

経路選択済み モードの Firepower Threat Defense インターフェイスの設定

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[ルーテッドインターフェイスおよびサブインターフェイスを設定して下さい](#)

[ステップ 1.論理インターフェイスを設定して下さい](#)

[ステップ 2.物理インターフェイスを設定して下さい](#)

[FTD ルーテッドインターフェイス オペレーション](#)

[FTD ルーテッドインターフェイス 外観](#)

[確認](#)

[FTD ルーテッドインターフェイスのパケットをトレースして下さい](#)

[関連情報](#)

概要

この資料は設定を、確認説明したもので、インライン ペアのバックグラウンド操作は Firepower Threat Defense (FTD) アプライアンスでインターフェイスします。

前提条件

要件

この資料のための特定の必要条件がありません。

使用するコンポーネント

- FTD コード 6.1.0.x を実行する ASA5512-X
- 6.1.0.x を実行する Firepower Management Center (FMC)

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。対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

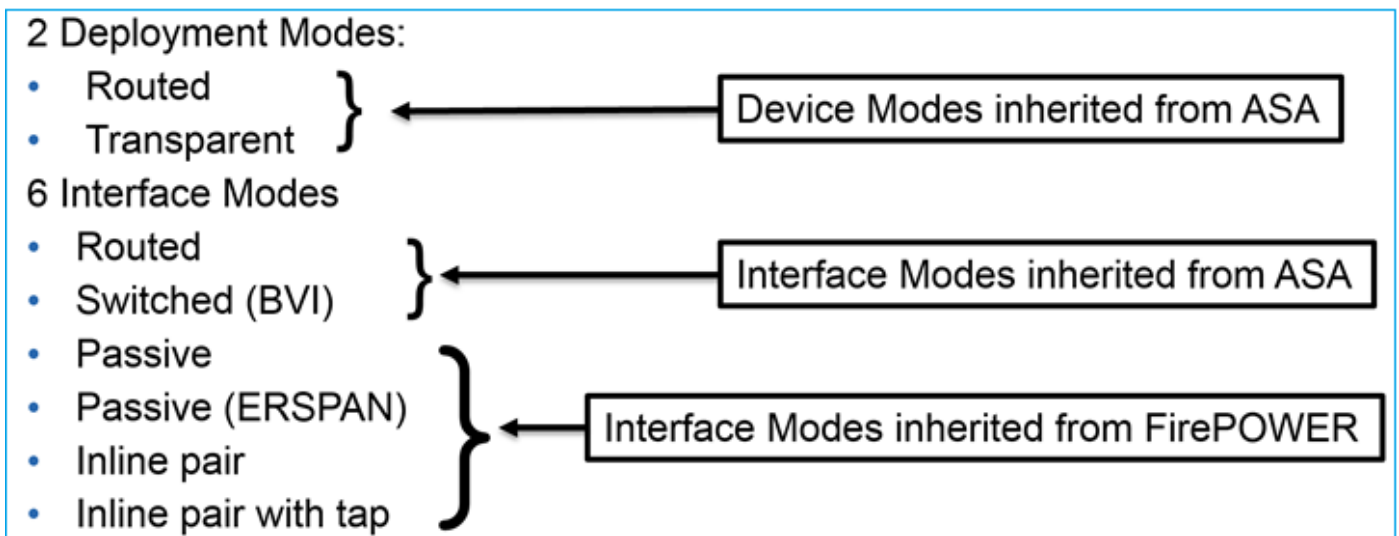
関連製品

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)、アマゾン Web サービス (AW)、キーボード/ビデオ/マウス (KVM)
- FTD ソフトウェアコード 6.2.x およびそれ以降。

背景説明

FTD は次のイメージに示すように 2 つの配置モードおよび 6 つのインターフェイス モードを提供します:



注: 単一 FTD アプライアンスのインターフェイス モードを混合できます。

さまざまな FTD 配備およびインターフェイス モードのハイレベルな概要:

FTD インターフェイス モード	FTD 配置モード	説明	トラフィックは廃棄することができます
Routed	Routed	リーナ完全なエンジンおよび Snort エンジン チェック	○
交換	トランスペアレント	リーナ完全なエンジンおよび Snort エンジン チェック	○
インライン ペア	経路選択済みか	リーナ部分的なエンジンおよび完	○

タップとのイン ラインペア	透過的な 経路選択済みか	全な Snort エンジン チェック リーナ部分的なエンジンおよび完	なし
パッシブ	透過的な 経路選択済みか	全な Snort エンジン チェック リーナ部分的なエンジンおよび完	なし
受動態 (ERSPAN)	Routed	全な Snort エンジン チェック リーナ部分的なエンジンおよび完	なし

設定

ネットワーク図



ルーテッドインターフェイスおよびサブインターフェイスを設定して下さい

サブインターフェイス G0/0.201 を設定し、次の必要条件によって G0/1 をインターフェイスさせて下さい:

interface	G0/0.201	G0/1
名前	内部	OUTSIDE
セキュリティゾーン	INSIDE_ZONE	OUTSIDE_ZONE
説明	内部	外部
補助的なインターフェイス ID	201	-
VLAN ID	201	-
IPv4	192.168.201.1/24	192.168.202.1/24
二重/速度	Auto	Auto

解決策

ステップ 1. 論理インターフェイスを設定して下さい

デバイス > デバイス管理 にナビゲートし、適切なデバイスを選択し、Edit アイコンを選択して下さい:

Overview Analysis Policies **Devices** Objects AMP Deploy System

Device Management NAT VPN QoS Platform Settings

By Group

Name	Group	Model	License Type	Access Control Policy
Ungrouped (8) FTD5512 10.62.148.10 - Cisco ASA5512-X Threat Defense		Cisco ASA5512-X Threat Defense	Base, Threat, Malware, URL Filtering	FTD5512

インターフェイス > Sub インターフェイスを『Add』を選択して下さい:

Overview Analysis Policies **Devices** Objects AMP Deploy System Help admin

Device Management NAT VPN QoS Platform Settings

FTD5512 Save Cancel

Cisco ASA5512-X Threat Defense

Devices Routing **Interfaces** Inline Sets DHCP

St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
	GigabitEthernet0/0		Physical			
	GigabitEthernet0/1		Physical			

Add Interfaces

- Sub Interface
- Redundant Interface
- Ether Channel Interface

必要条件によってサブインターフェイス設定を設定して下さい:

Add Sub Interface

Name: Enabled Management Only

Security Zone: ▼

Description:

General IPv4 IPv6 Advanced

MTU: (64 - 9198)

Interface *: ▼ Enabled

Sub-Interface ID *: (1 - 4294967295)

VLAN ID: (1 - 4094)

IP 設定をインターフェイスさせて下さい:

Add Sub Interface

Name:	<input type="text" value="INSIDE"/>	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Management Only
Security Zone:	<input type="text" value="INSIDE_ZONE"/>		
Description:	<input type="text" value="INTERNAL"/>		
General IPv4 IPv6 Advanced			
IP Type:	<input type="text" value="Use Static IP"/>		
IP Address:	<input type="text" value="192.168.201.1/24"/>	eg. 1.1.1.1/255.255.255.228	

物理インターフェイス (GigabitEthernet0/0) の下で二重および速度設定を規定して下さい:

General IPv4 IPv6 Advanced Hardware Configuration	
Duplex:	<input type="text" value="auto"/>
Speed:	<input type="text" value="auto"/>

物理インターフェイス (G0/0 この場合) をイネーブルに設定して下さい:

Edit Physical Interface	
Mode:	<input type="text" value="None"/>
Name:	<input type="text"/> <input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Management Only
Security Zone:	<input type="text"/>
Description:	<input type="text"/>
General IPv4 IPv6 Advanced Hardware Configuration	
MTU:	<input type="text" value="1500"/> (64 - 9198)
Interface ID:	<input type="text" value="GigabitEthernet0/0"/>

ステップ 2.物理インターフェイスを設定して下さい

必要条件によって GigabitEthernet0/1 物理インターフェイスを編集して下さい:

Edit Physical Interface

Mode: ▼

Name: Enabled Management Only

Security Zone: ▼

Description:

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: ▼

IP Address: eg. 1.1.1.1/255.255.255.228

- ルーテッドインターフェイスに関してはモードは次のとおりです: なし
 - 名前は ASA インターフェイス nameif と同等です
 - FTD ですべてのインターフェイスにセキュリティレベルが = 0 あります
 - 同じセキュリティトラフィックは FTD の適用されません。FTD インターフェイス (内側) とヘアピンング間のトラフィックは (内部) デフォルトで許可されます
- 『SAVE』 を選択し、展開して下さい。

確認

FMC GUI から:

St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
●	GigabitEthernet0/0		Physical			
●	GigabitEthernet0/1	OUTSIDE	Physical	OUTSIDE_ZONE		192.168.202.1/24(Static)
●	GigabitEthernet0/2		Physical			
●	GigabitEthernet0/3		Physical			
●	GigabitEthernet0/4		Physical			
●	GigabitEthernet0/5		Physical			
●	Diagnostic0/0		Physical			
●	GigabitEthernet0/0.201	INSIDE	SubInterf...	INSIDE_ZONE		192.168.201.1/24(Static)

FTD CLI から:

> **show interface ip brief**

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	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-Contro0/0	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

> **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 および FTD CLI 関連:

Edit Sub Interface

Name: Enabled Management Only

Security Zone:

Description:

General **IPv4** IPv6 Advanced

IP Type:

IP Address:

```
> show running-config interface g0/0.201
!
interface GigabitEthernet0/0.201
description INTERNAL
vlan 201
nameif INSIDE
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.201.1 255.255.255.0
```

> **show interface g0/0.201**

```
Interface GigabitEthernet0/0.201 "INSIDE", 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

>

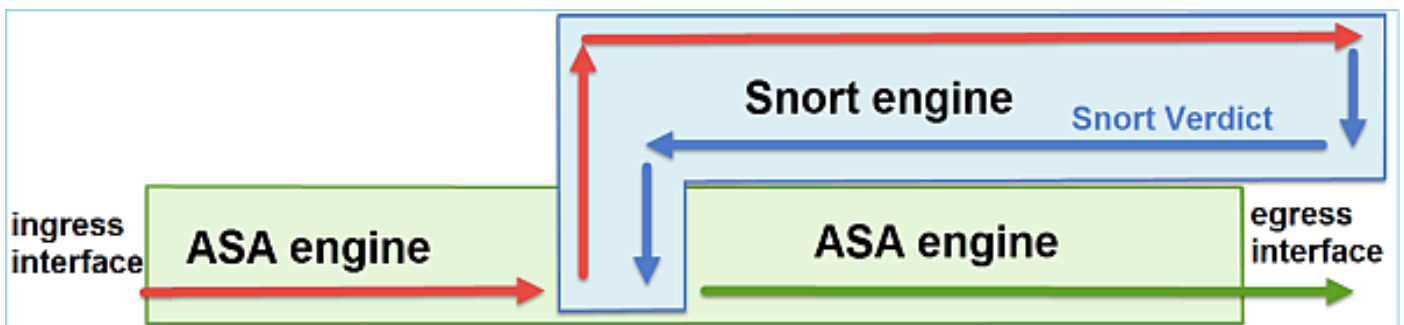
FTD ルーテッドインターフェイス オペレーション

ルーテッドインターフェイスが使用中のとき処理する FTD パケットを確認して下さい。

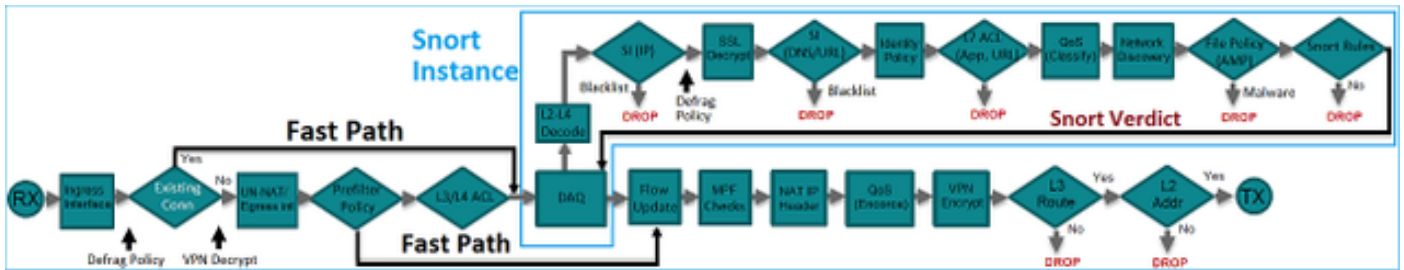
解決策

FTD アーキテクチャーの概要

FTD データ平面のハイレベルな概要:



次のピクチャは各エンジンの中で行われるいくつかのチェックを示します:



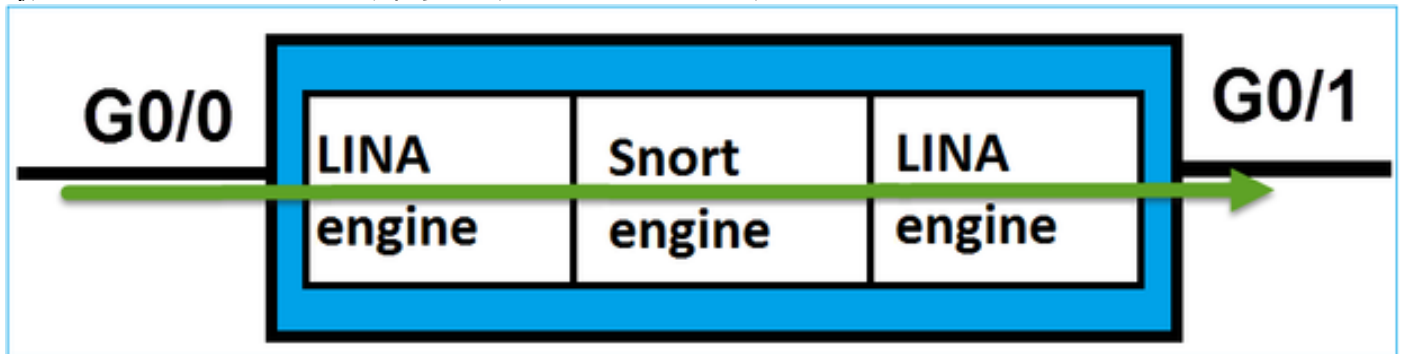
キーポイント

- 一番下チェックは FTD リーナ エンジン データパスに対応します
- ブルーボックスの中のチェックは FTD Snort エンジン 例に対応します

FTD ルーテッドインターフェイス 外観

- 経路選択済み配備でだけ利用可能
- 従来の L3 ファイアウォール配備
- 1つ以上の物理的か論理的な (VLAN) ルート可能なインターフェイス
- 設定されるべき NAT またはダイナミック ルーティング プロトコルのような割り当て機能
- パケットはルート ルックアップに基づいて転送され、ARP ルックアップに基づくネクストホップは解決されます
- 実際のトラフィックは廃棄することができます
- 完全なリーナ エンジン チェックは完全な Snort エンジン チェックと共に適用します

最後のポイントは次の通り視覚化することができます:



検証

FTD ルーテッドインターフェイスのパケットをトレースして下さい

ネットワーク図



応用ポリシーを見るのに次のパラメータとパケット トレーサーを使用して下さい:

インプットイ
ンターフェイ 内部
ス
プロトコル
/サービス TCPポート 80
送信元 IP 192.168.201.1
 00
宛先 IP 192.168.202.1
 00

解決策

ルーテッドインターフェイスが使用されるときパケットは標準的な ASA ルーテッドインターフェイスへの同じような方法で処理されます。ルート ルックアップ、モジュラ 政策の枠組 (MPF)、NAT、ARP ルックアップ等のようなチェックはリーナ エンジン データパスで起こっています。アクセスコントロール ポリシーがそう必要となればさらに、パケットは Snort エンジン (Snort 例の 1) によって評決 (ブラックリスト、ホワイトリスト) がリーナ エンジンに生成され、戻るところ検査されます:

```
> 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 -

Defau

lt/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

>

注: フェーズ 4 でパケットは UM_STATIC_TCP_MAP と呼ばれる TCP マップに対してチェックされます。これは FTD のデフォルト TCP マップです。

```
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

- [Firepower デバイスマネージャのための Cisco Firepower Threat Defense コンフィギュレーションガイド、バージョン 6.1](#)
- [Firepower Threat Defense の ASA 55xx-X デバイスでのインストール手順およびアップグレードします](#)
- [Firepower Threat Defense \(FTD\) キャプチャおよびパケットトレーサーを操作する場合](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)