FTDマネージャのアクセスデータインターフェイスの変更

内容

はじめに

このドキュメントでは、セキュアファイアウォール脅威対策(FTD)マネージャアクセスデータインターフェイスを変更する手順について説明します。

前提条件

要件

- 製品の基礎知識
- FTD管理およびデータインターフェイス上の管理に精通していること。

使用するコンポーネント

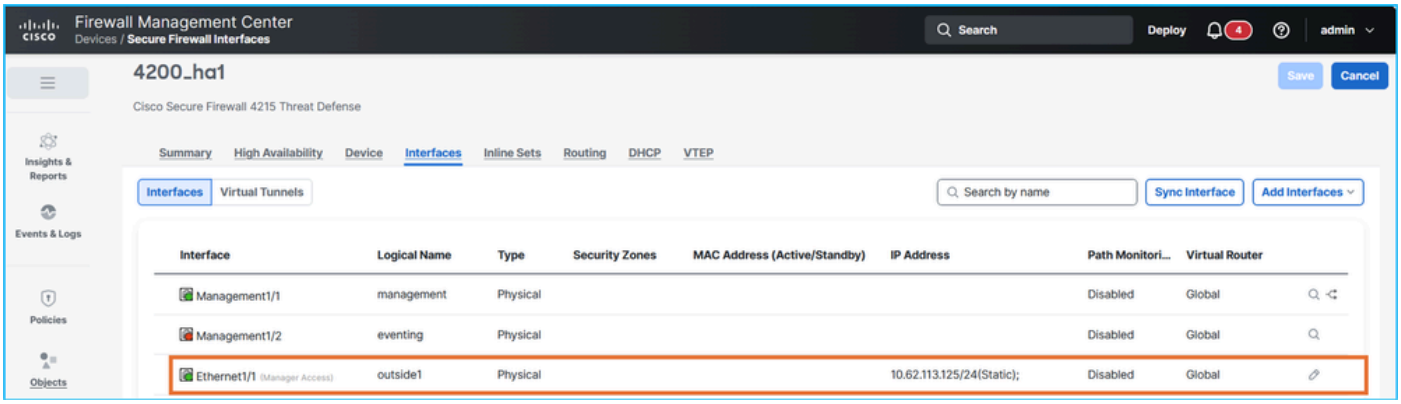
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure Firewall 4200
- セキュアファイアウォール脅威対策(FTD)10.0.x、7.6.4
- セキュアファイアウォール管理センター(FMC)10.0.x

初期設定

1. FMCは、アクティブとスタンバイのIPアドレス10.62.113.125と10.62.113.126をそれぞれ使用して、データインターフェイスEthernet1/1とnameif outside1を介して、ハイアベイラビリティ(HA)のFTDを管理します。



FTD CLISHでの検証：

<#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. FTD HAユニットとFMCの間にsftunnel接続が確立されます。

<#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. FTDはDNS解決を使用してFMCに接続します。マネージャは、完全修飾ドメイン名(FQDN)に基づいて設定されます。

<#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
…
```

DNSサーバにはoutside1インターフェイスを介して到達できます。

4. sftunnel接続は、Linaエンジン経由で確立されます。

<#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
```

設定手順

目標は、現在のoutside1インターフェイスからターゲットのoutside2インターフェイスにマネージャアクセスを移動することです。アクティブとスタンバイのoutside2のIPアドレスは、それぞれ10.62.114.51/24と10.62.114.52/24です。

FTDバージョン7.7.0以降では、冗長マネージャアクセスデータインターフェイスがサポートされており、複数のマネージャアクセスインターフェイスの設定と導入が可能です。この機能は、7.7.0より前のバージョンではサポートされていません。

このため、特定のステップがスキップされたり、異なるアクションが含まれたりします。

⚠ 注意:どの手順でも、FMCからFTDを登録解除/削除しないでください。

1. FTDへのコンソールアクセスを持つことを推奨します。

- Firepower 4100/9300の場合は、SSHを使用してシャーシに接続してから、connect module x consoleコマンドを使用してネイティブFTDコンソールに接続できます。ここでxはスロット/セキュリティモジュールIDです。
- マルチインスタンス(MI)モードでFTDを実行しているFirepower 4100/9300の場合は、SSHを使用してシャーシに接続してから、connect module x telnetコマンドを使用してネイティブFTDコンソールに接続できます。ここでxはスロット/セキュリティモジュールIDです。次に、connect ftd <ftd_id>コマンドを使用してFTDインスタンスに接続します。
- MIモードのセキュアファイアウォール3100/4200の場合は、SSHを使用してシャーシに接続してから、connect ftd <identifier>コマンドを使用してFTDコンソールに接続できます。

2. 保留中のポリシーを展開します。

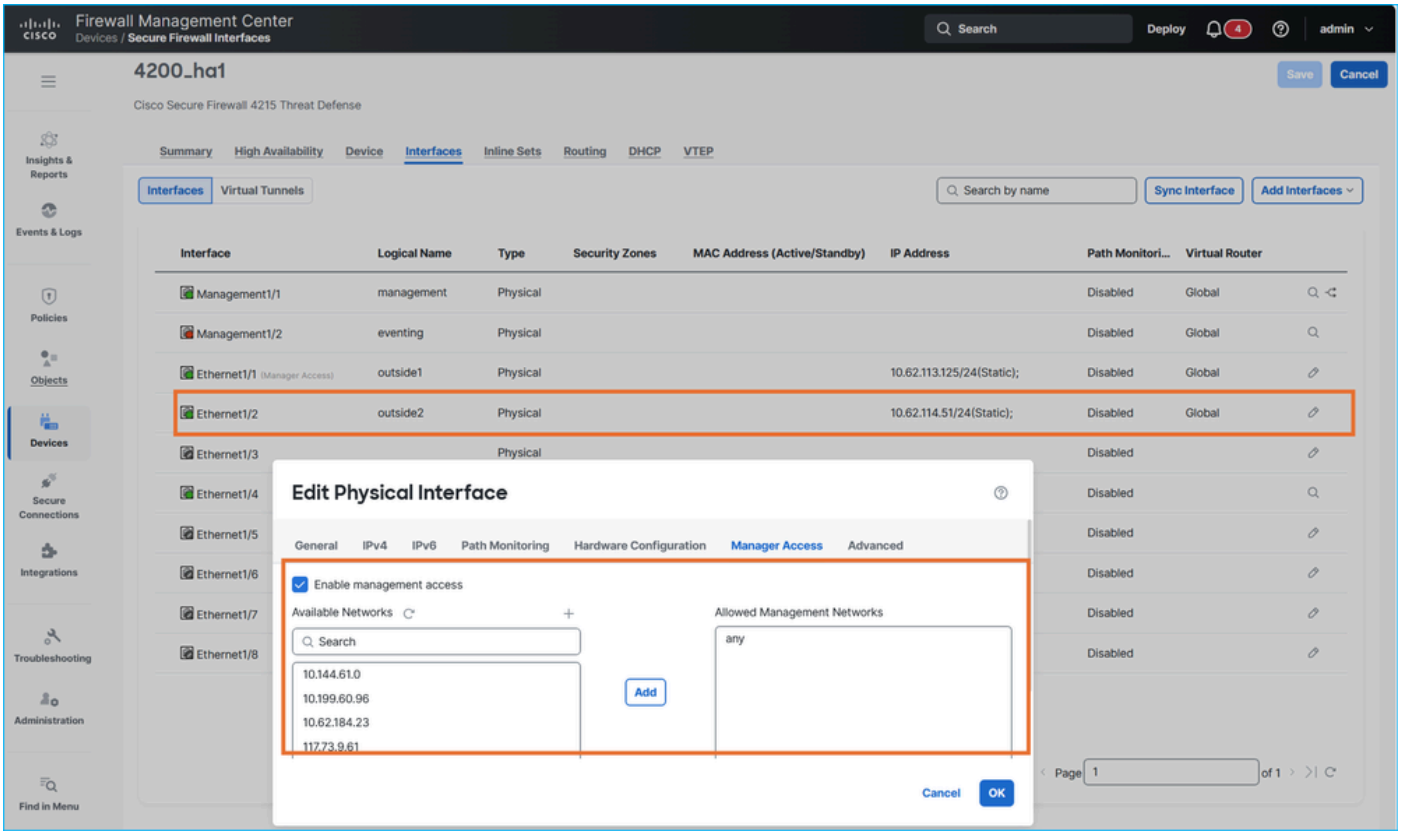
3. FTDとFMCのバックアップを取ることを強くお勧めします。FTD HAの場合は、両方のユニ

ットのバックアップを取ります。

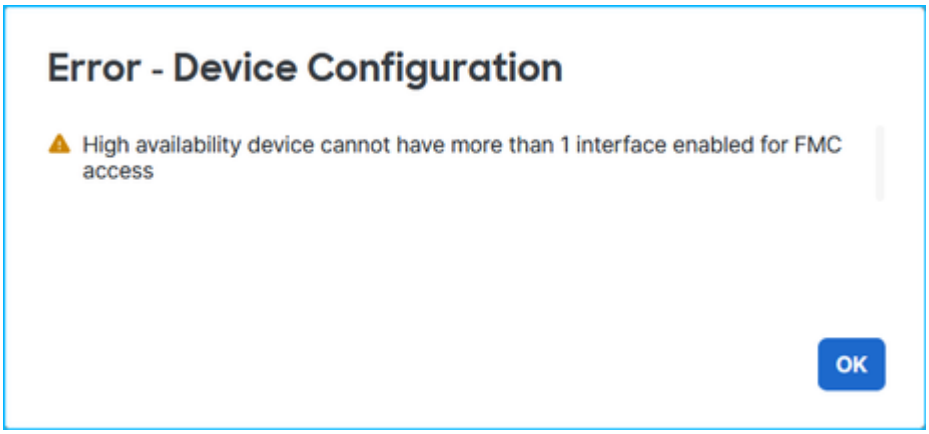
4. 必要に応じて、ターゲットインターフェイスのnameif、IPアドレス、セキュリティゾーン、およびその他のインターフェイス関連の設定を構成します。

5. ターゲットインターフェイスのスタンバイIPアドレスを設定します。

6. FTDソフトウェアバージョンが7.7.0以降の場合は、ターゲットインターフェイスでマネージャアクセスをイネーブルにし、必要に応じて管理アクセスネットワークを調整します。



7.7.0よりも前のFTDバージョンは、冗長マネージャアクセスデータインターフェイスをサポートしていないことに注意してください。2番目のマネージャアクセスインターフェイスを設定しようとすると、次のエラーメッセージが表示されます。



7.7.0よりも前のFTDバージョンでは、ステップ7と8を必ずスキップしてください。

7. ポリシーを展開し、FTD CLISHの設定を確認します。次の例では、nameif outside2を持つEthernet1/2インターフェイスのIPアドレスはそれぞれ10.62.114.51と10.62.114.52です。

```
<#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
```

outside2インターフェイスがsftunnel設定に追加されます。

```
<#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

ネットワークアドレス変換(NAT)テーブルにはさらに多くのルールがインストールされていますが、outside1インターフェイスを持つルールが使用されています。

<#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. ハイアベイラビリティステータスとインターフェイスモニタリングを確認します。

```
<#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. outside2インターフェイス経由でFTDを管理する場合は、プラットフォーム設定のSSH Accessセクションでアクセスが許可されていることを確認します。

10. 必要な変更を行い、ターゲットインターフェイスを介したドメインネームサーバ(DNS)およびFMCへの接続を許可します。

- FMCとFTDの間の接続にドメイン名解決(DNS)が必要な場合は、FTDが、DNSサーバに到達するために使用されるネクストホップへのターゲットインターフェイスを介して到達できる

ことを確認します。DNS解決もトランジットパスで許可する必要があります。
- FTDがターゲットインターフェイス経由で、FMCに到達するために使用されるネクストホップに到達できることを確認します。
- TCPポート8305を介したFMCとFTDの間の双方向接続が、ターゲットインターフェイス上のトランジットパスで許可されていることを確認します。接続は両方向で許可されている必要があります。

この場合、IP 10.62.114.1をターゲットインターフェイス上のデフォルトゲートウェイとして使用する必要があります。ネクストホップIPアドレスは、インターネット制御メッセージプロトコル(ICMP)を使用して到達可能です。

```
<#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
```

中継パスまたはネクストホップでICMPが管理上ブロックされている場合は、ネクストホップのMedia Access Control（MAC；メディアアクセス制御）アドレスが、show arpコマンドの出力に表示されており、有効であることを確認します。

```
<#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. FTDのバージョンに応じて、次の手順を実行します。

- バージョン7.7.0以降：FMCで、送信元インターフェイス(outside1)経由のマネージャアクセスを無効にし、ルーティングを調整します。これには、DNSサーバ（DNSを使用してFMCにアクセスする場合）へのルーティングと、ターゲットインターフェイス(outside2)経由のFMCが含まれます。 たとえば、特定のスタティックルートを設定するか、ターゲットインターフェイスでデフォルトゲートウェイを設定します。
- 7.7.0よりも前のバージョン：FMCで、送信元インターフェイス(outside1)経由のマネージャアクセスを無効にし、ターゲットインターフェイス(outside2)経由のマネージャアクセスを有効にし、ルーティングを調整します。これには、DNSを使用してFMCにアクセスする場合のDNSサーバへのルーティング、およびターゲットインターフェイス(outside2)経由のFMCへのルーティングが含まれます。 たとえば、特定のスタティックルートを設定するか、ターゲットインターフェイスでデフォルトゲートウェイを設定します。

12. ポリシーの展開

13. FTD CLISHでの確認：

<#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

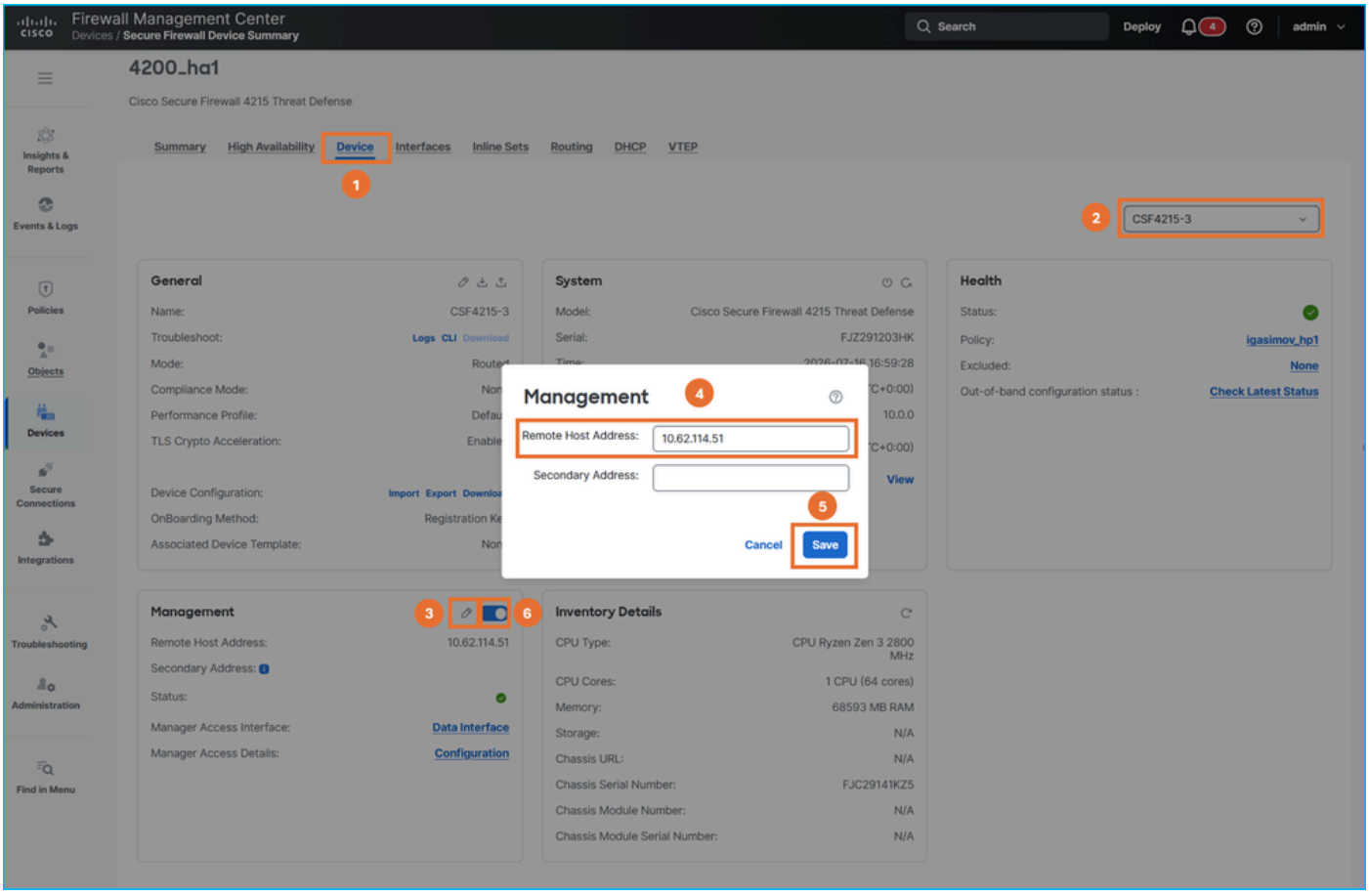
14. 「show network」CLISHコマンドの出力のDNSサーバを変更する必要がある場合は、新しいDNSサーバを設定します。

<#root>

>

configure network dns servers 192.0.2.184

15. FMCで、FTDの管理IPアドレスをoutside2のIPアドレスに変更してから、スライダを使用して接続を無効にしてから再度有効にします。HA内の両方のユニットに対して、この手順を繰り返します。



16. すべてのFTDでsftunnel接続を確認します。

<#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. プラットフォーム設定のDNSサーバーを変更する必要がある場合は、適切な構成の変更を行い、ポリシーを展開します。

管理接続のトラブルシューティング

確認には次のコマンドを使用します。

1. show network：管理インターフェイスの設定を表示します。
2. sftunnel-status-brief:sftunnelの接続ステータスを表示します。
3. show run sftunnel：ファイアウォールエンジン(Lina)のsftunnel設定を表示します。
4. show conn all port 8305:Linaエンジン経由のsftunnel接続を表示します。

管理接続の問題のトラブルシューティングについては、公式ガイドの「管理接続のトラブルシューティング」セクションを参照してください。

参照資料

1. Cisco Secure Firewall Management Centerデバイス設定ガイド、10.x
2. マネージャアクセスインターフェイスの変更
3. 管理接続のトラブルシューティング

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。