# ルーテッドモードでのFirepower Threat Defense(FTD)インターフェイスの設定

| 内容                                 |
|------------------------------------|
| <u>はじめに</u>                        |
| 前提条件                               |
| <u>要件</u>                          |
| <u>使用するコンポーネント</u>                 |
| <u>関連製品</u>                        |
| <u>背景説明</u>                        |
| <u>設定</u>                          |
| <u>ネットワーク図</u>                     |
| <u>ルーテッドインターフェイスとサブインターフェイスの設定</u> |
| <u>ステップ1:論理インターフェイスの設定</u>         |
| <u>ステップ 2:物理インターフェイスの設定</u>        |
| <u>FTD ルーテッド インターフェイスの動作</u>       |
| <u>FTD ルーテッド インターフェイスの概要</u><br>   |
|                                    |
| <u>FTDルーテッドインターフェイスでのパケットのトレース</u> |
| 関 <u>連情報</u>                       |

# はじめに

このドキュメントでは、Firepower Threat Defense(FTD)アプライアンスのインラインペアインターフェイス(IPAIR)の設定、検証、および動作について説明します。

# 前提条件

#### 要件

このドキュメントに関する特定の要件はありません。

#### 使用するコンポーネント

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。

- ASA5512-X:FTDコード6.1.0.x
- ・ Firepower Management Center(FMC): コード6.1.0.x

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ました。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。

#### 関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X
- FPR2100、FPR4100、FPR9300
- VMware (ESXi)、Amazon Web Services (AWS)、カーネルベース仮想マシン(KVM)
- FTDソフトウェアコード6.2.x以降

### 背景説明

firepower Threat Defense(FTD)には、次の図に示すように、2つの導入モードと6つのインターフェイスモードがあります。



№ 注:単一のFTDアプライアンスで複数のインターフェイスモードを混在させることができます。

さまざまなFTD導入モードとインターフェイスモードの概要は次のとおりです。

| FTDインターフ | FTD 展開モード | 説明 | トラフィックの |
|----------|-----------|----|---------|
|----------|-----------|----|---------|

| ェイス モード           |                           |                                    | ドロップの可否 |
|-------------------|---------------------------|------------------------------------|---------|
| Routed            | Routed                    | LINAエンジンとSnortエンジンの<br>フルチェック      | Yes     |
| 交換された             | トランスペアレ<br>ント             | LINAエンジンとSnortエンジンの<br>フルチェック      | Yes     |
| インライン ペア          | ルーテッドまた<br>はトランスペア<br>レント | 部分的なLINAエンジンと完全な<br>Snortエンジンのチェック | Yes     |
| タップ付きイン<br>ライン ペア | ルーテッドまた<br>はトランスペア<br>レント | 部分的なLINAエンジンと完全な<br>Snortエンジンのチェック | いいえ     |
| Passive           | ルーテッドまた<br>はトランスペア<br>レント | 部分的なLINAエンジンと完全な<br>Snortエンジンのチェック | いいえ     |
| パッシブ<br>(ERSPAN)  | Routed                    | 部分的なLINAエンジンと完全な<br>Snortエンジンのチェック | いいえ     |

# 設定

### ネットワーク図



## ルーテッドインターフェイスとサブインターフェイスの設定

次の要件に従って、サブインターフェイスG0/0.201とインターフェイスG0/1を設定します。

| インターフェイス       | G0/0.201         | G0/1             |
|----------------|------------------|------------------|
| [名前(Name)]     | INSIDE           | OUTSIDE          |
| セキュリティ ゾーン     | INSIDE_ZONE      | OUTSIDE_ZONE     |
| 説明             | INTERNAL         | EXTERNAL         |
| サブ インターフェイス ID | 201              | -                |
| VLAN ID        | 201              | -                |
| IPv4           | 192.168.201.1/24 | 192.168.202.1/24 |
| デュプレックス/速度     | 自動               | 自動               |

解決方法

ステップ1:論理インターフェイスの設定

Devices > Device Managementの順に移動し、適切なデバイスを選択してEditアイコンを選択します。

| Overview Analysis  | Policies    | Devices        | Objects    | АМР                            |                                      | Deploy         | 📀 Syst | tem        |
|--|-------------|----------------|------------|--------------------------------|--------------------------------------|----------------|--------|------------|
| Device Management  | NAT         | VPN Qos        | S Platform | n Settings                     |                                      |                |        |            |
|  |             |                |            |                                |                                      | By Group       | ~      | $\bigcirc$ |
| Name   |             |                | Group      | Model                          | License Type 🔺                       | Access Control | Policy |            |
| <ul> <li>Ungrouped (8)</li> <li>FTD5512<br/>10.62.148.10 - Ci</li> </ul> | sco ASA5512 | 2-X Threat Def | ense       | Cisco ASA5512-X Threat Defense | Base, Threat, Malware, URL Filtering | FTD5512        |        | ø          |

Add Interfaces > Sub Interfaceの順に選択します。

| Overv    | iew Analysis       | Policies Dev | vices Object | ts AMP         |                |                              | Deploy 📀   | System | Help 🔻      | admin 🔻   |
|----------|--------------------|--------------|--------------|----------------|----------------|------------------------------|------------|--------|-------------|-----------|
| Device   | e Management       | NAT VPN      | QoS Pla      | tform Settings |                |                              |            |        |             |           |
| FTD5512  |                    |              |              |                |                |                              |            |        |             | 🔀 Cancel  |
| Cisco As | A5512-X Threat Def | ense         |              |                |                |                              |            |        |             |           |
| Devie    | es Routing         | Interfaces   | Inline Sets  | DHCP           |                |                              |            |        |             |           |
| 2        |                    |              |              |                |                |                              |            | 0      | Add Inte    | rfaces •  |
| St       | Interface          |              | Logical Name | е Туре         | Security Zones | MAC Address (Active/Standby) | IP Address | 🔾 Sul  | o Interface |           |
| 0        | GigabitEtherne     | t0/0         |              | Physical       | 1              |                              |            | O Re   | dundant Int | erface    |
| 0        | GigabitEtherne     | t0/1         |              | Physical       |                |                              |            | CO Eth | er Channel  | Interface |

| Add Sub Interface   | Add Sub Interface       |  |  |  |  |  |  |
|---------------------|-------------------------|--|--|--|--|--|--|
| Name: INSI          | Enabled Management Only |  |  |  |  |  |  |
| Security Zone: INSI | DE_ZONE                 |  |  |  |  |  |  |
| Description: INTER  | RNAL                    |  |  |  |  |  |  |
| General IPv4 IF     | V6 Advanced             |  |  |  |  |  |  |
| MTU:                | 1500 (64 - 9198)        |  |  |  |  |  |  |
| Interface *:        | GigabitEthernet0/0      |  |  |  |  |  |  |
| Sub-Interface ID *: | 201 (1 - 4294967295)    |  |  |  |  |  |  |
| VLAN ID:            | 201 (1 - 4094)          |  |  |  |  |  |  |

### インターフェイスの IP 設定は次のとおりです。

| Add Sub Interface |          |              |         |                 |               |  |  |  |
|-------------------|----------|--------------|---------|-----------------|---------------|--|--|--|
| Name:             | INSIDE   |              | Chabled | Management Only |               |  |  |  |
| Security Zone:    | INSIDE_Z | ONE          | ~       |                 |               |  |  |  |
| Description:      | INTERNAL |              |         |                 |               |  |  |  |
| General IPv4      | 4 IPv6   | Advanced     |         |                 |               |  |  |  |
| IP Type:          |          | Use Static I | IP 💌    |                 |               |  |  |  |
| IP Address:       |          | 192.168.20   | 1.1/24  | eg. 1.1.1.1/25  | 5.255.255.228 |  |  |  |

物理インターフェイス(GigabitEthernet0/0)でデュプレックスと速度の設定を指定します。

| General | IPv4 | IPv6 | Advanced | Hardware Configuration |
|---------|------|------|----------|------------------------|
| Duplex: |      |      | auto     | ~                      |
| Speed:  |      |      | auto     | ~                      |

物理インターフェイス(この例では G0/0)をイネーブルにします。

| Edit Physical Interface |        |             |             |                 |  |  |  |  |
|-------------------------|--------|-------------|-------------|-----------------|--|--|--|--|
| Mode:                   | None   |             | ~           |                 |  |  |  |  |
| Name:                   |        |             | 🗹 Enabled   | Management Only |  |  |  |  |
| Security Zone:          |        |             | ~           |                 |  |  |  |  |
| Description:            |        |             |             |                 |  |  |  |  |
| General IPv4            | 1 IPv6 | Advanced    | Hardware Co | nfiguration     |  |  |  |  |
| MTU:                    |        | 1500        |             | (64 - 9198)     |  |  |  |  |
| Interface ID:           |        | GigabitEthe | rnet0/0     |                 |  |  |  |  |

ステップ2:物理インターフェイスの設定

要件に従って、GigabitEthernet0/1 物理インターフェイスを編集します。

| Edit Physical Interface |          |              |       |              |          |                     |          |  |
|-------------------------|----------|--------------|-------|--------------|----------|---------------------|----------|--|
| Mode:                   | None     |              | ~     |              |          |                     |          |  |
| Name:                   | OUTSIDE  |              |       | Enabled      | 🗌 Man    | agement Only        |          |  |
| Security Zone:          | OUTSIDE_ | ZONE         | •     |              |          |                     |          |  |
| Description:            | EXTERNAL |              |       |              |          |                     |          |  |
| General IPv4            | IPv6     | Advanced     | Hard  | dware Config | guration |                     |          |  |
| IP Туре:                |          | Use Static I | p     | ~            |          |                     |          |  |
| IP Address:             |          | 192.168.202  | .1/24 |              |          | eg. 1.1.1.1/255.255 | .255.228 |  |

- ・ ルーテッドインターフェイスのモード: None
- ・ [Name] は、ASA インターフェイスの nameif と同じです。
- FTD では、すべてのインターフェイスのセキュリティ レベルが 0 です。
- same-security-trafficはFTDには適用されません。FTDインターフェイス(inter)と(intra)の間のトラフィックはデフォルトで許可されます

Save and Deployを選択します。

#### 検証

#### FMC GUI:

| De | vices Routing Interfaces | Inline Sets [ | DHCP      |                |                              |                          |  |
|----|--------------------------|---------------|-----------|----------------|------------------------------|--------------------------|--|
| 2  |                          |               |           |                |                              | Add In                   | terfaces 🔹                               |
| St | Interface                | Logical Name  | Туре      | Security Zones | MAC Address (Active/Standby) | IP Address               |  |
| Θ  | 🛗 GigabitEthernet0/0     |               | Physical  |                |                              |                          | s an |
| Θ  | GigabitEthernet0/1       | OUTSIDE       | Physical  | OUTSIDE_ZONE   |                              | 192.168.202.1/24(Static) | ø  |
| 0  | GigabitEthernet0/2       |               | Physical  |                |                              |                          | ø  |
| 0  | GigabitEthernet0/3       |               | Physical  |                |                              |                          | ø  |
| 0  | GigabitEthernet0/4       |               | Physical  |                |                              |                          | ø  |
| 0  | GigabitEthernet0/5       |               | Physical  |                |                              |                          | P  |
| Θ  | Diagnostic0/0            |               | Physical  |                |                              |                          | Ø  |
| Θ  | GigabitEthernet0/0.201   | INSIDE        | SubInterf | INSIDE_ZONE    |                              | 192.168.201.1/24(Static) | Ø 🖥                                      |

#### <#root>

#### >

show interface ip brief

| Interface              | IP-Address    | 0K? | Method | Status           |      | Protocol |
|------------------------|---------------|-----|--------|------------------|------|----------|
| Gigabile therneto/o    | unassigneu    | IES | unset  | up               |      | up       |
| GigabitEthernet0/0.201 | 192.168.201.1 | YES | manual | up               |      | up       |
| GigabitEthernet0/1     | 192.168.202.1 | YES | manual | up               |      | up       |
| GigabitEthernet0/2     | unassigned    | YES | unset  | administratively | down | down     |
| GigabitEthernet0/3     | unassigned    | YES | unset  | administratively | down | down     |
| GigabitEthernet0/4     | unassigned    | YES | unset  | administratively | down | down     |
| GigabitEthernet0/5     | unassigned    | YES | unset  | administratively | down | down     |
| Internal-Control0/0    | 127.0.1.1     | YES | unset  | up               |      | up       |
| Internal-Data0/0       | unassigned    | YES | unset  | up               |      | up       |
| Internal-Data0/1       | unassigned    | YES | unset  | up               |      | up       |
| Internal-Data0/2       | 169.254.1.1   | YES | unset  | up               |      | up       |
| Management0/0          | unassigned    | YES | unset  | up               |      | up       |

#### <#root>

#### >

#### show ip

| System IP Addresses:   |         |               |               |        |
|------------------------|---------|---------------|---------------|--------|
| Interface              | Name    | IP address    | Subnet mask   | Method |
| GigabitEthernet0/0.201 | INSIDE  | 192.168.201.1 | 255.255.255.0 | manual |
| GigabitEthernet0/1     | OUTSIDE | 192.168.202.1 | 255.255.255.0 | manual |
| Current IP Addresses:  |         |               |               |        |
| Interface              | Name    | IP address    | Subnet mask   | Method |
| GigabitEthernet0/0.201 | INSIDE  | 192.168.201.1 | 255.255.255.0 | manual |
| GigabitEthernet0/1     | OUTSIDE | 192.168.202.1 | 255.255.255.0 | manual |

#### FMC GUI と FTD CLI の相関:

|   | > show running-config interface g0/0.201                           |
|---|--|
| Edit Sub Interface  | !<br>interface GigabitEthernet0/0 201                              |
| Name: INSIDE Enabled Management Only  | description INTERNAL<br>vlan 201                                   |
| Description: INTERNAL   | nameif INSIDE<br>cts manual  |
| General IPv4 IPv6 Advanced  | propagate sgt preserve-untag<br>policy static sgt disabled trusted |
| IP Type:         Use Static IP           IP Address:         192.168.201.1/24 | security-level 0<br>ip address 192.168.201.1 255.255.255.0         |

<#root>

```
show interface g0/0.201
Interface GigabitEthernet0/0.201
...
INSIDE
۳,
is up, line protocol is up
 Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
VLAN identifier 201
Description: INTERNAL
        MAC address a89d.21ce.fdea, MTU 1500
IP address 192.168.201.1, subnet mask 255.255.255.0
 Traffic Statistics for "INSIDE":
        1 packets input, 28 bytes
        1 packets output, 28 bytes
        0 packets dropped
>
show interface g0/1
Interface GigabitEthernet0/1 "OUTSIDE", is up, line protocol is up
 Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
        Input flow control is unsupported, output flow control is off
Description: EXTERNAL
        MAC address a89d.21ce.fde7, MTU 1500
IP address 192.168.202.1, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        1 packets output, 64 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 12 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (511/511)
        output queue (blocks free curr/low): hardware (511/511)
 Traffic Statistics for "OUTSIDE":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec, 0 bytes/sec
```

1 minute output rate 0 pkts/sec, 0 bytes/sec 1 minute drop rate, 0 pkts/sec 5 minute input rate 0 pkts/sec, 0 bytes/sec 5 minute output rate 0 pkts/sec, 0 bytes/sec 5 minute drop rate, 0 pkts/sec

#### FTD ルーテッド インターフェイスの動作

ルーテッドインターフェイスが使用されているときのFTDパケットフローを確認します。

解決方法

>

FTD アーキテクチャの概要

FTDデータプレーンの概要は次のとおりです。



次の図は、各エンジン内で実行されるチェックの一部を示しています。



要点

- 下部のチェックは、FTD LINAエンジンのデータパスに対応しています
- ・ 青いボックス内のチェックは、FTD の Snort エンジン インスタンスに相当します。

FTD ルーテッド インターフェイスの概要

- ・ ルーテッド展開でのみ使用可能
- 従来の L3 ファイアウォール展開
- 1 つ以上の物理または論理(VLAN)ルーティング可能インターフェイス
- NAT またはダイナミック ルーティング プロトコルなどの機能を設定可能
- パケットはルートルックアップに基づいて転送され、ネクストホップはARPルックアップに 基づいて解決されます
- ・ 実際のトラフィック ドロップ可能
- LINAエンジンのフルチェックは、Snortエンジンのフルチェックとともに適用されます

最後の理論は次のように視覚化できます。



### 確認

FTDルーテッドインターフェイスでのパケットのトレース

ネットワーク図



適用されているポリシーを確認するには、次のパラメータを指定してパケットトレーサを使用し ます。

| フェイス           |                 |
|----------------|-----------------|
| プロトコル<br>/サービス | TCP ポート 80      |
| 送信元 IP         | 192.168.201.100 |
| 宛先 IP          | 192.168.202.100 |

#### 解決方法

ルーテッドインターフェイスを使用すると、パケットは従来のASAルーテッドインターフェイス と同様に処理されます。ルートルックアップ、モジュラポリシーフレームワーク(MPF)、NAT、 ARPルックアップなどのチェックは、LINAエンジンデータパスで行われます。さらに、アクセス コントロールポリシーで必要な場合、パケットはSnortエンジン(Snortインスタンスの1つ)によ って検査され、判定が生成されてLINAエンジンに返されます。

#### <#root>

>

packet-tracer input INSIDE tcp 192.168.201.100 11111 192.168.202.100 80

Phase: 1

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface Result: ALLOW Config: Additional Information:

found next-hop 192.168.202.100 using egress ifc OUTSIDE

Phase: 2

Type: ACCESS-LIST

Subtype: log Result: ALLOW Config: access-group CSM\_FW\_ACL\_ global access-list CSM\_FW\_ACL\_ advanced permit ip any any rule-id 268437505 access-list CSM\_FW\_ACL\_ remark rule-id 268437505: ACCESS POLICY: FTD5512 - Default/1 access-list CSM\_FW\_ACL\_ remark rule-id 268437505: L4 RULE: DEFAULT ACTION RULE

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 3

Type: CONN-SETTINGS

Subtype: Result: ALLOW Config:

class-map class-default

match any

policy-map global\_policy

class class-default

```
set connection advanced-options UM_STATIC_TCP_MAP
```

service-policy global\_policy global

Additional Information:

Phase: 4

Type: NAT

Subtype: per-session Result: ALLOW Config: Additional Information:

Phase: 5

Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information:

Phase: 6 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information:

Phase: 7 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information:

Phase: 8 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information: New flow created with id 11336, packet dispatched to next module

```
Result:
```

input-interface: INSIDE

input-status: up
input-line-status: up

output-interface: OUTSIDE

output-status: up output-line-status: up Action: allow

>

Signature State St

<#root>

firepower#

show run all tcp-map

!

tcp-map UM\_STATIC\_TCP\_MAP
 no check-retransmission

no checksum-verification exceed-mss allow queue-limit 0 timeout 4 reserved-bits allow syn-data allow synack-data drop invalid-ack drop seq-past-window drop tcp-options range 6 7 allow tcp-options range 9 18 allow tcp-options range 20 255 allow tcp-options selective-ack allow tcp-options timestamp allow tcp-options window-scale allow tcp-options mss allow tcp-options md5 clear ttl-evasion-protection urgent-flag allow window-variation allow-connection

# 関連情報

! >

- <u>Cisco Firepower Threat Defense バージョン 6.1 コンフィギュレーション ガイド</u> (Firepower Device Manager 用)
- ASA 55xx-XデバイスでのFirepower Threat Defenseのインストールとアップグレード
- <u>Cisco Secure Firewall脅威対策</u>
- シスコのテクニカルサポートとダウンロード

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。