações diferentes.

⚠ Caution: Não cancele nem apague o registro de FTD do FMC em nenhuma etapa.

1. É recomendável ter acesso de console aos FTDs:

- No caso do Firepower 4100/9300, você pode se conectar ao chassi usando SSH e, em seguida, conectar-se ao console de FTD nativo usando o comando connect module x console, onde x é o ID do módulo de slot/segurança.
- No caso do Firepower 4100/9300 executando o FTD no modo de várias instâncias (MI), você pode se conectar ao chassi usando SSH e, em seguida, conectar-se ao console do FTD nativo usando o comando connect module x telnet, onde x é o ID do módulo de slot/segurança. Em seguida, conecte-se à instância de FTD usando o comando connect ftd <ftd_id> .
- No caso do Secure Firewall 3100/4200 no modo MI, você pode se conectar ao chassi usando SSH e, em seguida, conectar-se ao console FTD usando o comando connect ftd <identifier>.

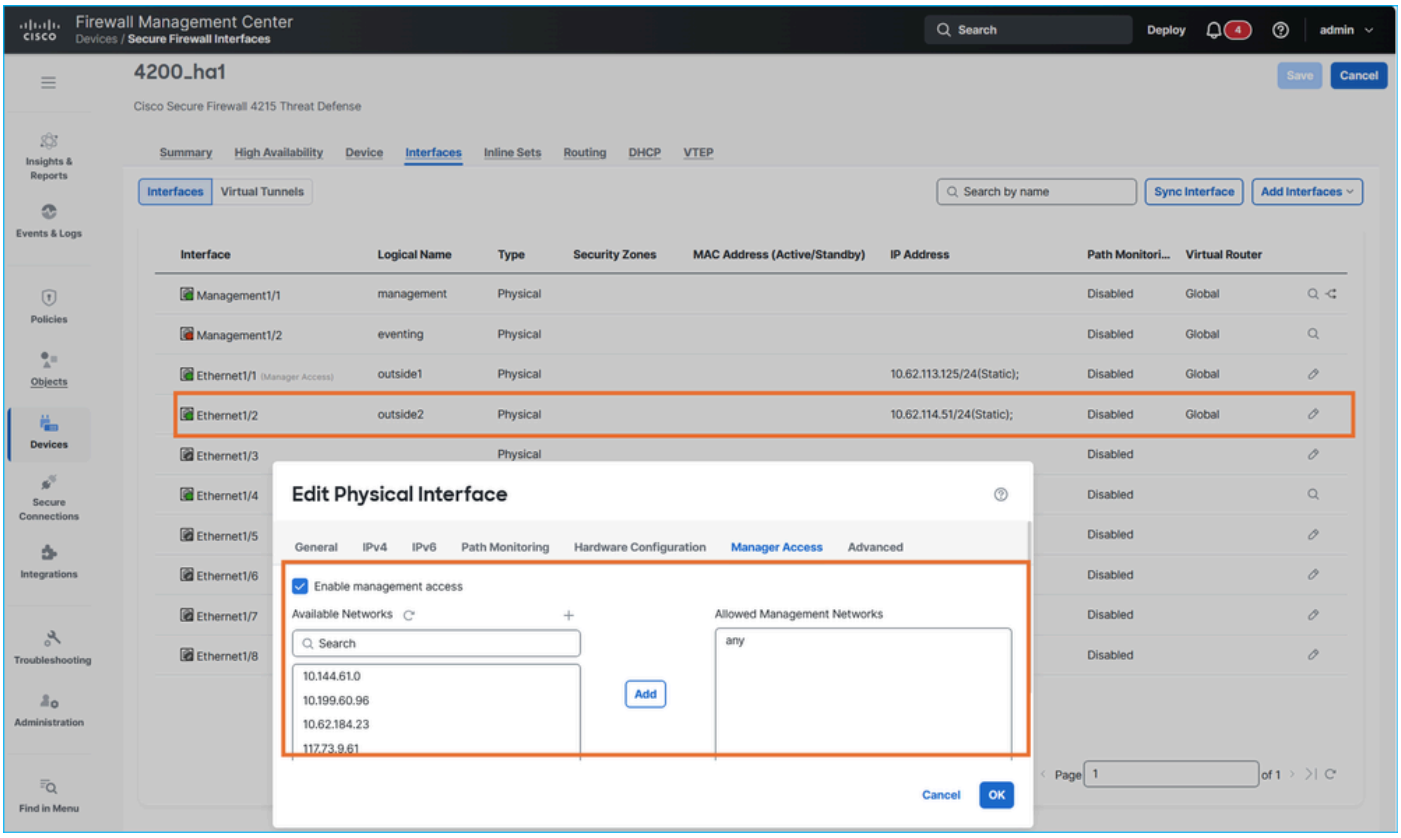
2. Implantar políticas pendentes.

3. É altamente recomendável fazer backups de FTD e FMC. No caso de FTD HA, pegue o backup de ambas as unidades.

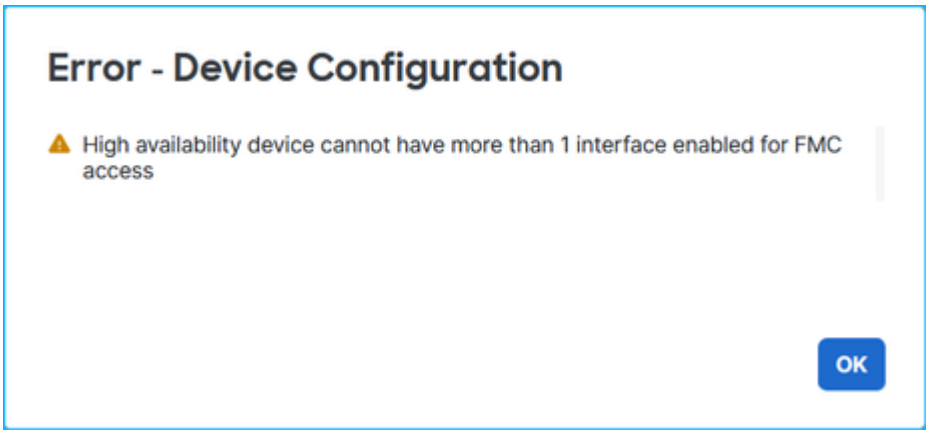
4. Configure o nome da interface de destino, o endereço IP, a zona de segurança e outras configurações relacionadas à interface, se aplicável.

5. Configure o endereço IP standby da interface de destino.

6. Se a versão do software FTD for 7.7.0 ou posterior, habilite o acesso do gerenciador na interface de destino e ajuste as redes de acesso de gerenciamento conforme necessário:



Observe que as versões do FTD anteriores à 7.7.0 não suportam interfaces redundantes de dados de acesso do gerenciador. A tentativa de configurar uma segunda interface de acesso do gerenciador resulta nesta mensagem de erro:



Certifique-se de ignorar as etapas 7 e 8 para versões do FTD anteriores à 7.7.0.

7. Implante as políticas e verifique as configurações na CLISH do FTD. Neste exemplo, a interface Ethernet1/2 com nameif outside2 tem os endereços IP 10.62.114.51 e 10.62.114.52, respectivamente:

```
<#root>

>

show ip


System IP Addresses:
Interface                Name                IP address      Subnet mask     Method
Ethernet1/1              outside1            10.62.113.125   255.255.255.0   manual <- source interf

Ethernet1/2              outside2            10.62.114.51    255.255.255.0   manual

<- target interface
Ethernet1/4              fover               10.9.0.21       255.255.255.0   unset
```

A interface outside2 é adicionada à configuração de sftunnel:

```
<#root>

>

show running-config sftunnel


sftunnel interface outside2
```

```
<- target interface

sftunnel interface outside1

<- source interface
sftunnel port 8305
sftunnel route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346
```

Embora regras adicionais sejam instaladas na tabela NAT (Network Address Translation Conversão de Endereços de Rede), as regras com a interface outside1 estão em uso:

```
<#root>

>

show nat detail


Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (outside1) source static nlp_server__sftunnel_0.0.0.0_intf5 interface  destination s
    translate_hits = 1448, untranslate_hits = 1448
    Source - Origin: 169.254.1.3/32, Translated: 10.62.113.125/24
    Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
    Service - Protocol: tcp Real: 8305 Mapped: 8305

2 (nlp_int_tap) to (outside2) source static nlp_server__sftunnel_0.0.0.0_intf6 interface  destination st


    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
    Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
    Service - Protocol: tcp Real: 8305 Mapped: 8305
3 (nlp_int_tap) to (outside1) source static nlp_server__sftunnel_::_intf5 interface ipv6  destination s
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:
    Destination - Origin: ::/0, Translated: ::/0
    Service - Protocol: tcp Real: 8305 Mapped: 8305
4

(nlp_int_tap) to (outside2) source static nlp_server__sftunnel_::_intf6 interface ipv6  destination stat


    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:
    Destination - Origin: ::/0, Translated: ::/0
    Service - Protocol: tcp Real: 8305 Mapped: 8305
5 (nlp_int_tap) to (outside1) source dynamic nlp_client_0_intf5 interface
    translate_hits = 653, untranslate_hits = 0
    Source - Origin: 169.254.1.3/32, Translated: 10.62.113.125/24
6

(nlp_int_tap) to (outside2) source dynamic nlp_client_0_intf6 interface
```

```
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
7 (nlp_int_tap) to (outside1) source dynamic nlp_client_0_ipv6_intf5 interface ipv6
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:
8

(nlp_int_tap) to (outside2) source dynamic nlp_client_0_ipv6_intf6 interface ipv6


    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:
```

8. Verificar o status de alta disponibilidade e o monitoramento da interface:

<#root>

>

show monitor-interface

```
        This host: Primary - Active


                Interface management (203.0.113.130): Normal (Monitored)
                Interface outside1 (10.62.113.125): Normal (Monitored)
                Interface outside2 (10.62.114.51): Normal (Monitored)

        Other host: Secondary - Standby Ready


                Interface management (203.0.113.131): Normal (Monitored)
                Interface outside1 (10.62.113.126): Normal (Monitored)
                Interface outside2 (10.62.114.52): Normal (Monitored)
```

9. Se você planeja gerenciar os FTDs pela interface outside2, certifique-se de que o acesso na seção Acesso SSH das configurações da plataforma seja permitido.

10. Faça as alterações necessárias para permitir a conectividade na interface de destino com os servidores de nomes de domínio (DNS) e o FMC:

- Se a resolução de nomes de domínio (DNS) for necessária para a conectividade entre o

FMC e os FTDs, certifique-se de que os FTDs tenham acessibilidade na interface de destino para o próximo salto usado para acessar os servidores DNS. A resolução DNS também deve ser permitida no caminho de trânsito.
- Garantir que os FTDs tenham acessibilidade na interface de destino até o próximo salto a ser usado para acessar o FMC.
- Assegurar que a conectividade bidirecional entre o FMC e os FTDs pela porta TCP 8305 é permitida no caminho de trânsito através da interface de destino. A conexão deve ser permitida em ambas as direções.

Nesse caso, o IP 10.62.114.1 precisa ser usado como gateway padrão na interface de destino. O endereço IP do próximo salto pode ser acessado usando o Internet Control Message Protocol (ICMP):

```
<#root>

>

ping 10.62.114.1


Please use 'CTRL+C' to cancel/abort...

Sending 5, 100-byte ICMP Echos to 10.62.114.1, timeout is 2 seconds:



!!!!!


Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Se o ICMP estiver administrativamente bloqueado no caminho de trânsito ou no próximo salto, certifique-se de que o endereço de Controle de Acesso ao Meio (MAC - Media Access Control) do próximo salto esteja visível na saída do comando show arp e seja válido:

```
<#root>

>

show arp


        fover 10.9.0.22 4c01.f7e9.e111 13275
        outside1 10.62.113.1 c02c.1782.2cbf 1
        outside1 10.62.113.126 4c01.f7e9.e10e 5453
```

```
outside2 10.62.114.1 c02c.1782.2cbf 0


        outside2 10.62.114.52 4c01.f7e9.e10f 5453
```

11. Execute estas etapas dependendo da versão do FTD:

- Versão 7.7.0 ou posterior: no FMC, desabilite o acesso do gerenciador na interface de origem (outside1), ajuste o roteamento, incluindo o roteamento para servidores DNS (se o DNS for usado para acessar o FMC) e o FMC na interface de destino (outside2). Por exemplo, configure rotas estáticas específicas ou configure o gateway padrão na interface de destino.
- Versão anterior à 7.7.0: no FMC, desabilite o acesso do gerenciador na interface de origem (outside1), habilite o acesso do gerenciador na interface de destino (outside2), ajuste o roteamento, incluindo o roteamento para servidores DNS (se o DNS for usado para acessar o FMC) e o FMC na interface de destino (outside2). Por exemplo, configure rotas estáticas específicas ou configure o gateway padrão na interface de destino.

12. Implantar políticas.

13. Verificar no FTD CLISH:

```
<#root>

>

show route 0.0.0.0



Routing entry for 0.0.0.0 0.0.0.0, supernet
  Known via "static", distance 1, metric 0, candidate default path
  Routing Descriptor Blocks:

  * 10.62.114.1, via outside2

<- default route over outside2
      Route metric is 0, traffic share count is 1


>

show running-config sftunnel
```

sftunnel interface outside2

<- sftunnel is enabled only over outside2
sftunnel port 8305

>

show nat detail

Manual NAT Policies Implicit (Section 0)

1 (nlp_int_tap) to (outside2) source static nlp_server__sftunnel_0.0.0.0_intf6 interface destination st

translate_hits = 3, untranslate_hits = 3

Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
Service - Protocol: tcp Real: 8305 Mapped: 8305
2 (nlp_int_tap) to (outside2) source static nlp_server__sftunnel_::_intf6 interface ipv6 destination s
translate_hits = 0, untranslate_hits = 0
Source - Origin: fd00:0:0:1::3/128, Translated:
Destination - Origin: ::/0, Translated: ::/0
Service - Protocol: tcp Real: 8305 Mapped: 8305
3 (nlp_int_tap) to (outside2) source dynamic nlp_client_0_intf6 interface
translate_hits = 407, untranslate_hits = 0
Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
4 (nlp_int_tap) to (outside2) source dynamic nlp_client_0_ipv6_intf6 interface ipv6
translate_hits = 0, untranslate_hits = 0
Source - Origin: fd00:0:0:1::3/128, Translated:

>

show conn all port 8305

31 in use, 42 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap 10.62.114.51(169.254.1.3):56853 outside2 198.51.100.23:8305, idle 0:00:06, bytes 33008

<- connectivity over outside2

TCP nlp_int_tap 10.62.114.51(169.254.1.3):32905 outside2 198.51.100.23:8305, idle 0:00:00, bytes 15959

<- connectivity over outside2

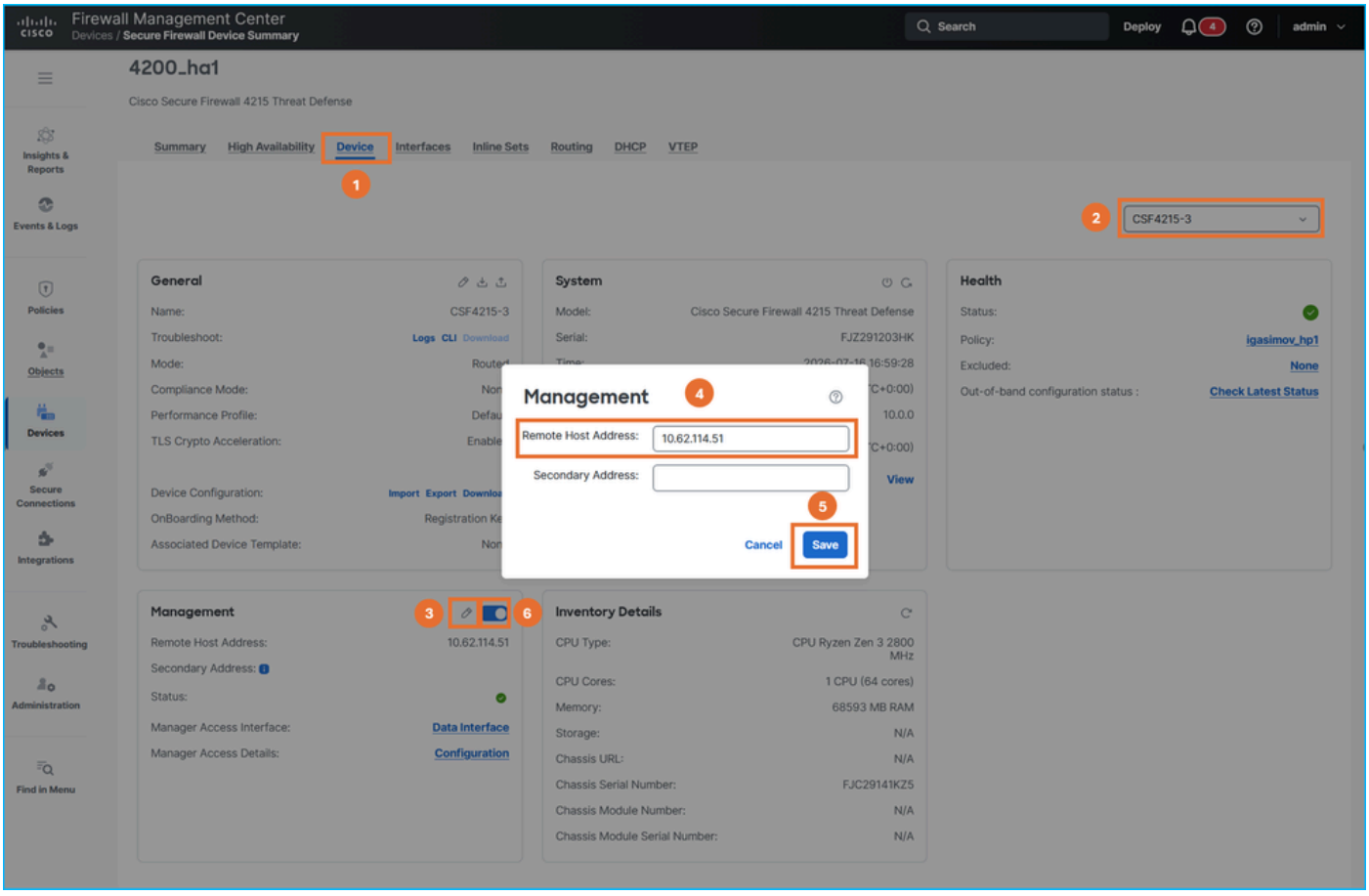
14. Se os servidores DNS na saída do comando 'show network' CLISH precisarem ser alterados, configure os novos servidores DNS:

<#root>

>

configure network dns servers 192.0.2.184

15. No FMC, altere o endereço IP de gerenciamento do FTD para o endereço IP outside2 e, em seguida, desative e reative a conectividade usando o controle deslizante. Repita este passo para ambas as unidades em HA:



16. Verifique a conectividade de sftunnel em todos os FTDs:

<#root>

>

sftunnel-status-brief

```
PEER:198.51.100.23
        SFTunnel Status:-
```

Channel A: Connected

Channel B: Connected

```
        Peer channel Channel-A is valid  type (CONTROL), using 'tap_nlp', connected to '198.51.100.23' v
        Peer channel Channel-B is valid  type (EVENT), using 'tap_nlp', connected to '198.51.100.23' vi
        Registration: Completed.
        IPv4 Connection to peer '198.51.100.23' Start Time: Thu Jul 16 16:37:14 2026 UTC
        Heartbeat Send Time:     Thu Jul 16 16:38:13 2026 UTC
        Heartbeat Received Time: Thu Jul 16 16:39:13 2026 UTC
        Last disconnect time   : Thu Jul 16 16:37:11 2026 UTC
        Last disconnect reason : Both control and event channel connections with peer went down

>
```

show conn all port 8305

```
32 in use, 42 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect
```

TCP nlp_int_tap 10.62.114.51(169.254.1.3):8305 outside2 198.51.100.23:36383, idle 0:00:00, bytes 23575

```
<- new connection over different source port
```

TCP nlp_int_tap 10.62.114.51(169.254.1.3):8305 outside2 198.51.100.23:50963, idle 0:00:01, bytes 12319

```
<- new connection over different source port
```

17. Se os servidores DNS nas configurações das plataformas precisarem ser alterados, faça as alterações de configuração apropriadas e implante políticas.

Solucionar problemas da conexão de gerenciamento

Use estes comandos para verificações:

1. show network - mostra a configuração da interface de gerenciamento.
2. sftunnel-status-brief - mostra o status da conectividade do sftunnel.
3. show run sftunnel - mostra a configuração do sftunnel no mecanismo de firewall (Lina).
4. show conn all port 8305 - mostra as conexões sftunnel através do mecanismo Lina.

Para solucionar problemas de conexões de gerenciamento, consulte a seção Solução de problemas de conexão de gerenciamento no guia oficial.

Referências

1. Guia de configuração de dispositivos do Cisco Secure Firewall Management Center, 10.x
2. Alterar a interface de acesso do gerente
3. Solucionando problemas da conexão de gerenciamento

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.